УЧЕБНОЕ ПОСОБИЕ ПОД РЕДАКЦИЕЙ М.С. ЦВЕТКОВОЙ
ПРОФИЛАКТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЕТЕЙ

Баранова Мария Вячеславовна,
главный специалист Информационного центра
ГАУ ДПО ЯО «ИРО»

Лучший «фильтр» обеспечения информационной безопасности в голове самого ребёнка, взрослым нужно только грамотно настроить этот «фильтр»

ЦИФРОВОЕ ПОКОЛЕНИЕ

Современные российские школьники

- домашний компьютер + гаджеты (мобильники, смартфоны, айпады)
- легко совмещают реальность и виртуальность
- Интернет становится важным инструментом социализации подрастающих поколений (посредством Интернета открывают для себя мир, новый человек в значительной степени формируется под его влиянием)
- Интернет дает пользователю огромные возможности как инструмент поиска и получения информации и как высокотехнологичное средство коммуникации

новое цифровое поколение, вооруженное разнообразными гаджетами и чувствующее себя естественно и непринужденно в Рунете и в Глобальной Сети в целом

ПОТРЕБНОСТЬ В ИНФОРМАЦИИ = ПОТРЕБНОСТЬ В ИНТЕРНЕТЕ

Современные школьники, у которых удовлетворены базовые потребности в еде, тепле, комфорте и безопасности, стремятся к удовлетворению более высоких потребностей — в любви и внимании, в признании, в самореализации и личностном росте. Дети и подростки пытаются реализовать вышеперечисленные потребности и в Интернете. Если общение в Интернете нередко создает лишь иллюзию удовлетворения потребности в любви и принятии, то в реализации познавательной потребности — жажды знаний и желания воспринимать как можно больше информации — Интернет играет сегодня ключевую роль. Непрерывная информационная связь с окружающим миром, социальной средой, в которой подросток действует как активный субъект, — одно из важнейших условий его информационной социализации. Ее важным фактором в XXI веке становится ***Интернет***.

ИНТЕРНЕТ

виртуальная культура

всемирная паутина

информационная социализация личности

сеть сетей

ИНТЕРНЕТ → профессиональная, социальная, бытовая реальности

→ ~~территориальные и временные границы~~

→ жизнь более разнообразная и информативная

становление культурной модели ИНФОРМАЦИОННОГО ОБЩЕСТВА

ИНТЕРНЕТ

Интернет **–**

это объединенные между собой компьютерные сети, глобальная мировая система передачи информации с помощью информационно-вычислительных ресурсов

ВИДЫ ИНФОРМАЦИИ В ИНТЕРНЕТЕ

Информационные сайты

Интернет изначально создавался как среда для обмена информацией , поэтому данная категория основная и является наиболее крупной.

Виды по характеру предоставляемого контента

- информационно-тематические,
- новостные,
- развлекательные сайты,
- сайты-библиотеки,
- сайты-базы, (например базы рефератов),
- разнообразные сайты-справочники,
- онлайн-энциклопедии и словари,
- сайты-каталоги, обобщающие информацию о других сайтах и т. п.

ВИДЫ ИНФОРМАЦИИ В ИНТЕРНЕТЕ

Онлайн-сервисы

К данной категории относятся поисковые системы, почтовые сервисы, хостинги, файлообменники, а также сайты для общения: форумы, блоги, чаты, доски объявлений, социальные Сети, сервисы «Вопрос-ответ», сайты знакомств, биржи фрилансеров и др.

Сайты электронной коммерции

Сюда входят в первую очередь интернет-магазины, сайты электронных платежных систем, сайты банков и системы онлайн-банкинга.

Интернет-представительства

Сюда входят как личные странички отдельных пользователей, так и официальные сайты органов государственной власти и различных организаций.

ИНТЕРНЕТ-ГРАМОТНОСТЬ = ИНТЕРНЕТ-БЕЗОПАСНОСТЬ

По сравнению со взрослыми дети, подростки и молодежь постигают технологические новинки на лету, естественно и без напряжения. Взрослые в силу занятости и уже привычных схем поведения не всегда за ними поспевают

Активное и длительное пребывание в нем — влиятельный фактор развития и социализации детей, в процессе которой формируются системы личных ценностей

В **2006–2007** годах началась интернетизация школы в рамках национального **проекта «Образование»**

последние российские и европейские исследования развеяли миф о том, что наши дети все умеют и знают в цифровом мире. По данным исследования Фонда Развития Интернет **75 %** подростков обучались использованию Интернета самостоятельно. Умение пользоваться Интернетом оказывается неявным знанием, полученным «на ощупь», через серию собственных проб и ошибок.

ВОПРОС БЕЗОПАСНОСТИ!!!

ДЕТИ В ИНТЕРНЕТЕ

Четверть российских детей проводит в Интернете от 7 до 14 часов в неделю

Каждый пятый – больше 21 часа в неделю, то есть около 3 часов в день

75% детей играют в игры сами с собой и против компьютера

- на приставках
- на компьютерах
- в Интернете
- на мобильных телефонах

64% - в одиночку

10% - с членами семьи

12% - с друзьями

ИНТЕРНЕТ-УГРОЗЫ ДЛЯ ДЕТЕЙ/ПОДРОСТКОВ

Контентные риски

- обилие откровенных материалов сексуального характера (дезориентация ребенка, вред психике, неверное представление о сути интимных отношений между людьми, эксплуатация и извращение естественного любопытства детей)
- дети все чаще используются дельцами от порнобизнеса в качестве моделей для детской порнографии
- пропаганда экстремизма, материалы террористического характера наносят серьезный вред здоровью, развитию и безопасности детей
- пропаганда наркотиков, насилия и жестокости, суицидального поведения, абортов, самоповреждений, в Сети немало сомнительных развлечений (онлайн-игры, пропагандирующие секс, жестокость и насилие, требующие немалых финансовых вложений, азартные игры) - опасны для неокрепшей детской психики
- электронные ресурсы, созданные и деструктивными религиозными сектами, - особая опасность для незрелой психики

ИНТЕРНЕТ-УГРОЗЫ ДЛЯ ДЕТЕЙ/ПОДРОСТКОВ

Нарушения безопасности

- скачивание неизвестных файлов, которые могут оказаться вирусами или содержать незаконную информацию
- опасность компьютерных мошенников, спамеров, фишеров (номер кредитной карточки родителей, пароль от электронного кошелька, свой настоящий адрес и т.п.)
- социальные сети и блоги, на которых ребенок оставляет о себе немало настоящей информации, завязывает небезопасные знакомства, нередко подвергается незаметной для него деструктивной психологической и нравственно-духовной обработке

Коммуникативные риски

- интернет-зависимость (появляется в навязчивом желании неограниченно долго продолжать сетевое общение)
- появление виртуальных знакомых и друзей, среди которых могут оказаться педофилы и извращенцы (груминг), мошенники и хулиганы, а виртуальное хамство и розыгрыши могут закончиться киберпреследованием и киберунижением (кибербуллинг, хеппислепинг, буллицид)

ПРОФИЛАКТИКА ИНТЕРНЕТ-УГРОЗ

информационно-просветительская деятельность –

воздействие на формирование грамотного и ответственного сознания у детей и родителей – знать правила безопасного поведения в Интернете

школа является очень важным каналом для распространения

Просвещение и обучение пользователей

- педагоги
- родители
- дети

- младшие школьники,
- школьники средних классов,
- старшеклассники

ПРОФИЛАКТИКА ИНТЕРНЕТ-УГРОЗ

- Знание проектов и программ официальных властей, общественных организаций и ресурсов известных компаний (например, Майкрософт) в области безопасности в Сети
- Разработка программ, методик проведения бесед
- Проведение мероприятий:

- единые классные часы
- дни безопасного интернета
- акции типа «Открытый микрофон» и др.
- организация работы школьного уполномоченного
- ознакомление с правилами и другой информацией по безопасности через сайт школы (специальный раздел), стенды в коридорах/классе (памятки, статьи о новых видах интернет-угроз и новых способах борьбы с ними)
- родительские собрания (беседы, памятки, игры и т.п.)

- Продвижение позитивного детского интернета (формирование позитивного образовательного интернет-пространства)

ОДОБРЕНА
решением федерального учебно-методического
объединения по общему образованию
(протокол от 26 октября 2020 № 4/20)

ПРИМЕРНАЯ ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА
УЧЕБНОГО КУРСА
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»
ДЛЯ ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЙ, РЕАЛИЗУЮЩИХ
ПРОГРАММЫ НАЧАЛЬНОГО ОБЩЕГО ОБРАЗОВАНИЯ

Место учебного курса «Информационная безопасность»

в учебном плане

Особенностью программы курса для начальных классов является ее органичное включение в учебно-воспитательную деятельность по социализации детей в окружающем их мире, который быстро меняется, наполняясь все новыми цифровыми сервисами и ресурсами. Программа курса рассчитана на 30 учебных часов и может быть реализована как за один год обучения, так и непрерывно с 1 по 4 класс по модулям содержания. Программа курса ориентирована на включение в контекст обучения и воспитания новых видов информационных угроз и средств противодействия им.

Реализация программы учебного курса возможна в разных формах:

— в рамках отдельного учебного курса «Информационная безопасность» для внеурочной деятельности по выбору из объема часов, формируемых самостоятельно образовательной организацией;

— в интеграции с предметом «Окружающий мир» или курсом «Информатика» по модулям содержания курса путем дополнения программы учебного предмета модулями программы учебного курса по информационной безопасности;

— в рамках часов, предусмотренных по программе воспитания (социализации) в образовательной организации для начального общего образования.

СОДЕРЖАНИЕ УЧЕБНОГО КУРСА «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ» ДЛЯ НАЧАЛЬНОГО ОБЩЕГО ОБРАЗОВАНИЯ

Содержание учебного курса «Информационная безопасность» программы складывается из двух линий:

1) Информационное пространство и правила информационной безопасности.

Модуль 1. Правила безопасной работы в сети Интернет с мобильным телефоном. Угрозы в сети Интернет и мобильных сетях связи

Модуль 2. Правила безопасной работы в сети Интернет с планшетом или на компьютере

2) Информационное общество и информационная культура

Модуль 3. Сеть Интернет

Модуль 4. Правила безопасной работы в социальной сети

ПЛАНИРОВАНИЕ УЧЕБНОГО КУРСА «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ» ДЛЯ НАЧАЛЬНОГО ОБЩЕГО ОБРАЗОВАНИЯ

Программа учебного курса для 10—11 классов среднего общего образования рассчитана на объем ***не менее 30 часов***. Программа курса может быть реализована как:

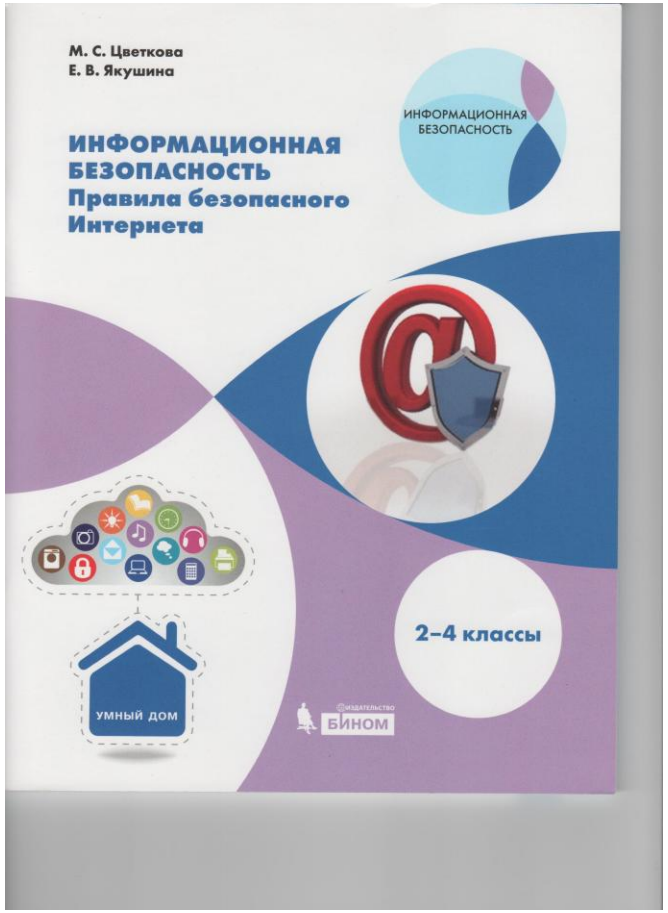
- самостоятельный учебный курс во внеурочной деятельности детей **за один год**
- в том числе в курсе «Информатика» (во 2, 3 или 4 классе)
- интегрирована **дополнительными модулями** содержания программы по курсу в программу по предмету «Окружающий мир» (с 1 по 4 класс по выбору образовательной организации) в форме проведения тематических уроков
- в рамках школьных мероприятий с участием родителей по модулям календарного планирования программы воспитания (социализации) обучающихся

Варианты учебного планирования:

Вариант 1. Планирование обучения **за один год обучения**. Один урок в неделю. 30 уроков.

