



СПРАВОЧНАЯ ИНФОРМАЦИЯ К СЦЕНАРИЮ ЗАНЯТИЯ | 5 КЛАСС

БЕЗОПАСНОСТЬ В СЕТИ ИНТЕРНЕТ

жизнь

гражданственность

СПРАВОЧНАЯ ИНФОРМАЦИЯ К СЦЕНАРИЮ ЗАНЯТИЯ «РАЗГОВОРЫ О ВАЖНОМ»

Занятие 6

«Безопасность в сети Интернет»

Интернет: возможности и риски

Жизнь современного человека трудно представить без цифровых сервисов и приложений. Онлайн-среда связана не только с массой полезных возможностей, но и с рисками для безопасности пользователя. Поэтому так важно развивать собственную цифровую грамотность, знать о возможных рисках и владеть разными методами защиты, в том числе и технологическими. Сфера кибербезопасности активно развивается — это ещё и перспективное направление для профессионального развития¹.

Чем больше времени человек проводит в сети, тем выше риски: от банальной утечки данных до реальных сроков лишения свободы за участие в преступных схемах. Многие по ошибке или невнимательности становятся соучастниками цифровых преступлений. Лучший способ защиты от злоумышленников — знать о существующих рисках и сознательно их избегать.

Цифровой мир похож на реальный: как в реальном мире есть преступники и мошенники, так и в цифровом следует быть аккуратным и не доверять абсолютно всем. Незнакомого человека не пускают в дом и не рассказывают ему свои секреты — значит, и в интернете нельзя думать, что опасность не грозит.

Личная ответственность в цифровой среде — это осознанная забота о себе, которая становится вкладом в безопасность общества и государства².

Основные понятия

Кибербезопасность — совокупность правил и практик защиты от атак злоумышленников в цифровом пространстве.

Аккаунт (учётная запись) — опознавательная информация о пользователе, которая указывается при регистрации на сервисах и сайтах.

Профиль — расширенная совокупность личной, финансовой и другой информации пользователя.

Социальная инженерия — разные виды манипуляций и обмана, цель которых — заставить человека раскрыть личные данные, получить доступ к его личной и финансовой информации.

¹ Из УМК 2022/2023 учебного года (Кибербезопасность).

² Из УМК 2025/2026 учебного года (Цифровой щит. Основные правила безопасности в сети Интернет).

Овершеринг (буквально «чрезмерно много делиться») — избыточное размещение информации личного характера о себе или других людях в общедоступных источниках, в частности в социальных сетях. О явлении широко заговорили ещё в 2013 году³.

Фишинг (англ. phishing, от fishing — рыбная ловля, выуживание) — вид интернет-мошенничества, с помощью которого злоумышленники получают доступ к конфиденциальным данным пользователей (реквизиты банковских карт, логины и пароли), обманом предлагают загрузить вредоносные программы или продают несуществующие услуги. Мошенники буквально стараются «выудить» информацию у пользователя.

Фишинговые сайты — поддельные сайты банков, социальных сетей, маркетплейсов, госорганов. Интерфейсом они похожи на оригиналы, однако у них искажённое доменное имя.

Дропперы (дропы) (от англ. drop — бросать, уронить) — люди, задействованные в нелегальных схемах по выводу средств через свои счета и карты. Нередко человек становится дроппером, даже не подозревая об этом, что не освобождает его от ответственности.

Кардинг — вид мошенничества с использованием платёжной карты или её реквизитов.

Кибербуллинг — систематическая травля в сети.

Сваттинг (от англ. SWAT — спецназ) — заведомо ложное сообщение об угрозе преступления или о происшествии, чтобы направить сотрудников экстренных служб по ложному адресу.

Доксинг (от сокр. docs — документы) — сбор и распространение личной информации о человеке без его согласия, часто с целью шантажа, мести или травли.

Сим-бокс — устройство, объединяющее десятки сим-карт с удалённым доступом, с которых дистанционно совершаются звонки и рассылаются сообщения. Если одну карту блокируют, устройство переключается на другую.

Цифровая гигиена — навыки, которые помогают защитить личные данные, не попадаться на уловки мошенников и сохранять спокойствие в сети⁴.

Фейк — действие или заявление, направленное на введение в заблуждение; манипуляция, основанная на эмоциональном воздействии на человека.

Дипфейк — фотографии, видеоролики или аудиозаписи, созданные с помощью искусственного интеллекта. Современные технологии позволяют делать дипфейки даже из нескольких фотографий, в том числе с мобильного устройства; подделывать можно не только лицо, но и голос.

Фактчекинг — дословно «проверка фактов».

Фактоид — сомнительная информация, принимаемая за правду.

³ Из УМК 2022/2023 учебного года (Кибербезопасность).

⁴ Из УМК 2025/2026 учебного года (Цифровой щит. Основные правила безопасности в сети Интернет).

Медиаграмотность — способность получать, анализировать, оценивать и передавать сообщения в разных формах.

Критическое мышление — способность ставить информацию под сомнение, смотреть на проблему с разных сторон и делать обоснованные выводы⁵.

Цифровой след

Цифровой след — необратимая совокупность данных. Любое действие человека в интернете остаётся навсегда. Информация, размещённая в сети, становится общедоступной и может быть использована злоумышленниками либо обращена против самого пользователя.

Вымышленные имена и картинки вместо фотографий не дают полной анонимности. Удалённые переписки восстанавливают эксперты, человека находят по камерам и геолокации телефона. Цифровой мир — часть единого правового поля государства: противоправные действия в сети не анонимны и преследуются по закону. Цифровой след всегда приведёт к тому, кто его оставил, а незнание закона не освобождает от ответственности⁶.

Что нельзя публиковать в сети

Публикация номера телефона, адреса или полного имени многократно повышает уязвимость и открывает мошенникам прямой канал для шантажа, фишинга и других манипуляций. Часто человек сам рассказывает о себе слишком много. Распространённые ошибки пользователей:

- открытый профиль;
- геолокация на фото и в публикациях;
- номер школы или адрес на фото;
- имя и фамилия в профиле, номер телефона в открытом доступе;
- сведения о составе семьи;
- номер карты и пароль в сохранённых сообщениях⁷.

Опасны и прямые эфиры из дома: без заготовленного текста легко случайно назвать адрес или показать обстановку квартиры, ценные вещи, родственников. Фото и видео с близкими и друзьями не стоит выкладывать без их разрешения; для личных публикаций лучше использовать фильтр «Только для близких друзей». Не публикуют фото паспорта и других документов, билетов, посадочных

⁵ Из УМК 2024/2025 учебного года (Век информации. 120 лет Информационному агентству России ТАСС).

⁶ Из УМК 2025/2026 учебного года (Цифровой щит. Основные правила безопасности в сети Интернет).

⁷ Из УМК 2025/2026 учебного года (Цифровой щит. Основные правила безопасности в сети Интернет).

талонов: по фото билета мошенник может пройти на мероприятие вместо владельца⁸.

Надёжный пароль и защита аккаунта

Надёжный пароль содержит специальные знаки, заглавные и строчные буквы, цифры и не связан с пользователем. Для паролей не подходят имя, возраст, дата рождения, клички животных, имена родственников, а также комбинации только из цифр или только из букв и элементарные наборы вроде 123456 или абвгд. На разных сервисах нужны разные пароли, менять их рекомендуется раз в полгода. Дополнительную защиту даёт двухфакторная аутентификация.

Проверка на сервисе 2ip.ru/passcheck показывает, как быстро можно взломать пароль:

123456789 — за 0 секунд;

ANNa11 — за 14 секунд;

ANNAPERSIK — за 588 минут;

Jack4321 — за 910 минут;

persik1234 — за 254 часа;

ANNA_JACK — за 1889 часов;

A!-2na1234 — за 6810 лет;

A!-7n9aj234 — за 544 770 лет.