Вариант 2. Планирование обучения/программы воспитания по модулям **с 1 по 4 класс**.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. ПРАВИЛА БЕЗОПАСНОГО ИНТЕРНЕТА. 2–4 КЛАССЫ : УЧЕБНОЕ ПОСОБИЕ М. С. ЦВЕТКОВА, Е. В. ЯКУШИНА



Предназначено для проведения уроков информационной безопасности в рамках предмета «Окружающий мир» или курса «Информатика» во 2–4 классах.

Включает темы: «Правила безопасной работы в сети Интернет с мобильным телефоном», «Правила безопасной работы в сети Интернет с планшетом или на компьютере», «Путешествуем в сети Интернет», «Правила безопасной работы в социальной сети». Широко представлены задания с использованием электронного приложения, а также тесты для самоконтроля.

К пособию на сайте издательства прилагается бесплатное электронное приложение с открытыми познавательными ресурсами для начальной школы в сети Интернет (http://lbz.ru/metodist/authors/ib/2-4.php)

Часть 1

ПРАВИЛА БЕЗОПАСНОЙ РАБОТЫ В СЕТИ ИНТЕРНЕТ С МОБИЛЬНЫМ ТЕЛЕФОНОМ

Мобильным телефоном пользуются для разговора на расстоянии и для передачи текстовых сообщений. Сейчас это самый распространённый способ общения среди людей. Главное достоинство мобильного телефона в том, что его можно носить с собой и в любом месте быть постоянно на связи.

Современные телефоны (их называют смартфоны, то есть умные телефоны) подключаются к Интернету. Поэтому с помощью смартфона можно использовать различные возможности этой глобальной сети.

Рис. 6. Виды мобильных телефонов

Мобильный телефон работает с применением спутниковой связи.

В мире миллионы мобильных телефонов, люди связываются друг с другом по нескольку раз в день. Они могут разговаривать, даже видеть своего собеседника на экране, посылать текстовые сообщения через СМС — службу мгновенных сообщений, контактировать по сетям рассылок, передавать картинки, видео- и звуковые записи.

> Нужно соблюдать культуру общения, а также осторожность при получении звонков и сообщений от незнакомых тебе адресатов.

Запомни правила Смайлика для безопасной работы с мобильным телефоном, о которых будет рассказано дальше.

1.1. СМС от неизвестных лиц

Если ты получил СМС от неизвестных лиц, помни, что на них нельзя отвечать. Никогда не выполняй просьбы, не обращай внимания на содержание СМС-сообщений от незнакомых людей.

Тебя может подстерегать множество опасностей. Такие СМС обнуляют деньги на твоём счёте. Они могут быть направлены на достижение различных вредных целей.

Никогда не выполняй просьбы, не обращай внимания на содержание СМС от неизвестных тебе лиц. Показывай такие СМС своим близким в семье!

Обратись к родителям, чтобы они связались с мобильным оператором твоего телефона и выяснили, почему приходят такие СМС.

С помощью старших нужно заблокировать нежелательные адреса или навязчивые рекламные рассылки.

Тест 1. Выбери номер правильного ответа для каждого вопроса.

1) Расшифруй, что значит СМС.
- а) Специальные мгновенные сообщения.
- б) Служба мгновенных сообщений.
- в) Служба мобильных сообщений.

2) Что позволяет делать СМС?
- а) Обмениваться текстовыми сообщениями.
- б) Обмениваться фотографиями.
- в) Обмениваться видеороликами.

3) В каких случаях необходимо соблюдать культуру общения?
- а) Культуру общения, а также осторожность следует соблюдать при общении в школе, а также в незнакомых местах.
- б) Культуру общения следует соблюдать при общении только при телефонном разговоре.
- в) Культуру общения следует соблюдать всегда и везде, во всех случаях.

4) Что необходимо сделать, если ты получил СМС от неизвестных лиц?
- а) Посоветоваться с родителями и удалить СМС.
- б) Сразу написать ответ.
- в) Не отвечать на СМС.

5) Опиши свои действия, если ты получил СМС-сообщение или звонок от незнакомца с просьбой перечислить деньги на его номер телефона.
- а) Выполню просьбу незнакомца.
- б) Покажу такие СМС или расскажу о таких звонках своим друзьям.
- в) Обращусь к родителям, чтобы они связались с мобильным оператором телефона и заблокировали номер отправителя.

1.2. Ложные сообщения

Не всем СМС можно доверять. Сначала нужно проанализировать текст полученного сообщения, даже если оно пришло от знакомых тебе людей. Возможно, оно содержит ложь.

Бывают сообщения, которые путём обмана выманивают деньги. Например, кто-то просит тебя срочно положить какую-то сумму на номер чужого телефона. Не торопись выполнять эту просьбу. Обязательно покажи сообщение близким, удали его.

Все денежные вопросы решай прежде всего с родителями. Если тебе пришло подозрительное СМС, сразу обратись к ним.

Никогда не сообщай номер своего телефона незнакомым людям, не публикуй его в Интернете в открытом доступе. Некоторые сайты просят пользователя ввести номер своего телефона. В дальнейшем он добавляется в базу адресов рассылки СМС-спама (навязчивых рекламных сообщений) и может быть использован для противозаконных действий.

Тест 2. Выбери номер правильного ответа для каждого вопроса.

6) Всем ли СМС, пришедшим на твой номер телефона, можно доверять?
   а) Да.
   б) Нет.

7) С кем нужно решать вопрос о пополнении счёта на телефоне?
   а) Только с родителями.
   б) С неизвестными тебе отправителями СМС-сообщений.
   в) Со всеми людьми, которые это предлагают.

8) Можно ли передавать свой номер телефона на сайтах в социальных сетях?
   а) Да.
   б) Нет.

9) Что такое СМС-спам?
   а) Навязчивые рекламные сообщения, нежелательная рассылка.
   б) Полезная информация.

1.3. Угрозы в СМС

Не реагируй на угрозы в твой адрес — часто злоумышленники используют испуг, чтобы выманивать деньги.

Бывает, что недруги угрожают тебе, причём ты знаешь, кто это.

1.4. Звонки с предложениями

Звонок с рекламой, предложением что-то купить или подключиться к какой-то услуге может повлечь денежные траты и нанести тебе вред.

Спокойно и кратко сообщи, что тебе ничего не нужно, и отключи звонок или удали СМС-сообщение.

Тест 4. Выбери номер правильного ответа.

12) Как реагировать на звонок или СМС-сообщение с рекламой, предложением что-то купить или подключиться к какой-то услуге?

а) Всегда спокойно и кратко сообщать, что тебе ничего не нужно, прервать звонок. Показать номер звонка родителям, чтобы они заблокировали этот номер.

б) Поддержать беседу.

в) Выполнить просьбу, требование, содержащиеся в рекламном сообщении.

1.6. Подключение телефона к «Вай-Фай» сети

Сейчас в общественных местах доступно бесплатное подключение к беспроводной сети «Вай-Фай» (Wi-Fi) для выхода в Интернет.

Современный смартфон имеет возможность подключения к беспроводным сетям Wi-Fi.

В настройках телефона можно увидеть список доступных Wi-Fi сетей.

Открытые сети НЕ отмечены значком «замок». Обычно при подключении смартфона к открытой сети Wi-Fi требуется регистрация, для чего необходимо сообщить номер твоего телефона, на который придёт СМС с паролем доступа в сеть. При этом на экране будет указано, что ты соглашаешься с тем, что сообщаешь свои данные (личный номер телефона).

Если сеть Wi-Fi открыта и для подключения к ней не требуется регистрация, то пользоваться ею опасно, так как в такой сети возможна кража личных данных.

Защищённая частная сеть Wi-Fi показана в списке сетей на твоём телефоне со значком «замок». При попытке входа в такую сеть будет запрошен пароль доступа, который известен только пользователям этой сети.

ЭЛЕКТРОННОЕ ПРИЛОЖЕНИЕ К ПОСОБИЮ ПРАВИЛА БЕЗОПАСНОГО ИНТЕРНЕТА 2-4 КЛАССЫ СЕРИИ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

серии «Информационная безопасность» для 2–4 классов — смотри сайт издательства, раздел «Авторские мастерские»:

http://lbz.ru/metodist/authors/ib/2-4.php

Задание 1.1

Посмотри дома со взрослыми или на уроке с помощью учителя видеоурок «Уроки хороших манер. Дресс-код / Как пользоваться мобильным телефоном».

Составь свою памятку правил пользования мобильным телефоном.

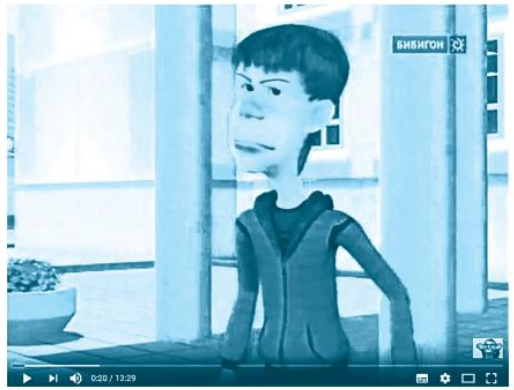


Рис. 7. Видеоурок «Уроки хороших манер»

27

Часть 1. Правила безопасной работы в сети Интернет с мобильным телефоном

Задание 1.1

Посмотри дома со взрослыми или на уроке с помощью учителя видеоуроки.

Ознакомься с видеоуроком канала БИБИГОН "Дресс-код / как пользоваться мобильным телефоном"

Составь свою памятку правил пользования мобильным телефоном

Задание 1.2

Ознакомься с видеоуроком СПАС Экстрим "Мобильные мошенники"

Ответь на вопрос: *Кто такие мобильные мошенники и чем они опасны?*

https://lbz.ru/metodist/authors/ib/2-4.php

ЭЛЕКТРОННОЕ ПРИЛОЖЕНИЕ К ПОСОБИЮ ПРАВИЛА БЕЗОПАСНОГО ИНТЕРНЕТА 2-4 КЛАССЫ СЕРИИ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Часть 2. Правила безопасной работы в сети Интернет с планшетом или на компьютере

Задание 2.2

Используй пособие компании МТС для младших школьников с сайта «Дети в Интернете»

(http://www.safety.mts.ru/ru/deti_v_inete/for_children/rules/)

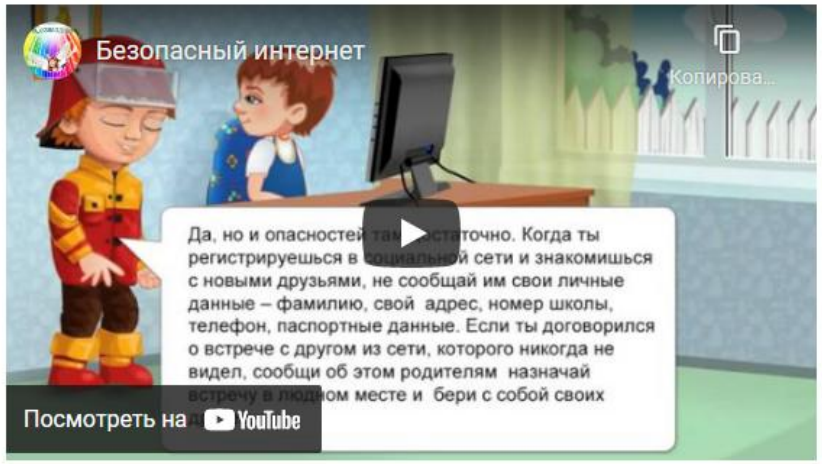
Пособие для раскрашивания: Скачать

Распечатай, прочитай тексты и раскрась картинки.

Задание 2.3

Посмотри дома с вместе со взрослыми или на уроке с помощью учителя видеоурок СПАС Экстрим Безопасный интернет

Составь личную памятку безопасности в сети Интернет



https://lbz.ru/metodist/authors/ib/2-4.php

ОДОБРЕНА
решением федерального учебно-методического объединения по общему образованию
(протокол от 26 октября 2020 № 4/20)

ПРИМЕРНАЯ ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА
УЧЕБНОГО КУРСА
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»
ДЛЯ ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЙ, РЕАЛИЗУЮЩИХ
ПРОГРАММЫ ОСНОВНОГО ОБЩЕГО ОБРАЗОВАНИЯ

Место учебного курса «Информационная безопасность» в учебном плане

Особенностью программы курса является ее поэтапное развитие для разных возрастных групп обучающихся основного общего образования с учетом из возрастных особенностей. Программа курса ориентирована на включение в контекст обучения и воспитания новых видов информационных угроз и средств противодействия им. Программа курса представлена ***двумя разделами по возрастным группам:*** для **5—6** классов и 7—9 классов.

Реализация программы учебного курса возможна в разных формах:

— как дополнительные модули обучения в интеграции с предметами «Информатика» и (или) «ОБЖ» для двух возрастных групп: **5—6** и 7—9 классов (от 30 учебных часов для каждой возрастной группы);

— в рамках отдельного учебного курса «Информационная безопасность» для внеурочной деятельности по выбору из объема часов, формируемых самостоятельно образовательной организацией;

— в рамках часов, предусмотренных по программе воспитания (социализации) в образовательной организации для разных уровней общего образования.

СОДЕРЖАНИЕ УЧЕБНОГО КУРСА «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ» ДЛЯ ОСНОВНОГО ОБЩЕГО ОБРАЗОВАНИЯ

Содержание учебного курса «Информационная безопасность» для разных возрастных модулей программы складывается из двух линий:

5 – 6 классы

1) Информационное общество и информационная культура.

Модуль 1. Информационное общество

2) Информационное пространство и правила информационной безопасности.

Модуль 2. Правила пользователей сети Интернет

ПЛАНИРОВАНИЕ УЧЕБНОГО КУРСА «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ» ДЛЯ ОСНОВНОГО ОБЩЕГО ОБРАЗОВАНИЯ

Программа учебного курса для **5—6 классов** основного общего образования рассчитана на объем не менее 30 часов. Программа курса может быть реализована по выбору образовательной организации как:

- самостоятельный учебный курс во внеурочной деятельности детей **за один год обучения**
- отдельными модулями в программах освоения учебных предметов «Информатика» и (или) «ОБЖ» (в **5—6 классах**)
- в рамках школьных мероприятий с участием родителей интегрирована модулями в календарное планирование программы воспитания

Варианты учебного планирования:

Вариант 1. Планирование обучения **за один год обучения**. Один урок в неделю. 30 уроков.

Вариант 2. Планирование обучения по модулям в **5—6 классах**.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. БЕЗОПАСНОЕ ПОВЕДЕНИЕ В СЕТИ ИНТЕРНЕТ. 5–6 КЛАССЫ : УЧЕБНОЕ ПОСОБИЕ ЦВЕТКОВА М. С., ЯКУШИНА Е. В.

Предназначено для проведения уроков информационной безопасности в 5–6 классах (в рамках курсов «Информатика», «ОБЖ», во внеурочной деятельности) и состоит из двух частей: что нужно знать о сети Интернет и как использовать её ресурсы при самостоятельной работе.

К пособию на сайте издательства прилагается бесплатное электронное приложение с видеоматериалами в открытом доступе телеканала Карусель и ИТ-компаний (http://lbz.ru/metodist/authors/ib/5-6.php)

Часть 1

ЧТО НУЖНО ЗНАТЬ? ПРОСТРАНСТВО ИНТЕРНЕТА НА ПЛАНЕТЕ ЗЕМЛЯ

Интернет прочно вошёл в нашу жизнь. Повсеместное его распространение сильно влияет на общение людей, делая открытым мгновенное взаимодействие для получения разнообразной информации в любой точке мира. Можно покупать билеты, заказывать товары, читать книги, просматривать кинофильмы — главное, чтобы была доступна Сеть. Благодаря Интернету появилась возможность учиться и работать не выходя из дома. Интернет не знает границ, единственный барьер — это разные языки, на которых говорят жители Земли. Но и здесь уже предлагается электронный перевод.

Сейчас Интернет превратился в **единое информационное пространство**, которое нас всех окружает, непрерывно поставляя информацию. Оно *влияет* на наше мнение и поведение, причём как в хорошую, так и в плохую сторону.

Информационное пространство стало нашим окружающим миром, и нам нужно учиться в нём жить, различая полезное и вредное, доброе и злое, правдивое и лживое, важное и второстепенное, правильное и ошибочное...

ЭЛЕКТРОННОЕ ПРИЛОЖЕНИЕ

Задание 1.1

Ознакомьтесь с видеоматериалами. Обсудите в группе, какие угрозы таит в себе Интернет.

Сайт «Безопасный Интернет для детей»: **http://i-deti.org/**

- Видеоролик «Угрозы Интернета для детей»: **http://i-deti.org/video/**
- Видеоролик «Мировой опыт защиты детей в Интернете»: **http://i-deti.org/video/**

4. _____
5. _____
6. _____
7. _____
8. _____

1.2. Что такое Всемирная паутина

Всемирная паутина — это Сеть с информацией, которая размещена на разных компьютерах. Информация имеет адрес (имя), по которому её можно отыскать в Сети. Она передаётся в цифровых кодах, а смотреть и читать на компьютерах и устройствах, подключённых к Сети, её можно в привычном нам виде.

Эта информация представлена во Всемирной паутине в виде веб-сайтов. Веб-сайты можно сравнить с книгами, а веб-страницы — со страницами этих книг. Но в отличие от бумажных страниц обычных печатных книг, информация на которых не меняется, веб-страницы могут изменяться, включая видео- и аудиовставки, а также ссылки — слова или картинки, по которым переходят на другие веб-сайты или веб-страницы.

Книгу нужно листать по страницам, чтобы переходить к новой информации в ней, а веб-сайты позволяют путешествовать по Всемирной паутине, переходя по ссылкам от сайта к сайту.

На веб-сайтах размещаются новости, рисунки, анимация, фильмы, звукозаписи, различные формы общения (чаты, форумы, видеоконференции). Эти страницы могут открываться на любых компьютерах, но хранятся они на определённых компьютерах, которые находятся в разных частях света. При выходе на веб-сайт не важно, насколько далеко расположен он от вас, поскольку в Интернете отсутствуют ограничения расстояний.

Чтобы работать с веб-сайтами на компьютере или в устройстве, должна быть установлена специальная программа для просмотра веб-страниц, которая называется **браузер** (проводник). Именно она ведёт нас от сайта к сайту по ссылкам или по именам веб-сайтов.

3. Что лежит в основе веб-документа?
   а) Текст.
   б) Изображение.
   в) Гипертекст.
4. Что может быть гипертекстом?
   а) Текст.
   б) Изображение.
   в) И текст, и изображение.
5. Какой текст называется гипертекстом?
   а) Электронный текст с гиперссылками в нём.
   б) Текст в печатной книге, где есть ссылки.
   в) Текстовый файл.

1.3. Путешествие по сети Интернет: сайты и электронные сервисы

Каждый пользователь Интернета:

- путешествует по сайтам с помощью программы-браузера, открывает для себя новые сайты;
- ищет нужную информацию во Всемирной паутине с помощью популярных информационно-поисковых систем (например, Яндекса);
- использует электронную почту, получает и передаёт информацию;
- находит и скачивает на свой компьютер программы, книги или музыку;
- общается в чатах, на форумах, в социальных сетях;
- учится с помощью электронных курсов и т. д.

Даже в знакомом месте можно заблудиться. А что будет, если мы отправимся «бродить», ссылка за ссылкой, в Интернете?

Сайтов в Сети множество. С одной стороны, путешествовать по Интернету и случайным образом просматривать встретившуюся на пути информацию на первых порах довольно интересно, но это занимает много времени и не всегда приносит пользу.

Для поиска нужной информации в Интернете существуют специальные программы, они называются поисковыми машинами. Но необходимо знать, как с этими программами работать, как строить запрос на поиск, как его уточнить, чтобы не просматривать

Браузер или антивирусная программа может выявить негативную информацию, поэтому при выборе сайта из списка ссылок в ответ на запрос вы получите сообщение об угрозе.

Рис. 3. Сообщение об угрозе на сайте

Общение людей — **социальные коммуникации** расширились с распространением мобильных телефонов, смартфонов и специальных программ-приложений к ним. Для всех мобильных устройств работает программа-приложение — служба мгновенных сообщений, сокращённо СМС. Это приложение объединяет всех пользователей мобильных телефонов и позволяет им мгновенно передавать сообщения.

Так, используя службу мгновенных сообщений, МЧС России информирует граждан о предстоящих изменениях погоды, в том числе опасных (метель, ураганный ветер, град и т. д.).

Огромной популярностью пользуются в настоящее время **социальные сети**, предназначенные для сетевого общения на специальных сайтах.

Социальная сеть позволяет людям из разных уголков мира мгновенно связываться и общаться друг с другом, например, в группах, объединённых общими интересами.

Тест 3. Выберите правильные ответы.

1. Что нельзя делать в Интернете?
   а) Бессистемно путешествовать по сайтам, тратить на это всё свободное время.
   б) Использовать электронную почту, получать и передавать информацию.
   в) Искать нужную информацию во Всемирной паутине с помощью информационно-поисковых систем (например, Яндекса).
   г) Находить и скачивать на свой компьютер программы, книги или музыку с пиратских сайтов.
   д) Некультурно общаться в чате, на форуме, в социальной сети, распространять негативную и ложную информацию.
2. Для поиска нужной информации в Интернете необходимо следующее.
   а) Случайным образом просматривать встретившуюся в Сети информацию.
   б) Использовать специальные сервисы, они называются «поисковые машины» или «поисковые системы».
   в) Анализировать полученную на электронную почту информацию, прежде чем отвечать.
3. Какие сервисы в сети Интернет предназначены для коммуникации (общения)?
   а) Службы мгновенных сообщений (мессенджеры).
   б) Социальные сети.
   в) Поисковые машины.
4. Что можно сказать о грамотном пользователе сети Интернет?
   а) Занимается распространением ложной, агрессивной, грубой, негативной информации.
   б) Вежливый собеседник, не скрывающий свои намерения, соблюдающий правила информационной безопасности.
   в) Не зависит от Интернета, находит время для творчества, спортивного досуга, живого общения с друзьями и близкими людьми.
   г) Злоумышленник, который похищает личную информацию и пользуется ею в недобрых целях.

1.4. Как стать пользователем Интернета

Выйти в сеть Интернет можно с разных устройств. К ним относятся:

- мобильный телефон;
- планшет;
- компьютер;
- смарт-телевизор.