К профилю стоит привязать актуальный номер телефона и указать настоящие имя и фамилию, установить реальное фото: так восстановить профиль в случае взлома будет проще. Важно разобраться в настройках приватности во всех соц-сетях⁹.

Регулярно проверяйте раздел «Активные сессии» или «Устройства» в настройках мессенджеров, чтобы убедиться, что к аккаунту не подключены посторонние. Логины, пароли и коды из СМС не передают никому и ни под каким предлогом: код подтверждения никогда не запрашивают сотрудники банков или ведомств¹⁰.

⁸ Из УМК 2022/2023 учебного года (Кибербезопасность).

⁹ Из УМК 2022/2023 учебного года (Кибербезопасность).

¹⁰ Из УМК 2025/2026 учебного года (Цифровой щит. Основные правила безопасности в сети Интернет).

Как действуют мошенники

Основные угрозы для пользователя соцсетей:

- кража профиля через взлом логина и пароля;
- манипуляция, чтобы пользователь сам передал свои данные;
- доступ к сохранённым личным данным и данным банковской карты;
- продуманное мошенничество на основе открытой информации о человеке;
- обман через подменные и анонимные профили;
- мошенничество на основе утечки данных со сторонних ресурсов.

Типичные приёмы злоумышленников:

- изучают открытую информацию в профиле и подробности жизни человека;
- провоцируют на эмоции и торопят, чтобы не дать разобраться в происходящем;
- создают копию официального сайта с похожими буквами в адресе или сайт с подозрительно низкими ценами;
- выдают себя за администрацию сайта, техподдержку или организацию, сообщают о штрафе или о том, что родственник попал в беду;
- предлагают продолжить знакомство офлайн и присылают ссылку для «покупки билетов», например в кино;
- рассылают спам-сообщения друзьям пользователя со взломанной страницы¹¹.

Мошенники не показывают своё лицо, не называют настоящее имя или выдают себя за других. Они предлагают работу, деньги, подарки, игровую валюту, чтобы заставить человека сделать то, что им нужно. Самая распространённая цель фишинга — получить доступ к аккаунту в мессенджере, чтобы потом писать людям из списка контактов с просьбой одолжить денег¹².

Признаки обмана и социальной инженерии

Слишком лёгкие деньги

Если за простые действия обещают очень высокий доход — это повод насторожиться. Лёгких денег не бывает.

Запрос доступа

Если требуют доступ к счёту, карте или аккаунту — это не работа, а ловушка.

Давление

Фразы «всё законно», «все так делают», «я тоже так работаю» — моральное давление. Законные предложения в нём не нуждаются.

¹¹ Из УМК 2022/2023 учебного года (Кибербезопасность).

¹² Из УМК 2025/2026 учебного года (Цифровой щит. Основные правила безопасности в сети Интернет).

Срочность

Слова «срочно», «прямо сейчас», «последний шанс», «иначе будет поздно» — главный маркер манипуляции. Законные организации не требуют немедленных действий под угрозой.

Секретность

Требование никому не рассказывать и обещание «об этом никто не узнает» всегда должны настораживать.

Запугивание

Страх уголовной ответственности, обвинения в «спонсировании терроризма» или «утечке данных» — распространённая легенда мошенников.

«Проверочные задания»

Просьбы оформить карту, скачать приложение, включить демонстрацию экрана или передать устройство курьеру — это вовлечение в преступную схему.

Важно помнить: «безопасных счетов» не существует, так же как не бывает «дистанционных обысков» и «декларации наличных накоплений». Звонящего «из банка» лучше прервать и перезвонить по номеру с официального сайта. Фото, голос и даже видеосвязь могут быть поддельными, поэтому в сети действует принцип нулевого доверия: по умолчанию не доверять никому, пока информация не подтверждена. Решения не стоит принимать в состоянии гнева, усталости или болезни¹³.

Аренда аккаунтов и дропперство

Подростку могут предложить: «Просто дай доступ к аккаунту — получишь 1000 рублей за 5 минут». Такие аккаунты используют зарубежные мошеннические кол-центры, чтобы обходить блокировки: с них рассылают мошеннические сообщения, распространяют экстремистский контент, выманивают деньги у друзей владельца. Отвечает за это хозяин аккаунта. Сделки по покупке или аренде аккаунтов в 100% случаев связаны с противоправной деятельностью.

Дропперство — схема, при которой преступники используют чужой банковский счёт для вывода денег, добытых незаконным путём. Счёт становится транзитным, а его владелец — соучастником мошенничества. Образно говоря, человека просят поддержать дверь, пока грабитель выносит вещи. Если на карту пришёл перевод от незнакомца и тут же просят вернуть деньги «на правильный счёт», соглашаться нельзя. Фразы «я не знал» или «меня просто попросили» в суде не освобождают от ответственности¹⁴.

¹³ Из УМК 2025/2026 учебного года (Цифровой щит. Основные правила безопасности в сети Интернет).

¹⁴ Из УМК 2025/2026 учебного года (Цифровой щит. Основные правила безопасности в сети Интернет).

Вовлечение подростков в преступные схемы

Под видом «подработки» подростков вербуют курьерами, просят сфотографировать объекты или совершить поджог. Незнакомцы в начале общения спрашивают, где человек живёт и есть ли рядом железная дорога, а не о навыках и умениях. Курьер рискует свободой напрямую, а организаторы часто находятся за границей. Поджог на железной дороге, который подросток считал «подработкой», квалифицируется как терроризм.

Пример: в Иркутской области 18-летний юноша поверил «сотруднику финансового мониторинга», перевёл на «безопасный счёт» бабушкины сбережения, а затем по указке «сотрудника ФСБ» поджёг объект инфраструктуры. Ему грозит до 20 лет по статье «Террористический акт». Схема состоит из трёх шагов:

- легенда о «безопасном счёте» или срочном переводе под предлогом «спасения» или «декларации» денег;
- прикрытие авторитетом: «ФСБ», «госструктуры»;
- ступенчатое вовлечение: сначала перевод денег, потом поджог. Человек уже нарушил закон, и страх ответственности или шантаж становится инструментом дальнейшего давления.

Первые три действия при подобном предложении: не отвечать, сделать скриншот, показать родителям или учителю и обратиться в полицию¹⁵.

Деструктивный контент и сообщества

Деструктивный контент — информация, которая провоцирует агрессию или страх, призывает к насилию или нарушению закона, распространяет ненависть. Чаще всего он встречается в закрытых чатах и каналах. Признаки:

- громкие заголовки: «Смотри, пока не удалили!», «Только для своих!», «Слив», «Нажми, и узнаешь то, что так давно скрывали!»;
- попытка вызвать сильную тревогу, страх, гнев или ненависть к группе людей;
- деление мира на «своих и чужих», ультимативные утверждения, агрессивная лексика и капслок;
- призывы к изоляции от близких, опасным для здоровья действиям, оправдание насилия;
- романтизация депрессивных состояний и рискованных поступков как признака исключительности;
- отсутствие ссылок на проверяемые источники.

Правильная реакция — закрыть страницу, не комментировать, не спорить и не пересылать (пересылая, человек становится частью распространения), пожаловаться модераторам и рассказать взрослому. Эмоциональная реакция — именно то, на что рассчитывают создатели такого контента.

¹⁵ Из УМК 2025/2026 учебного года (Цифровой щит. Основные правила безопасности в сети Интернет).

В деструктивные сообщества втягивают тремя способами:

через исключительность: «Ты не такой, как все. Ты видишь то, что скрыто от других»;

через секретность: «То, что здесь происходит, остаётся здесь. Если расскажешь — тебя не поймут»;

через давление или жалость: «Ты что, слабак?» или «Тебя все обижают, а мы — твоя настоящая семья».