К Интернету сейчас можно подключиться, используя: домашнюю проводную сеть, спутниковый Интернет или мобильный Интернет, доступ к которому покупают у оператора связи.

Для того чтобы подключить к Сети мобильный телефон или планшет, необходимо иметь SIM-карту с поддержкой мобильного Интернета или же использовать беспроводную сеть «Wi-Fi», находящуюся в свободном доступе или защищённую паролем.

При выборе тарифа для вашей мобильной Сети вы знакомитесь со списком услуг Интернета, которые предоставляются по каждому тарифу, и оплачиваете один из тарифов.

В общественных местах, например в аэропорту, гостинице, образовательной организации, вам может быть предоставлен бесплатный доступ в сеть «Wi-Fi». Но нужно внимательно относиться к незащищённой сети, так как она может быть опасна.

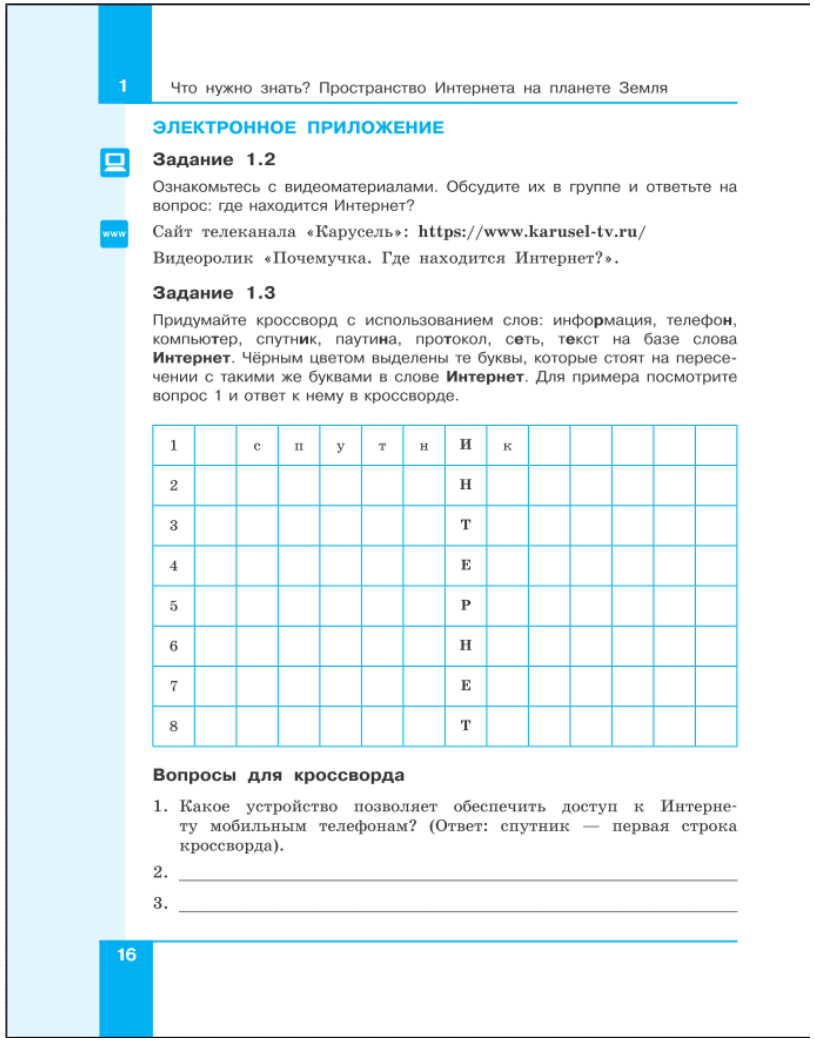
При подключении к «Wi-Fi» нужно зарегистрироваться, так как вы становитесь пользователем этой Сети. При регистрации требуется указать личные данные, например ваш мобильный телефон или электронную почту, на которые придёт код доступа в Интернет. После ввода необходимой информации в ваше устройство произойдёт подключение к Сети.

Ваши данные при регистрации получает провайдер — это организация, которая предоставляет услуги Интернета. Обычно с провайдером заключают договор взрослые люди, например ваши родители, администраторы образовательных и иных организаций.

Важно помнить, что Интернет — это очень мощный инструмент для работы и использовать его надо, соблюдая следующие правила информационной безопасности:

- правила антивирусной защиты своего устройства;
- правила анализа информации и поведения для защиты от мошенников в Интернете;
- правила сетевого этикета и культуры сетевого взаимодействия, защиты от агрессии в Сети;
- правила защиты авторских прав (пиратские сайты);

ЭЛЕКТРОННОЕ ПРИЛОЖЕНИЕ К ПОСОБИЮ БЕЗОПАСНОЕ ПОВЕДЕНИЕ В СЕТИ ИНТЕРНЕТ. 5-6 КЛАССЫ СЕРИИ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ



1 Что нужно знать? Пространство Интернета на планете Земля

ЭЛЕКТРОННОЕ ПРИЛОЖЕНИЕ

Задание 1.2

Ознакомьтесь с видеоматериалами. Обсудите их в группе и ответьте на вопрос: где находится Интернет?

Сайт телеканала «Карусель»: **https://www.karusel-tv.ru/**

Видеоролик «Почемучка. Где находится Интернет?».

Задание 1.3

Придумайте кроссворд с использованием слов: информация, телефон, компьютер, спутник, паутина, протокол, сеть, текст на базе слова **Интернет**. Чёрным цветом выделены те буквы, которые стоят на пересечении с такими же буквами в слове **Интернет**. Для примера посмотрите вопрос 1 и ответ к нему в кроссворде.

1		с	п	у	т	н	**И**	к					
2							**Н**						
3							**Т**						
4							**Е**						
5							**Р**						
6							**Н**						
7							**Е**						
8							**Т**						

Вопросы для кроссворда

1. Какое устройство позволяет обеспечить доступ к Интернету мобильным телефонам? (Ответ: спутник — первая строка кроссворда).
2. _____
3. _____

16

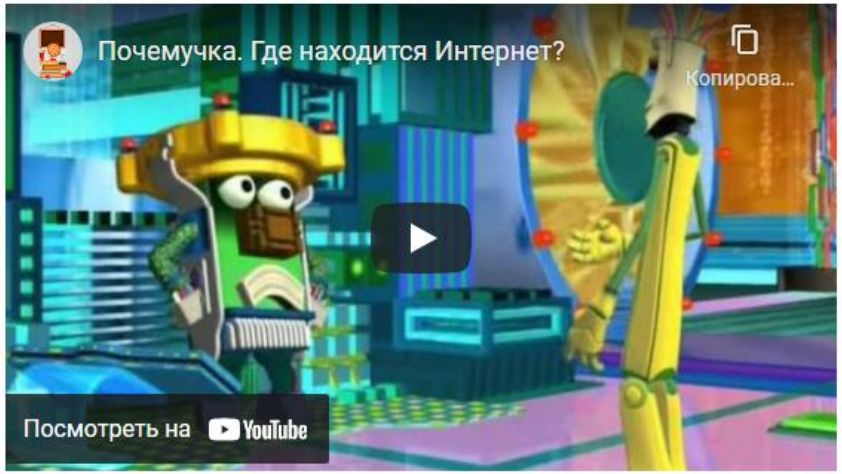
Задание 1.2

Ознакомься с видеоуроком Телеканала Карусель: Почемучка. Где находится Интернет?

Ответь на вопрос: что такое Интернет?

Сайт телеканала «Карусель»: https://www.karusel-tv.ru/

Видеоролик «Почемучка. Где находится Интернет?»



https://lbz.ru/metodist/authors/ib/5-6.php

ОДОБРЕНА
решением федерального учебно-методического объединения по общему образованию
(протокол от 26 октября 2020 № 4/20)

ПРИМЕРНАЯ ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА
УЧЕБНОГО КУРСА
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»
ДЛЯ ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЙ, РЕАЛИЗУЮЩИХ
ПРОГРАММЫ ОСНОВНОГО ОБЩЕГО ОБРАЗОВАНИЯ

Место учебного курса «Информационная безопасность» в учебном плане

Особенностью программы курса является ее поэтапное развитие для разных возрастных групп обучающихся основного общего образования с учетом из возрастных особенностей. Программа курса ориентирована на включение в контекст обучения и воспитания новых видов информационных угроз и средств противодействия им. Программа курса представлена ***двумя разделами по возрастным группам:*** для 5—6 классов и **7—9 классов**.

Реализация программы учебного курса возможна в разных формах:

— как дополнительные модули обучения в интеграции с предметами «Информатика» и (или) «ОБЖ» для двух возрастных групп: 5—6 и **7—9 классов** (от 30 учебных часов для каждой возрастной группы);

— в рамках отдельного учебного курса «Информационная безопасность» для внеурочной деятельности по выбору из объема часов, формируемых самостоятельно образовательной организацией;

— в рамках часов, предусмотренных по программе воспитания (социализации) в образовательной организации для разных уровней общего образования.

СОДЕРЖАНИЕ УЧЕБНОГО КУРСА «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ» ДЛЯ ОСНОВНОГО ОБЩЕГО ОБРАЗОВАНИЯ

Содержание учебного курса «Информационная безопасность» для разных возрастных модулей программы складывается из двух линий:

7 – 9 классы

1) Информационное общество и информационная культура

Модуль 1. Современное информационное пространство и искусственный интеллект

Модуль 2. Современная информационная культура

2) Информационное пространство и правила информационной безопасности

Модуль 3. Угрозы информационной безопасности

ПЛАНИРОВАНИЕ УЧЕБНОГО КУРСА «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ» ДЛЯ ОСНОВНОГО ОБЩЕГО ОБРАЗОВАНИЯ

Программа учебного курса для **7—9 классов** основного общего образования рассчитана на объем не менее 30 часов. Программа курса может быть реализована по выбору образовательной организации как:

- самостоятельный учебный курс во внеурочной деятельности детей **за один год обучения**
- отдельными модулями в программах освоения учебных предметов «Информатика» и (или) «ОБЖ» (в 7—9 классах)
- в рамках школьных мероприятий с участием родителей интегрирована модулями в календарное планирование программы воспитания

Варианты учебного планирования:

Вариант 1. Планирование обучения **за один год обучения**. Один урок в неделю. 30 уроков.

Вариант 2. Планирование обучения по модулям **в 7—9 классах**.

ОДОБРЕНА
решением федерального учебно-методического
объединения по общему образованию
(протокол от 26 октября 2020 № 4/20)

ПРИМЕРНАЯ ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА УЧЕБНОГО ПРЕДМЕТА «ИНФОРМАТИКА» (МОДУЛЬ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ») ДЛЯ ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЙ, РЕАЛИЗУЮЩИХ ОБРАЗОВАТЕЛЬНЫЕ ПРОГРАММЫ ОСНОВНОГО ОБЩЕГО ОБРАЗОВАНИЯ

Место учебного модуля в учебном плане

Программа разработана и может реализовываться на уроках информатики в 7–9 классах общеобразовательной организации по принципу модульной программы. Программа учебного курса рассчитана на 32 учебных часа, из них 18 часов — учебных занятий, 3 часа — проверка знаний, 9 часов — подготовка и защита учебных проектов, 2 часа — повторение. Учебные занятия по программе могут быть реализованы в рамках внеурочной деятельности в различных вариантах:

— в течение одного учебного года в 7, 8 или 9 классах;

— по одной теме последовательно в 7, 8 и 9 классах;

— произвольно распределены учителем в зависимости от интереса и готовности школьников.