Закрытая группа с входом только по приглашению — повод насторожиться. Сомнение — защитный механизм: если уговаривают сделать то, что вызывает сомнение, нужно сказать «нет». Слова «ты особенный», «только для своих», «мы — семья» от чужого человека — не забота, а контроль. Помогают защититься критичность, связь с семьёй и друзьями, доверие собственным ощущениям¹⁶.

Фейки и проверка информации

Огромный поток сообщений из соцсетей и телеграм-каналов не даёт полной и правдивой картины происходящего: посты могут быть ошибочны или намеренно искажены, а получив ложную информацию, человек может принять неправильное решение. Фейки основаны на эмоциях, поэтому люди спешат поделиться ими, не проверив. Сенсационные новости распространяются быстрее, даже если не соответствуют действительности. «Уткой» называют любую недостоверную информацию, запущенную ради сенсации.

Фейки бывают преднамеренными и непреднамеренными. При пересказе по цепочке даже правдивая новость искажается и из нейтральной становится эмоциональной. Например, видео с медведями на пляже, которое блогеры неоднократно выдавали за свежую новость, снято в Калифорнии на озере Тахо в 2016 году. Трейлер о «летающих пингвинах» был первоапрельским розыгрышем 2008 года. Лайки не являются критерием достоверности.

Чек-лист «Как отличить фейк от правды»:

- прочитать новость целиком, а не только заголовок;
- проверить автора публикации;
- найти первоисточник и дату публикации;
- убедиться, что это не розыгрыш и не шуточный портал;
- проверить информацию в нескольких источниках, лучше официальных;
- проверить факты, цифры, цитаты, фото и видео (например, обратным поиском по картинкам);
- обратить внимание на ошибки и шаблонные формулировки;

¹⁶ Из УМК 2025/2026 учебного года (Цифровой чит. Основные правила безопасности в сети Интернет).

- проверить веб-адрес сайта, чтобы исключить фишинг;
- контролировать свой эмоциональный фон.

Необходимо не только распознавать фейки, но и не распространять их. Лучше всего получать информацию из проверенных и авторитетных источников, а сенсацию из школьного чата сначала уточнить у взрослых или на сайте школы¹⁷.

Алгоритм «Разоблачи мошенника»

Кто отправитель? Знаком ли этот человек, почему он пишет, настоящий ли аккаунт?

Куда ведёт ссылка? Совпадает ли адрес с официальным, нет ли ошибок и лишних символов?

К чему призывают? «Срочно», «немедленно», «последний шанс», угрозы, «никому не говори».

Можно ли взять паузу? Что будет, если подождать и посоветоваться с родителями?

Есть ли безопасный способ? Позвонить в банк, написать в службу поддержки, спросить у взрослых¹⁸.

Базовые правила цифровой гигиены

Использовать сложные и уникальные для каждого сервиса пароли.

Включить двухфакторную аутентификацию.

Устанавливать приложения только из официальных магазинов: сторонние сайты часто распространяют программы-шпионы.

Пользоваться отдельной картой для онлайн-платежей с ограниченным балансом.

Настроить приватность в соцсетях и мессенджерах.

Не сохранять пароли в браузере на чужих устройствах.

Не использовать публичный Wi-Fi для банковских операций.

Не переходить по неизвестным ссылкам.

Не отправлять фото документов и коды из СМС.

Не публиковать избыточную личную информацию: адрес, геолокацию, данные о семье и поездках¹⁹.

¹⁷ Из УМК 2024/2025 учебного года (Век информации. 120 лет Информационному агентству России ТАСС).

¹⁸ Из УМК 2025/2026 учебного года (Цифровой щит. Основные правила безопасности в сети Интернет).