ОДОБРЕНА
решением федерального учебно-методического
объединения по общему образованию
(протокол от 26 октября 2020 № 4/20)

ПРИМЕРНАЯ ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА УЧЕБНОГО ПРЕДМЕТА «ИНФОРМАТИКА» (МОДУЛЬ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ») ДЛЯ ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЙ, РЕАЛИЗУЮЩИХ ОБРАЗОВАТЕЛЬНЫЕ ПРОГРАММЫ ОСНОВНОГО ОБЩЕГО ОБРАЗОВАНИЯ

цели

- формирование у обучающихся навыков *информационной культуры*, профилактики негативных тенденций в информационной культуре;
- умение соблюдать *нормы информационной этики и права*; знание о роли информационных технологий и устройств в жизни людей;
- формирование навыка и умения *безопасного и целесообразного поведения* при работе с компьютерными программами и в сети Интернет;
- формирование активной позиции в получении знаний и умений *выявлять информационную угрозу, определять степень её опасности*, предвидеть *последствия информационной угрозы и противостоять им*;
- обеспечение условий для *повышения защищённости детей от информационных рисков и угроз*.

СОДЕРЖАНИЕ МОДУЛЯ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ» УЧЕБНОГО ПРЕДМЕТА «ИНФОРМАТИКА»

Содержание модуля программы соответствует темам ***примерной основной образовательной программы основного общего образования (ПООП ООО) учебного предмета «Информатика»***, а также расширяет их за счёт привлечения жизненного опыта обучающихся в использовании всевозможных технических устройств (персональных компьютеров, планшетов, смартфонов и пр.), позволяет правильно ввести ребёнка в цифровое пространство и корректировать его поведение в виртуальном мире.

Основное содержание модуля Программы представлено разделами:

- «Безопасность общения»
- «Безопасность устройств»»
- «Безопасность информации»

ИНТЕРНЕТ-РЕСУРСЫ О БЕЗОПАСНОМ ИНТЕРНЕТЕ

1. «Азбука Безопасности» - http://azbez.com/safety/internet
2. Портал Российского Оргкомитета по проведению Года Безопасного Интернета - http://www.saferinternet.ru/
3. Сайт посвящен проблеме безопасной, корректной и комфортной работы в Сети. Интернет-угрозы и эффективное противодействие им - http://saferunet.ru/ Центр безопасного Интернета в России.
4. Фонд развития интернета Информация о проектах, конкурсах, конференциях и др. по компьютерной безопасности с безопасности Интернета - www.fid.ru
5. «Основы безопасности детей и молодежи в Интернете» — интерактивный курс по Интернет-безопасности - http://laste.arvutikaitse.ee/rus/html/etusivu.htm
6. «Безопасность детей в интернете». Информация для родителей: памятки, советы, рекомендации - http://www.internet-kontrol.ru/stati/bezopasnost-detey-v-internete.html
7. Образовательно выставочный проект "Дети в Интернете" - http://detionline.com/mts/about
8. 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 - http://interneshka.net/ - «Интернешка».

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. КИБЕРБЕЗОПАСНОСТЬ. 7–9 КЛАССЫ: УЧЕБНОЕ ПОСОБИЕ ЦВЕТКОВА М.С., ХЛОБЫСТОВА И.Ю.

Предназначено для проведения уроков по информационной безопасности в 7–9 классах (информатика, ОБЖ), а также для внеурочной деятельности обучающихся в форме курса по выбору школьников.

Пособие ориентировано на современные тенденции в области безопасной работы в сети Интернет, включая доступные для школьников социокультурные ресурсы, новые средства глобальной медиасреды, цифровые устройства в быту.

Состоит из разделов «Киберпространство», «Киберкультура» и «Киберугрозы» для изучения материала и проведения практических работ в 7, 8 и 9 классах соответственно и раздела «Проверь себя» для итогового контроля.

К пособию на сайте издательства прилагается бесплатное электронное приложение с видеоматериалами в открытом доступе телеканала Наука и ИТ компаний (http://lbz.ru/metodist/authors/ib/7-9.php).

Раздел 1
КИБЕРПРОСТРАНСТВО

1.1. Киберпространство

Термин «киберпространство» в современном смысле означает цифровое открытое пространство, используемое в мире посредством компьютеров и цифровой информации. По мнению французского философа Пьера Леви, *киберпространство* — это пространство обработки информации в электронной форме в режиме реального времени («здесь и сейчас»). Это пространство позволяет получать, передавать, моделировать и фиксировать информацию, создавая электронные среды и управляя различными устройствами.

Первой основной составляющей, породившей киберпространство, является компьютерная сеть Интернет как средство мгновенного и дешёвого подключения к информационному взаимодействию из любой точки мира, передачи, хранения и получения информации. Интернет — глобальная всемирная компьютерная сеть для обмена информацией, сочетающая в себе различные компьютерные сети. Эта сеть уже не имеет географических границ.

Второй составляющей киберпространства являются участники информационного взаимодействия — это люди и машины, которые умеют обрабатывать информацию. На основе единых правил обмена информацией (протокола TCP/IP) Интернет обеспечивает доступ к компьютерам, различным группам людей, информационным ресурсам и электронным услугам, приборам и машинам, электронным хранилищам информации.

Но главной составляющей киберпространства является цифровая информация и компьютерные программы, которые могут нести как созидание новых возможностей, так и разрушение.

Можно с уверенностью сказать, что большая часть совершающихся в киберпространстве операций осуществляются именно на основе информации в сети Интернет.

Киберпространство охватывает весь мир. На основе отчётов о глобальном цифровом рынке **(files.lbz.ru/authors/ib/1-1-1-7-9.pdf)** при населении мира 7,593 миллиардов человек:

- Количество пользователей Интернета в 2018 году достигло 4,021 млрд человек (53% населения мира), что на 7% больше по сравнению с аналогичным периодом прошлого года.
- Аудитория социальных сетей в 2018 году составила 3,196 млрд человек — это плюс 13% к прошлогоднему показателю.
- Мобильными телефонами в 2018 году пользовались 5,135 млрд человек (68% населения мира) — на 4% больше, чем год назад.

отмечают необходимость не только в рамках отдельных государств, но и при международном сотрудничестве создавать системы безопасности в киберпространстве — обеспечивать *кибербезопасность*.

Процессы, протекающие в мире, — террор, войны, экономическая борьба — внедрились и в киберпространство, вводя в лексикон такие термины, как «кибервойна», «кибертерроризм», «кибершпионаж» и т. п. В отличие от традиционных видов вооружения в киберпространстве применяются виды *информационного оружия*, причём и в мирное время. *Кибероружие* может быть использовано не только государством, но и террористами, криминальным миром и отдельными лицами.

Со временем многие государства начали осознавать, что война может идти и в цифровом мире. Этот мир воспринимается и как пространство новой, пятой виртуальной (искусственно созданной человечеством) реальности, кроме освоения человеком реального мира — ресурсов земли, водного и воздушного пространства, космоса.

Киберпространство находится под угрозой противостояний и войн.

Борьба между соперничающими друг с другом странами и организациями уже наблюдается и в интернет-пространстве. Киберпространство как пространство информационных потоков населения планеты несомненно несёт в себе конфликты интересов. Главная задача мирного киберпространства — обезопасить свои информационные потоки и массивы информации в сети Интернет.

Системы защиты от какой-либо возможной угрозы в киберпространстве должны быть постоянно в состоянии готовности к отражению кибератак.

В этом пособии мы выясним, какие угрозы сопровождают нас в киберпространстве и как избежать их разрушительного воздействия.

Кроме того, мы познакомимся с различными достижениями новых кибертехнологий, направленных на развитие творчества и обеспечение удобства жизни людей.

Задания

1. С использованием поисковой системы Яндекс узнайте, что такое протокол обмена данными TCP/IP, что такое «виртуальная реальность».
2. Электронное приложение. Задание 1.1.1. Статья «Интернет 2017–2018 в мире и в России: статистика и тренды».
3. Электронное приложение. Задание 1.1.2. Видеоурок «Наука 2.0. Виртуальная реальность. Большой скачок».
4. Ответьте на вопрос: какие угрозы может нести киберпространство человечеству?

1.2. Кибермиры

Кибермиры — это новые цифровые ресурсы для жизни общества и новые умные технологии для экономики, услуг и производства, отражение практически всех аспектов нашей настоящей реальной жизни в виртуальном (компьютерном) пространстве. Развитие кибермиров должно обеспечивать безопасность для человека.

Киберпространство и кибермиры в нём создаются людьми. В современном реальном компьютеризированном мире развиваются новые технологии искусственного интеллекта — «умные», или *смарт-технологии*. Эти технологии позволяют машинам, компьютерным системам обучаться на основе информации, которую они обрабатывают, и создавать самим новые информационные объекты, вступать во взаимодействие с другими машинами и с людьми, то есть порождать новые кибермиры или вносить в имеющиеся новые возможности. Смарт-технологии сильно изменяют общество, так как в реальной жизни появляются новые отношения между людьми и «умными» машинами, которые нужно учитывать.

Создаваемый человечеством кибермир основан на развитии Интернета. Интернет в настоящее время из глобальной среды связи компьютера с компьютером преобразуется в среду более высокого уровня в киберпространстве: взаимодействие человека с машинами и машин с машинами с использованием Интернета вещей, облачных технологий, дополненной реальности, умными машинами, робототехническими системами и предприятиями, и т. п., что заметно изменяет формы жизни общества.

Кибермир — это естественная среда нормальной деятельности человека, дополненная виртуальными аналогами: киберискусством, киберобразованием, киберофисами, кибербанками, киберполицейскими, кибербиблиотеками, киберпредприятиями, кибермедициной...

Так же как и реальная среда жизни людей, кибермиры наполняют киберпространство и требуют непрестанного контроля за безопасностью жизни людей и государств. Иначе человечество получит вместо средства к развитию цивилизации тупиковый разрушительный ход истории.

Задания

1. С использованием поисковой системы узнайте, что такое киберкостюм, экзоскелет. Объясните, какую пользу может принести кибермир человеку.
2. Электронное приложение. Задание 1.2.1. Видеоурок «Наука 2.0. Экзоскелет».
3. Ответьте на вопрос: где могут использоваться экзоскелеты? (Объясните для разных видов деятельности: медицины, военной сферы, спорта.)

1.3. Киберфизическая система

Киберфизические системы (Cyber-Physical System, CPS) — это системы, состоящие из различных природных объектов, компьютерных и робототехнических систем и устройств, работающих как единое целое. В таких системах обеспечивается чёткая программная координация между вычислительными и физическими ресурсами. Компьютеры осуществляют анализ и управление физическими процессами с использованием обратной связи. Происходящее в физических системах анализируется компьютером, который определяет обратную реакцию в виде управляющей команды устройству, а устройство оказывает влияние на вычисления и наоборот.

Сложность такого взаимодействия говорит о том, что киберфизическая система — это не усложнение существующих автоматизированных систем, которые работают на основе заложенного в них алгоритма действий. Это создание «умных систем», которые встроены в те или иные физические устройства (искусственный интеллект) с использованием мгновенной обратной связи и принятия решений по управлению устройством на основе полученной от него или из окружающего реального мира, в котором действует устройство, информации.

В кибертехнических системах соединяются технические инженерные модели (механические, строительные, электрические, биологические, химические, экономические и др.) и компьютерные модели, которые работают как одно целое.

Можно перечислить ключевые технологии, которые используются в киберфизических системах. Объединённые в единое целое, они меняют существующие отношения между человеком и машиной.

- *Большие данные* и *аналитика* — сбор и всесторонняя оценка данных из разных источников, основа для принятия решений в режиме реального времени.
- *Автономные роботы* — промышленные роботы, которые могут выполнять довольно сложные операции, а системы компьютерного зрения позволяют роботам взаимодействовать друг с другом и автоматически корректировать свои действия. Причём люди смогут находиться рядом с ними, влиять на них, и это вполне безопасно.
- *Компьютерное зрение* (техническое зрение) — теория и технология создания машин, которые могут производить обнаружение, отслеживание и классификацию объектов. Как научная дисциплина компьютерное зрение относится к теории и технологии создания искусственных систем, получающих информацию из изображений. Видеоданные могут быть представлены множеством форм, таких как видеопоследовательность, изображения с различных камер, или трёхмерными данными.
- *Моделирование и симуляторы* — создание моделей реальных объектов и процессов для их исследования, а также для изучения их поведения или поведения человека в смоделированных условиях

Задания

1. С использованием поисковой системы узнайте, что такое «Умный дом», «Умное предприятие».
2. Электронное приложение. Задание 1.3.1. Видеоурок «Наука 2.0. Искусственный интеллект (Большой скачок)».
3. Электронное приложение. Задание 1.3.2. Видеоурок «Управление дронами».
4. Ответьте на вопрос: как используется Интернет вещей? (Объясните для разных видов применения: умный дом, смарт-автомобиль, дрон.)

1.4. Кибероbщество

Кибероbщество — это новая форма общественных отношений людей в цифровом мире. Эти отношения в основном начали формироваться с появлением социальных сетей, где люди взаимодействуют, зачастую не зная, с кем они общаются в действительности.

Особенностью кибероbщества стал тот факт, что каждый пользователь сети Интернет формирует свой образ в соответствии со своими пожеланиями, часто не совпадающими с реальным образом. Человек в Сети изначально анонимен, в социальных сетях эта анонимность фиксируется как его заставка в личной странице — «ник» аккаунта. Сменив реальное имя на ник, человек уже закрывается от своего реального образа. Кроме того, в Сети не нужны характеристики реального человека — внешность, пол, возраст и т. п., что делает невозможным в общении через ник дать характеристику реальной личности. Так в сети каждый её посетитель может творить свой виртуальный образ.

Присоединяясь к кибероbществу, человек получает в Интернете полную свободу в сотворении своего образа, а может быть, и нескольких образов. В социальных сетях общаются реальные люди, скрытые для всех за созданными ими образами. С одной стороны, интересно общаться с неизвестным тебе человеком, а с другой стороны, есть опасность получить в «друзья» совсем не тех людей, за которых они себя выдают в Сети.

Каждая отдельная личность кибероbщества фактически живёт в двух разных мирах: в реальной жизни и информационном пространстве под маской ника.

Реальный социальный мир характеризует каждого человека данными о нём, например: пол, возраст, национальность или гражданство, профессиональная принадлежность, внешность, религиозные убеждения, состояние здоровья, социальный статус, хобби, образование, увлечения и пр. Информационный мир не имеет этих границ, и в нём представить себя в Сети возможно двумя путями:

1) через перенос в киберпространство своего реального образа;
2) через виртуальную реконструкцию своего образа.

Таким образом, Интернет создал совершенно новую среду взаимодействия людей в виде своих вымышленных виртуальных образов, что поменяло и нравственные ориентиры общества — когда анонимность может прийти в киберпространство не с добром, а со злом.

Это зло может передаваться в виде оскорблений, унижения достоинства людей в сети, распространения фальшивой информации о человеке, травли людей с корыстными или хулиганскими намерениями для достижения неблаговидных целей.

Важно знать, что личность в сети Интернет может быть установлена на основе анализа регистрационных данных при вхождении в социальные сети, и лица, негативно ведущие себя в киберпространстве, использующие психологическое воздействие на людей или преступные действия по отношению к человеку, могут привлекаться по закону к ответственности, в том числе и уголовной, влекущей различные по степени тяжести наказания.

Сетевой этикет

В киберпространстве серьёзное влияние на молодых людей оказывают социальные сети, где пользователи постоянно делятся фото- и видеоинформацией, пишут друг другу сообщения, обсуждают те или иные события культурной и общественной жизни, вместе играют и т. д. В такой насыщенной информацией среде молодым людям приходится постоянно отвлекаться, чтобы взаимодействовать друг с другом: отвечать на личные сообщения, комментировать фото и видео. Скорость реакции зачастую очень высока, и в ответах много неточностей, грамматических ошибок, а бывает, и ненормативных слов. Всё это вносит в культуру общения нежелательные привычки, от которых нужно избавляться, так как в дальнейшем они могут сильно навредить человеку в его отношениях с друзьями, а также партнёрами по работе. *Кибероbщество* разработало сетевой этикет, определяющий основные всеобщие нормы сетевой культуры, которые, конечно, нужно соблюдать. Он не отличается от этикета в реальной жизни, основанного на уважении к людям и соблюдении культуры общения и поведения.

Клиповое мышление

Наша цивилизация как кибероbщество уже в повседневной жизни непрерывно и в высоком темпе работает с большими объёмами электронной информации в виде веб-сайтов, почтовых сообщений, зрительных и звуковых фрагментов (клипов), что приводит к снижению внимания, критического осмысленного восприятия информации, характерного для докомпьютерной «книжной» цивилизации. Таким образом, у современного человека растёт фрагментарность в восприятии информации, развивается *«клиповое мышление»* (увидел, ответил, стёр или забыл).

Английское слово clip в переводе на русский имеет следующие значения: отрезок, фрагмент, отрывок (или кадр) из фильма. Считается,

Кибермания

Киберобщество несёт психологические угрозы и самому человеку в нём. Компьютерная или интернет-зависимость — это непреодолимое пристрастие человека к проведению времени за компьютером или в сети Интернет. Интернет-зависимость дополнилась теперь и кибермманией благодаря появлению различных новых устройств, позволяющих не только работать с информацией в Интернете, но и погружаться в виртуальные миры...

Кибермания — это широкий термин, обозначающий большое количество проблем поведения и контроля над влечениями.

Кибермания характеризуется стремлением уйти от повседневности в виртуальные миры. В этот момент человек не только отбрасывает насущные заботы на задний план, но и прекращает индивидуально-личностное развитие, поскольку полностью подчинён виртуальной реальности. Таким образом люди фактически отказываются от своей реальной жизни. Несколько типов такой зависимости в киберобществе, которые были выделены учёными в своих исследованиях, характеризуются следующим образом:

- Пристрастие к виртуальным знакомствам — избыточность знакомых и друзей в Сети, навязчивое стремление постоянно проверять чат или электронную почту.
- Навязчивая потребность присутствия в Сети — игра в онлайновые азартные игры, постоянные покупки или участие в аукционах.
- Информационная перегрузка (бесконтрольный веб-серфинг) — бесконечные путешествия по Сети, поиск информации по базам данных и поисковым сайтам.
- Кибераддикция — навязчивое желание проводить время в компьютерных играх, в том числе в сети Интернет.

Как показывает практика, наибольшую активность в Интернете среди школьников имеют подростки. Они активно осваивают интернет-

Кибергражданe

Учёные считают, что в развитии Интернета и веб-сайтов всемирной паутины как основы киберпростанства нет и никогда не было общего планирования, мы являемся свидетелями настоящей самоорганизации «коллективного разума» — киберобщества. Таким образом, пространство Интернета развивается по всем законам эволюции как живой организм, клетками которого являются люди в сети Интернет, а теперь они дополняются роботами в сети Интернет — умными машинами. Сегодня, когда мы находимся в самом начале стремительно развивающейся эпохи формирования киберпространства, трудно понять, каким же станет это киберпространство через несколько десятилетий.

Все пользователи сети Интернет — это *кибергражданe*, или граждане Интернета, у которых нет географических границ для взаимодействия. Каким будет кибергражданин в глобальном киберобществе?

Следует учитывать, что в сети Интернет могут присутствовать не только реальные люди! Кибергражданами могут выступать виртуальные пользователи, за которыми стоят не люди, а компьютерные программы, обрабатывающие поступающую к ним информацию. *Бот* — это сокращение от слова робот (*интернет-бот*, веб-бот). Программа «бот» выполняет автоматически по заданному алгоритму действия на основе полученной информации в сети Интернет, которую бот собирает и анализирует для конкретных пользователей сети.

Такие боты в системе интернет-торговли уже работают, они активно анализируют чаты, социальные сети и могут предложить конкретным людям — пользователям сети — ту или иную продукцию или услуги, проанализировав информацию этих пользователей. Например, анализ посещений сайтов, поиска конкретной информации позволяет боту сделать вывод о предпочтениях человека и направить на его личную страницу в сети или на электронную почту рекламную рассылку или предложение о товаре или услуге.

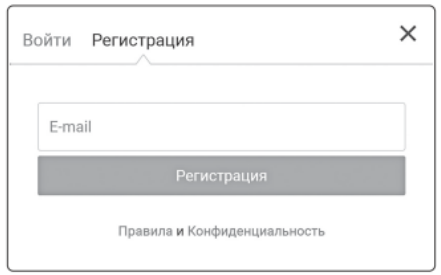
1.7. Практикум к разделу 1

1. Электронное приложение. Задание 1.7.1.

   Практическая работа на основе онлайн-курса Академии Яндекс «Безопасность в Интернете» **(https://academy.yandex.ru/events/online-courses/internet_security/)**.

   Практическую работу рекомендуется выполнять в группах по 2–3 учащихся.

   Используя кнопку «регистрация», перейдите на открытый сайт онлайн-курса **https://stepik.org/course/191/syllabus**. Подтвердите адрес электронной почты, перейдите по ссылке, полученной в письме, и начните обучение.



   Пройдите обучение по теме «Безопасные онлайн-платежи». (Как использовать электронный кошелёк или банковскую карту, чтобы не стать жертвой обмана.)

2. Выполните тест 1 в разделе «Проверь себя».

Раздел 4
ПРОВЕРЬ СЕБЯ

Оцените высказывания или ответьте на вопросы тестов по темам к разделам «Киберпространство», «Киберкультура» и «Киберугрозы». К каждому высказыванию или вопросу можно выбрать только один правильный ответ (Да — 1, Нет — 0). К своему ответу укажите страницу пособия, где имеется описание ответа.

Тест 1. Киберпространство

1.1. Киберпространство

№	Верно ли высказывание?	Да — 1	Нет — 0	Страница
1	Киберпространство — это цифровое открытое пространство, используемое в мире посредством компьютеров и цифровой информации			
2	Киберпространство — это пространство обработки информации в электронной форме в режиме «вчера и сегодня»			
3	Единственной составляющей, породившей киберпространство, является компьютерная сеть Интернет			
4	Участниками киберпространства являются только люди и их информационное взаимодействие			
5	Главной составляющей киберпространства является цифровая информация и компьютерные программы			
6	Большая часть совершающихся в киберпространстве операций осуществляются именно на основе информации в сети Интернет			
7	Основной прирост пользователей сети Интернет приходится на электронную почту			
8	Хакер — это преступник, незаконно использующий свои широкие компьютерные знания во вредительской деятельности			
9	Системы безопасности в киберпространстве называются киберопасностью			
10	В киберпространстве применяются традиционные виды вооружения			

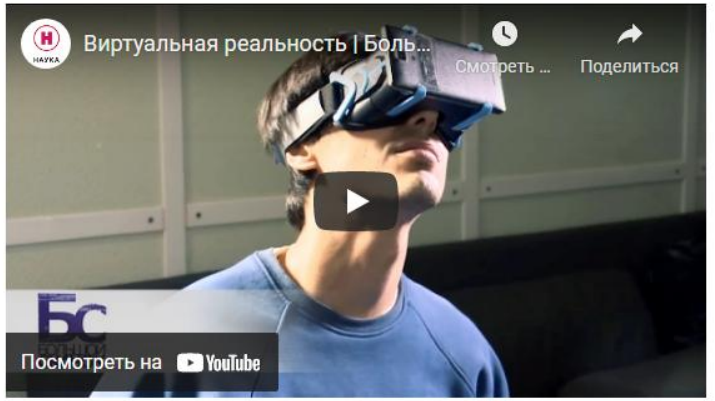
ЭЛЕКТРОННОЕ ПРИЛОЖЕНИЕ К ПОСОБИЮ КИБЕРБЕЗОПАСНОСТЬ. 7-9 КЛАССЫ СЕРИИ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Раздел 1. Киберпространство