¹⁹ Из УМК 2025/2026 учебного года (Цифровой щит. Основные правила безопасности в сети Интернет).

Правила для младших школьников

Никогда не давать свои аккаунты другим людям и не брать чужие — это как отдать незнакомцу ключи от квартиры.

Не соглашаться стать «помощником» и переводить деньги.

Если в сети встретилось что-то пугающее, грубое или странное — не смотреть, не делиться и рассказать взрослому.

Не нажимать на подозрительные ссылки.

Не сообщать незнакомцам личные данные: где живёшь, учишься, где работают родители.

Всегда рассказывать родителям или учителю, если встретилось что-то непонятное.

Обновлять пароли, пользоваться антивирусными программами.

Чтобы доверять человеку, недостаточно пообщаться с ним в интернете несколько дней. Настоящие друзья и взрослые никогда не попросят перевести деньги, сфотографировать мамину карту или дать доступ к аккаунту. Как в реальной жизни есть правила безопасности — переходить дорогу на зелёный свет, закрывать входную дверь, так и в цифровом мире есть свои правила²⁰.

Ситуации из жизни

«Курьер»

Парню в мессенджере предложили подработку: забирать наличные у пожилых людей и переводить на биткоин-кошелёк. За первый заказ заплатили 5000 рублей, на второй раз его задержала полиция — это были деньги обманутых пенсионеров.

«Украли аккаунт»

Девушка за обещанные 1000 рублей дала код от аккаунта «для голосования в конкурсе». Через час всем её контактам пришло: «Срочно займи 10 000, потом объясню».

«Фото с геолокацией»

Парню в чате фанатов игры за «крутой скин» предложили сфотографировать трансформаторную будку и прислать координаты. Через неделю пришли с обыском: это была подготовка к теракту.

«Розыгрыш»

Участника канала с «тёплой атмосферой своих» попросили прислать фото паспорта и селфи с ним для «закрытого розыгрыша». Вскоре на его имя пытались оформить займы, а фото паспорта выложили в открытый канал.

²⁰ Из УМК 2025/2026 учебного года (Цифровой чит. Основные правила безопасности в сети Интернет).

«Звонок из полиции»

Девочке позвонили с номера «Полиция» и сказали, что маму посадят, если срочно не «задекларировать имущество»: нужно собрать деньги и ценности и передать курьеру.

«Игровая валюта»

Незнакомец в игровом чате за валюту дал «простые задания»: взять телефон мамы, открыть онлайн-банк и переслать данные²¹.

«Продюсер»

Девочке написал «продюсер» любимой группы и предложил кастинг, для которого нужна платная фотосессия. Просил перевести деньги как можно быстрее, после оплаты пропал.

«Взломанный блогер»

Подписчики блогера получили просьбу прислать деньги на лечение её животного. Они знали, что у неё аллергия на животных, поняли, что аккаунт взломан, и пожаловались модератору²².

Куда обращаться за помощью

Если ребёнок столкнулся с мошенниками, важно сказать ему, что он не виноват, но общение с мошенниками нужно прекратить; номера можно добавить в чёрный список. Обращаться в полицию необходимо даже при неудачной попытке обмана: это помогает установить причастных и предотвратить другие преступления.

Полиция

Заявление принимают в любом отделе внутренних дел независимо от места преступления; для несовершеннолетнего нужно присутствие родителя или законного представителя. Переписку не удаляют: скриншоты, ссылки, реквизиты, СМС и выписки — доказательства. Сообщить можно и по телефонам 102/112.

Подозрительный звонок

Сообщить через «Госуслуги» (pos.gosuslugi.ru/lkp/poll-anti-fishing) и сотовому оператору, чтобы номер промаркировали как нежелательный.

Деструктивный контент

Электронная форма Роскомнадзора или приложение «РКН» с точным адресом страницы.

Фишинговый сайт

Система мониторинга «Антифишинг» Минцифры (paf.occsirt.ru).