1.1 Киберпространство

Задание 1.1.1
Интернет 2017–2018 в мире и в России: статистика и тренды
Читать

Задание 1.1.2
Наука 2.0 Виртуальная реальность. Большой скачок



Задания

1. С использованием поисковой системы Яндекс узнайте, что такое протокол обмена данными TCP/IP, что такое «виртуальная реальность».
2. Электронное приложение. Задание 1.1.1. Статья «Интернет 2017–2018 в мире и в России: статистика и тренды».
3. Электронное приложение. Задание 1.1.2. Видеоурок «Наука 2.0. Виртуальная реальность. Большой скачок».
4. Ответьте на вопрос: какие угрозы может нести киберпространство человечеству?

https://lbz.ru/metodist/authors/ib/7-9.php

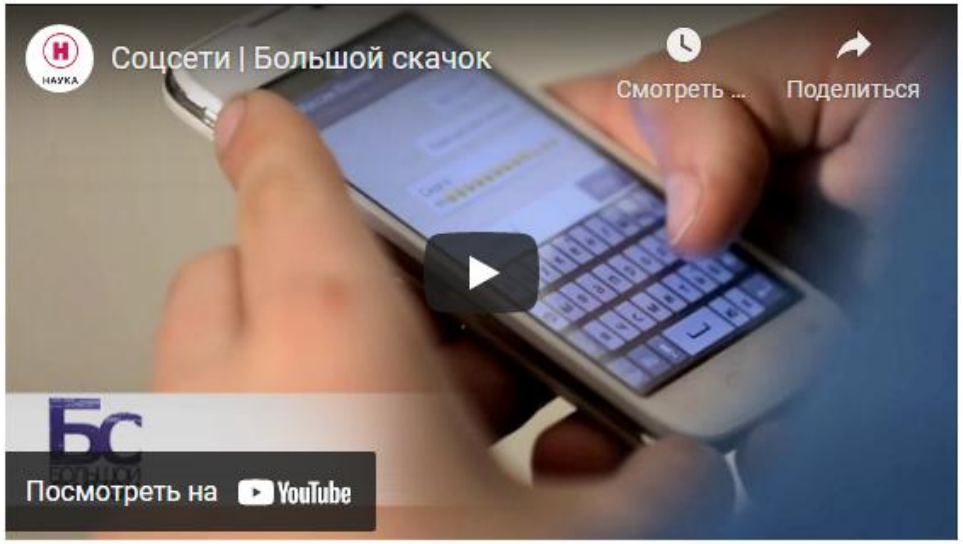
ЭЛЕКТРОННОЕ ПРИЛОЖЕНИЕ К ПОСОБИЮ КИБЕРБЕЗОПАСНОСТЬ. 7-9 КЛАССЫ СЕРИИ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

1.4 Киберобщество

Задание 1.4.1
Наука 2.0 Соцсети. Большой скачок

Задания

1. С помощью поисковой системы Яндекс найдите объяснение понятию «кибербуллинг». Объясните следующие действия для противостояния этому явлению:
   - знать, что все люди ответственны за то, что они смотрят, что они делают, что они публикуют в Интернете. За негативное вмешательство в личную сферу граждан следует ответственность по закону;
   - сохранить обращения как свидетельства действий правонарушителя;
   - представить доказательства при обращении в правоохранительные органы.
2. Электронное приложение. Задание 1.4.1. Видеоурок «Наука 2.0. Соцсети. Большой скачок».
3. Электронное приложение. Задание 1.4.2. Видеоурок «Киберстандарт.РФ: “Территория БезОпасности”».
4. Ответьте на вопрос: какие угрозы для личности есть в киберобществе?



https://lbz.ru/metodist/authors/ib/7-9.php

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. КИБЕРБЕЗОПАСНОСТЬ. 10–11 КЛАССЫ: УЧЕБНОЕ ПОСОБИЕ ЦВЕТКОВА М.С., ГОЛУБЧИКОВ С.В., НОВИКОВ В.К., СЕМИБРАТОВ А.М., ЯКУШИНА Е.В.

Практическое пособие предназначено для изучения основ правовой грамотности и норм ответственности несовершеннолетних за правонарушения в сфере информационной безопасности.

Пособие включает практические работы по уровням «знать» и «применять», а также набор проектных заданий для выполнения в группах учащихся на компьютерах.

К пособию на сайте издательства прилагается бесплатное электронное приложение с видеоматериалами в открытом доступе телеканала Наука и ИТ компаний (http://lbz.ru/metodist/authors/ib/10-11.php).

Глава 1

ПОНЯТИЕ ЮРИДИЧЕСКОЙ ОТВЕТСТВЕННОСТИ ЗА ПРАВОНАРУШЕНИЯ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. Практическая работа «Знать»

Документы в области информационной безопасности

1.1.1. Основные документы в области информационной безопасности Российской Федерации

Вопросы информационной безопасности Российской Федерации регулируются документами:

- Указ Президента РФ от 9 мая 2017 года № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы»;
- Указ Президента РФ от 5 декабря 2016 года № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»;
- Распоряжение Правительства РФ от 2 декабря 2015 года № 2471-р «Об утверждении концепции информационной безопасности детей»;
- Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

В сфере информационной безопасности планируется сформировать информационное пространство для реализации творческих возможностей, доступности историко-культурного наследия, социализации молодёжи, а также обеспечить снижение уровня противоправного и преступного поведения среди детей и формирование у детей уважительного отношения к интеллектуальной собственности и авторскому праву, сознательный отказ от использования «пиратского» контента.

Контрольные вопросы

1. Что понимается в Доктрине информационной безопасности
   – под информационной сферой?
   – под информационной структурой Российской Федерации?
   – под информационной безопасностью?
2. Что понимается в Стратегии развития информационного общества
   – под цифровой экономикой?
   – под экосистемой цифровой экономики?

1.2.2. Функции, принципы и виды юридической ответственности

Цели юридической ответственности находят своё отражение и конкретизируются в её функциях (рис. 1.1), к которым можно отнести: карательную, штрафную, превентивную (предупредительную), воспитательную, правовосстановительную (компенсационную), организующую (регулятивную).

Рис. 1.1. Функции юридической ответственности

…ают как реакция обще-
…правонарушителем. Это
…что иное, как средство
…го существования. Дан-
…ия юридического стату-
…обод, либо возложением

Рис. 1.2. Виды правонарушений, юридической ответственности и наказаний

3. Объясните основные понятия, которые используются в Стратегии развития информационного общества в РФ.
4. Ознакомьтесь с документами и подготовьте презентацию по выбору:
   1) «Принципы обеспечения информационной безопасности детей» (по материалам Концепции информационной безопасности детей).
   2) «Основные информационные угрозы» (по материалам Доктрины информационной безопасности Российской Федерации).
   3) «Россия в современном информационном обществе» (по материалам Стратегии развития информационного общества в Российской Федерации).

1.1.2. Информация как объект правовых отношений

Ознакомьтесь со статьями Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Контрольные вопросы

1. Объясните, что понимается:
   – под информацией как объектом правовых отношений (ст. 5–9).
   – под распространением информации (ст. 10, 10.1–10.5).
   – под защитой информации и ответственностью за правонарушения (ст. 16–17).

1.2. Практическая работа «Знать»

Понятие «юридическая ответственность»

Важным направлением любой деятельности, в том числе в области информационной безопасности (защиты информации), является установление ответственности за совершённые правонарушения в этой области. Ответственность представляет собой сложное и многоплановое социальное явление, а также личную обязанность гражданина отвечать за поступки и действия, за их последствия.

Ответственность — это определённый уровень негативных последствий для человека в случае нарушения им установленных государством обязательных требований и норм в нормативных правовых актах (в том числе в области информационной безопасности):

- Конституции Российской Федерации;
- федеральных конституционных законах;
- федеральных законах;
- указах Президента Российской Федерации;

- постановлениях Правительства Российской Федерации;
- приказах федеральных органов государственной власти, зарегистрированных в Минюсте России.

Правовые нормы ответственности в области информационной безопасности установлены в Российской Федерации на основе федеральных законов:

- Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 30 ноября 1994 года № 51-ФЗ «Гражданский кодекс Российской Федерации» (ГК РФ);
- Федеральный закон от 30 декабря 2001 года № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях» (КоАП РФ);
- Федеральный закон от 13 июня 1996 года № 63-ФЗ «Уголовный кодекс Российской Федерации» (УК РФ) и Федеральный закон от 18 декабря 2001 года № 174-ФЗ «Уголовно-процессуальный кодекс Российской Федерации» (УПК РФ).

Контрольные вопросы

1. Что такое ответственность?
2. Какие нормы ответственности установлены в ФЗ № 436 «О защите детей от информации, причиняющей вред их здоровью и развитию»?

1.2.1. Юридическая ответственность

Юридическая ответственность — правоотношение, в которое вступает с одной стороны государство в лице его компетентных органов и должностных лиц, а с другой стороны — правонарушитель (лицо), на которого возлагается обязанность отвечать за совершённое им правонарушение.

Основанием юридической ответственности является наличие правонарушения. Юридическая ответственность, являясь одним из видов ответственности, выступает важной мерой защиты интересов личности, государства и общества.

Юридическая ответственность наступает в результате нарушения запретов и предписаний, установленных государством в нормативных правовых актах в виде обязательных требований (норм), и проявляется в применении к правонарушителям мер государственного принуждения (санкций).

Право применять меры принуждения предоставлено только государственным органам (федеральным, субъектов Российской Федерации и муниципальным) и должностным лицам в пределах их полномочий.

Тест 1

Выберите один вариант ответа для каждого вопроса.

№	Вопрос	Варианты ответов	Ответ
А.	***Поставьте в соответствие приведённые определения и понятия юридической ответственности.***		
1	Противоправное деяние, представляющее такую форму поведения субъекта права, которое посягает на общественные отношения, охраняемые государством	1 — проступок 2 — преступление 3 — наказание	
2	Форма противоправного поведения субъекта права, причиняющая вред обществу		
3	Средство самозащиты общества от нарушения условий его существования		
Б.	***Поставьте в соответствие приведённые определения и принципы юридической ответственности.***		
4	Обязанность лица (человека), совершившего правонарушение, претерпевать определённые лишения (ограничения) государственно-властного характера, предусмотренные нормами права	1 — юридическая ответственность 2 — презумпция невиновности 3 — равенство перед законом	
5	Лица (граждане), совершившие правонарушения, равны перед законом и подлежат ответственности независимо от пола, расы, национальности, языка, происхождения, имущественного и должностного положения, места жительства, отношения к религии, убеждений, принадлежности к общественным объединениям, а также других обстоятельств		
6	Лицо подлежит юридической ответственности только за те правонарушения, в отношении которых установлена его вина		

№	Вопрос	Варианты ответов	Ответ
В.	***Поставьте в соответствие приведённые определения и формы виновности.***		
7	Лицо, совершившее правонарушение, сознавало противоправный характер своего деяния, предвидело и желало наступления его последствий или сознательно допускало их	1 — небрежность 2 — неосторожность 3 — умысел	
8	Субъект правонарушения предвидел наступление противоправных последствий своего деяния, но вследствие легкомыслия надеялся их предотвратить		
9	Субъект правонарушения не предвидел наступления противоправных последствий своего деяния, хотя должен был и мог их предвидеть		

2.2. Практическая работа «Применять»

Гражданско-правовая ответственность несовершеннолетних за проступки в области информационной безопасности (защиты информации)

За нарушение обязательных требований в области информационной безопасности (защиты информации) возможно привлечение к гражданско-правовой ответственности. При этом меры гражданско-правовой ответственности предусмотрены в общем виде в законодательстве в области защиты информации и в Гражданском кодексе Российской Федерации.

В соответствии с ч. 2 ст. 17 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» лица, права и законные интересы которых были нарушены в связи с разглашением информации ограниченного доступа или иным неправомерным использованием такой информации, вправе обратиться в установленном порядке за судебной защитой своих прав, в том числе с исками *о возмещении убытков, компенсации морального вреда, защите чести, достоинства и деловой репутации*.

При этом требование о возмещении убытков не может быть удовлетворено в случае предъявления его лицом, не принимавшим мер по соблюдению конфиденциальности информации.