Персональные данные ребёнка в сети

Общественная приёмная Роскомнадзора, требование к владельцу ресурса удалить данные, бесплатные консультации Центра правовой помощи гражданам в цифровой среде (4people.grfc.ru).

²¹ Из УМК 2025/2026 учебного года (Цифровой щит. Основные правила безопасности в сети Интернет).

²² Из УМК 2022/2023 учебного года (Кибербезопасность).

Кража аккаунта на «Госуслугах»

Горячая линия 8-800-100-70-10 или центр обслуживания. После восстановления — сменить пароль, проверить личные данные и историю операций, заказать кредитную историю, включить двухфакторную аутентификацию, указать доверенный контакт и поставить самозапрет на кредиты.

Поддержка

Единый общероссийский телефон доверия²³.

Ответственность по закону

С 5 июля 2025 года за дропперство предусмотрена уголовная ответственность с 16 лет (ст. 187 УК РФ): до 6 лет лишения свободы и штраф от 300 тыс. до 1 млн рублей. Если дропом стал ребёнок младшего возраста, его могут поставить на учёт в полиции, а родителей — оштрафовать или обязать вернуть деньги.

С 1 сентября 2025 года введены ст. 274.5 УК РФ и ст. 13.29.2 КоАП РФ (аренда аккаунтов). Если участник схемы не достиг возраста уголовной ответственности, к ответственности привлекаются родители по ст. 5.35 КоАП РФ²⁴.

Федеральный закон № 149-ФЗ «Об информации...»: ст. 10.6 обязывает владельца соцсети выявлять и ограничивать недостоверную информацию, ст. 15.3 — основание для блокировки сайтов с недостоверной информацией.

Статья 13.15 КоАП РФ — за распространение в СМИ и интернете заведомо недостоверной информации под видом достоверных сообщений.

Статья 207.1 и 207.2 УК РФ — за публичное распространение заведомо ложной информации об угрозах жизни и безопасности граждан и общественно значимой информации, повлекшее тяжкие последствия²⁵.

Интересные факты

Каждую секунду пользователи соцсетей отправляют около 20 тысяч сообщений.

В 2024 году Информационному агентству России ТАСС исполнилось 120 лет. Главной задачей агентства его гендиректор Андрей Кондрашов называет «охранять информационные рубежи России», а архивы ТАСС — страховка от фальсификации исторических фактов.

В ноябре 2021 года ТАСС открыло корреспондентский пункт на МКС и стало первым и единственным СМИ мира с представительством в космосе.

²³ Из УМК 2025/2026 учебного года (Цифровой чит. Основные правила безопасности в сети Интернет).

²⁴ Из УМК 2025/2026 учебного года (Цифровой чит. Основные правила безопасности в сети Интернет).

²⁵ Из УМК 2024/2025 учебного года (Век информации. 120 лет Информационному агентству России ТАСС).

Верная формулировка известного выражения для века информации: «Кто владеет достоверной информацией, тот владеет миром»²⁶.

Постразговор

Что почитать:

- Шарова Л. «Стоп Угроза. Безопасный интернет»
- Каретникова Е. «Маршрут не построен»
- Белоус А. «Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения»

Что посмотреть:

- Мультсериал «Смешарики. Азбука цифровой грамотности», 2019
- Сериал Движения Первых «Золотые сети» о кибербезопасности
- Видеоцикл «Антивербовка» и марафон «Навыки для жизни» Движения Первых
- Подкаст «Разговор по делу. Инфобезопасность»

Проекты:

- «Школа кибербезопасности Движения Первых»: обучающиеся становятся киберволонтерами и проводят «КиберУрок» для сверстников (киберволонтеры.будвдвдвижении.рф)²⁷.

²⁶ Из УМК 2024/2025 учебного года (Век информации. 120 лет Информационному агентству России ТАСС).

²⁷ Из УМК 2025/2026 учебного года (Цифровой щит. Основные правила безопасности в сети Интернет).