Согласно ч. 3 ст. 17 вышеприведённого Федерального закона, в случае если распространение определённой информации ограничивается или запрещается федеральными законами, гражданско-правовую ответственность за распространение такой информации не несёт лицо, оказывающее услуги:

- *по передаче информации*, предоставленной другим лицом, при условии её передачи без изменений и исправлений;
- *по хранению информации* и обеспечению доступа к ней при условии, что это лицо не могло знать о незаконности распространения информации.

2.2.1. Ответственность за проступок в области присвоения авторства (плагиат)

Плагиат относится к категории правонарушений и представляет собой особую форму нарушения интеллектуальных прав, суть которого состоит в присвоении авторства на чужое произведение литературы, искусства или науки.

Последствие нарушения любого субъективного гражданского права, в том числе права авторства, заключается в возможности применения к нарушителю мер гражданско-правовой ответственности, а также уголовной и административной ответственности.

Чаще всего плагиат находит своё выражение в присвоении авторства на чужие результаты интеллектуального труда путём публикации их под своим именем. Плагиат возможен и в частичном использовании чужого произведения или цитировании без ссылки на источник. Плагиатом также могут быть признаны неправомерные действия по принуждению к соавторству.

Для плагиата необязательно опубликование созданного произведения, достаточно нахождение его в какой-либо объективной форме, например в виде рукописи или в составе другого произведения. Главный

2.2.2. Ответственность за проступок — оскорбление, в том числе в социальных сетях

Свободный доступ к Всемирной сети и возможность общения с любыми пользователями Интернета зачастую сопровождаются свободой выражений, моральные рамки которых ограничиваются особенностями воспитания.

Порой пользователь Сети сталкивается с такой проблемой, как оскорбления в свой адрес, размещённые другими лицами.

Наказание за оскорбление в Интернете станет возможным только при наличии следующих аспектов:

- имеет место унижение чести и достоинства человека;
- запись содержит не принятые к использованию в обществе слова и выражения.

Подобные действия наказуемы в соответствии с нормами права.

В соответствии с п. 1 ст. 23 Конституции РФ каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени.

Согласно п. 4 ст. 29 Конституции РФ, каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом.

ЭЛЕКТРОННОЕ ПРИЛОЖЕНИЕ К ПОСОБИЮ ПРАВОВЫЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. 10-11 КЛАССЫ

Материалы к пособию

Учебно-тематическое планирование по курсу «Правовые основы информационной безопасности» 10-11 классы

Глава 1

Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
http://www.consultant.ru/document/cons_doc_LAW_61798/

Указ Президента Российской Федерации №203/2017 г. «О стратегии развития информационного общества в Российской Федерации до 2030 года»

Указ №646/2016 г. «Об утверждении Доктрины информационной безопасности Российской Федерации»

Распоряжение Правительства Российской Федерации от 2 декабря 2015 г. № 2471-р «Концепция информационной безопасности детей»

ДОКУМЕНТЫ, РЕГУЛИРУЮЩИЕ РАЗВИТИЕ ИНФОРМАЦИОННОГО ОБЩЕСТВА В РОССИИ

Конституция Российской Федерации
http://www.constitution.ru/

Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29.12.2010 N 436-ФЗ (ред. от 01.05.2019) https://fzrf.su/zakon/o-zashchite-detej-ot-informacii-436-fz/

Курсы Цифровая грамотность

Глава 2

Федеральный закон от 30 ноября 1994 года № 51-ФЗ «Гражданский кодекс Российской Федерации (ГК РФ).
http://www.consultant.ru/document/cons_doc_LAW_5142/

Глава 3

Федеральный закон от 30 декабря 2001 года № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях» (КоАП РФ)
http://www.consultant.ru/document/cons_doc_LAW_34661/

Изменения КоАП 2021 года

Глава 4

Федеральный закон от 13 июня 1996 года № 63-ФЗ «Уголовный кодекс Российской Федерации» (УГ РФ)
http://www.consultant.ru/document/cons_doc_LAW_10699/

https://lbz.ru/metodist/authors/ib/10-11.php

ЭЛЕКТРОННОЕ ПРИЛОЖЕНИЕ К ПОСОБИЮ ПРАВОВЫЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. 10-11 КЛАССЫ

2. Лицензионное соглашение свободного ПО Линукс

Задание 2.1

Ознакомься со статьей

Лицензирование *на сайте* ***Виртуальная энциклопедия Linux по-русски***

Читать

Задание 2.3

Ознакомься со статьей ***Лицензирование***

Ознакомься с лицензионным соглашением свободного ПО Линукс

Читать

https://lbz.ru/metodist/authors/ib/10-11.php

ЭЛЕКТРОННОЕ ПРИЛОЖЕНИЕ К ПОСОБИЮ ПРАВОВЫЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. 10-11 КЛАССЫ

https://lbz.ru/metodist/authors/ib/10-11.php

9. Личный контент в облаке и система его защиты

Задание 9.1

Ознакомься со статьей

Облачные угрозы: эксперты рассказывают о защите данных в облачных сервисах *на сайте* ***Securenews***

Читать

10. Онлайн-курс Основы информационной безопасности

Задание 10.1

Ознакомься с бесплатным курсом

Основы информационной безопасности *на сайте* ***НОУ ИНТУИТ***

1. Для участия в курсе необходимо зарегистрироваться:
Перейди по ссылке
2. Изучи 15 лекций курса , после каждой лекции пройти тест.
3. Проверь себя – сдай экзамен
4. Получи сертификат

ОДОБРЕНА
решением федерального учебно-методического объединения по общему образованию
(протокол от 26 октября 2020 № 4/20)

ПРИМЕРНАЯ ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА

УЧЕБНОГО КУРСА

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

ДЛЯ ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЙ, РЕАЛИЗУЮЩИХ

ПРОГРАММЫ СРЕДНЕГО (ПОЛНОГО) ОБЩЕГО ОБРАЗОВАНИЯ

Место учебного курса «Информационная безопасность» в учебном плане

Особенностью программы курса является ее включение в контекст не только обучения, но и воспитания в условиях быстро нарастающих новых видов информационных угроз и развития средств противодействия им, отраженных в законодательстве Российской Федерации.

Реализация программы учебного курса возможна в разных формах:

— в интеграции с предметами «Обществознание» и «Информатика» (раздел «Социальная информатика») для 10—11 классов (от 30 учебных часов);

— в рамках отдельного учебного курса «Информационная безопасность» для внеурочной деятельности по выбору из объема часов, формируемых самостоятельно образовательной организацией;

— в рамках часов, предусмотренных по программе воспитания (социализации) в образовательной организации общего образования.

Программа учебного курса поддерживается электронными ресурсами на основе документальных фильмов, анимационных ресурсов и электронных практикумов в открытом доступе от ИТ-компаний Российской Федерации в рамках их участия в проектах по информационной безопасности для детей. В основе курса лежат технические, этические и правовые нормы соблюдения информационной безопасности, установленные контролирующими и правоохранительными органами, а также практические рекомендации ведущих ИТ-компаний и операторов мобильной связи Российской Федерации.

СОДЕРЖАНИЕ УЧЕБНОГО КУРСА «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ» ДЛЯ СРЕДНЕГО (ПОЛНОГО) ОБЩЕГО ОБРАЗОВАНИЯ

Содержание учебного курса «Информационная безопасность» программы складывается из двух линий:

1) Информационное общество и информационная культура.

Модуль 1. Правовые основы информационной безопасности.

Модуль 2. Профилактика правонарушений в сфере информационной безопасности.

2) Информационное пространство и правила информационной безопасности

Модуль 3. Практика применения правил и норм информационной безопасности.

ПЛАНИРОВАНИЕ УЧЕБНОГО КУРСА «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ» ДЛЯ СРЕДНЕГО (ПОЛНОГО) ОБЩЕГО ОБРАЗОВАНИЯ

Программа учебного курса для 10—11 классов среднего общего образования рассчитана на объем ***не менее 30 часов***. Программа курса может быть реализована по выбору образовательной организации как:

- самостоятельный учебный курс во внеурочной деятельности за один год обучения
- отдельными модулями в программах освоения учебных предметов «Информатика» и (или) «Обществознание»
- в рамках школьных мероприятий с участием родителей
- интегрирована модулями в календарное планирование программы воспитания.

Программу курса можно реализовать в дистанционной форме.

Варианты учебного планирования:

Вариант 1. Планирование обучения за один год обучения. Один урок в неделю. 30 уроков.

Вариант 2. Планирование обучения по модулям в 10—11 классах.

ПРОФИЛАКТИКА ИНТЕРНЕТ-УГРОЗ

Если у тебя возникли вопросы или проблемы при работе в онлайн-среде,
обязательно расскажи об этом кому-нибудь, кому ты доверяешь. Твои родители или другие взрослые могут помочь или дать хороший совет о том, что тебе делать. Любую проблему можно решить!
Ты можешь обратиться на линию помощи «Дети онлайн» по телефону: **88002500015** (по России звонок бесплатный) или по e-mail: helpline@detionline.org

Специалисты посоветуют тебе, как поступить

АКТИВНОЕ ОБЩЕНИЕ В СЕТЯХ, ЧАТАХ

Проба навыков межличностного общения, подготовка к реальным контактам в социуме

Но! -

Подмена реального общения виртуальным

Быстрое раздражение, вспышки гнева, желание кричать, швырять вещи, ощущение скуки, отсутствие интереса ко всему

Привлекает анонимность в интернет-среде – образ тролля, буллинг и т.д.

«Неважно, какие игрушки мы дарим детям, воспитываем их всё равно мы, а не гаджеты и телевизор»

ПРАВИЛЬНОЕ ИСПОЛЬЗОВАНИЕ

телефон, планшет – покупают родственники

!!! под контролем родителей

разумное использование цифровых технологий - мощный инструмент развития речи, социальных навыков, эмоционального восприятия окружающего мира – активное исследование, принятие решений, применений знаний

Рано нельзя! – с подготовительной группы, младшего школьного возраста, иначе:

- задержка социального развития (препятствие развития эмпатии, навыков социальной коммуникации)
- препятствие развитию мелкой моторики, письма
- задержка эмоционального развития: гаджет приравнивается к игрушке, к чему-то очень привлекательному, он становится объектом манипуляций (не позволяют научиться контролировать свои эмоции – сунуть гаджет в руки, лишь бы успокоился)

Профилактика Интернет-зависимости

- оговаривать условия пользования (базовые требования) – что можно, что нельзя: правильное поведение в цифровом мире
- оговаривать время, продолжительность пользования (гигиенические нормы: 20 минут в день дошкольники; 30-40 минут в день младшие школьники; час и более старшие школьники, но не каждый день)
- проявлять интерес к тому, чем занят ребёнок, заниматься ВМЕСТЕ с ребёнком – объяснять, показывать
- если есть проблемы в жизни – может появиться «неправильное» поведение в сети
- личный пример: «воспитывайте себя»
- гигиенические нормы и требовательность их соблюдения: до 12 лет дети склонны слушаться

Профилактика Интернет-зависимости

- разумная стратегия контроля (время: сколько и когда, компьютер должен находиться в ОБЩЕЙ зоне, мотивированность требований, поддержка диалога с ребёнком)
- «живые» люди - чаще приглашать гостей, ходить в гости самим, собираться компаниями – живое общение
- «живые» интересы - совместные развлечения, прогулки, кино, театры, мастер-классы и т.п.
- нехватка внимания и ласки – окружить вниманием, обнимать (не менее 8 раз в день), разговаривать – диалог, проявлять интерес к жизни ребёнка: что интересного/нового в школе? во что играли? семейное чтение и обсуждение!!!

СПАСИБО ЗА ВНИМАНИЕ!

Информационный центр
ГАУ ДПО ЯО «ИРО»
Телефон: 8(4852) 23-09-57
E-mail: baranova@iro.yar.ru