Примерная матрица
занятия по программе «Я. МОЯ СЕМЬЯ. МОЯ РОДИНА»
8 класс
Тема: Чему можно доверять в интернете?[1]
Время проведения: февраль
Целевая установка: расширение представлений учащихся об информационной безопасности в сети Интернет; повышение грамотности учащихся в вопросах безопасного поведения в сети; расширение знаний о способах распознавания недостоверной информации.
Методическая установка:

Предложенная матрица тематического занятия является примерной, при ее реализации необходимо учитывать особенности класса, технические возможности учреждения образования.

Занятие может быть проведено в учебном кабинете.

Накануне занятия рекомендуется провести опрос учащихся (приложение 1), результаты которого станут основой для введения в тему занятия.

Для закрепления информации можно оформить методический материал в виде памяток, информации на сайте учреждения образования.

Источники и ресурсы:

1. Актуальные вопросы обеспечения информационной безопасности: пособие для педагогов учреждений образования, реализующих образовательные программы общего среднего образования / В.Ю. Арчаков [и др.]. – Минск: Народная асвета, 2022. – 167 с. : ил., табл.
2. Закон Республики Беларусь «О правах ребенка» (ст.37)
3. Детский правовой сайт: видеоролик Персональные данные в интернете, листовка Безопасный интернет, флаер Мои правила онлайн безопасности

[1] **Матрица подготовлена с использованием материалов:** Концавенко Е. Л., педагога социального ГУО «Гимназия № 5 г. Минска имени Героев встречи на Эльбе»; Шведовой-Юницкой О. В., заместителя директора по учебной работе ГУО «Новоселковская средняя школа Ошмянского района»; Бутько Е.А., классного руководителя 8 класса ГУО «Лелюкинская средняя школа Ивьевского района».

4. Информация Национального центра защиты персональных данных Республики Беларусь: памятка «Детям о персональных данных», видеоролик Вредные советы о персональных данных, рекомендации для учащихся «Важные правила БезОпасности персональных данных»

Структурный компонент занятия	Содержательный компонент занятия
Вводный этап	Для введения в тему занятия можно использовать результаты опроса учащихся, проведенного накануне занятия (приложение 1). Актуализация темы занятия с помощью упражнения «Снежный ком». Педагог может предложить учащимся назвать как можно больше слов, связанных с понятием «безопасный интернет». Педагог акцентирует внимание на том, что Интернет может быть средством для обучения, отдыха или общения. Он же может быть источником серьезных проблем. Поэтому очень важно быть в курсе существующих интернет-угроз и знать, что предпринять для обеспечения собственной безопасности. Одна из угроз – фейковая информация, направленная на вовлечение несовершеннолетних в противозаконные, противоправные действия, участие в различного рода несанкционированных действиях. Схема действия деструктивных групп следующая: выброс недостоверной, часто «шокирующей» информации, нагнетание негатива путем добавления новостей, подтверждающих фейковую информацию, поиск «виновных» в случившемся и, как итог, призыв к активным действиям (участие в митингах, демонстрациях, акциях протеста). Основной способ борьбы с фейковой информацией – критическое мышление (важнейший навык XXI в.). Люди, которые способны анализировать информацию, не подвержены влиянию громких суждений и эмоциональных высказываний. Существует ряд приемов, позволяющих распознать недостоверную информацию.
Основной этап	**Обсуждение с учащимися вопросов** о распознавании недостоверной информации в сети. *1. Что такое фейк? Для чего создается фейковый контент?* *2. Как распознать: фейковый аккаунт в социальных сетях? фейковое изображение? фейковую новость?*

	3. Как проверить информацию? *4. Как не стать жертвой фейковых писем-сообщений?* Для обсуждения вопросов предлагается использовать материал приложения 2. Рекомендуется организовать работу учащихся в группах по **обсуждению ситуаций, предложенных в приложении 3** с последующим представлением мнения группы классу. Наши действия в интернете, к сожалению, могут привести к нежелательным последствиям в реальном мире. Мы создаем профили в соцсетях и других сервисах, оставляем свои данные на разных ресурсах. Часто сами сервисы просят нас рассказать что-то о своей жизни, поделиться эмоциями, указывать места, которые вы часто посещаете, других людей на фотографии и т.д. *Рекомендуется обсудить с учащимися вопрос:* **как обеспечить свою безопасность в Интернете?** (приложение 4). В завершение занятия можно провести **викторину** «Что я знаю о безопасной работе в Интернете» (приложение 5).
Заключительный этап	При подведении итогов занятия педагог акцентирует внимание учащихся на следующем: - не всякая информация в сети Интернет является достоверной; - к информации следует относиться критически: проверять аккаунты, изображения, новостные сообщения и др.; - при появлении писем-сообщений важно сохранять рассудительность, предварять любые действия звонком; - в случае, если стали жертвой мошенников, немедленно сообщить родителям, педагогам. Для закрепления знаний учащихся по теме занятия целесообразно предложить им выполнить практическое задание: разработать флаер «Как не стать жертвой фейковой информации». В учреждении образования может быть организован конкурс флаеров, плакатов по данной теме.

Приложение 1

Анкета для предварительного опроса учащихся

1. Вы пользуетесь дома интернетом? *Да Нет*
2. Сколько времени вы обычно проводите в сети?
   менее 1 часа в день
   1-2 часа в день
   более 2-х часов
   более 3-х часов
3. С какой целью вы используете Интернет?
   поиск учебной информации
   общение с друзьями
   просмотр роликов, фильмов
   онлайн игры
   другое _____
4. Приходилось ли вам сталкиваться с фейковой информацией в сети Интернет? *Да Нет*
5. Можете ли вы отличить недостоверную информацию в Интернете от достоверной? *Да Нет*
6. Получали ли вы сообщения в соцсетях и мессенджерах с просьбами перечислить деньги, проголосовать за участника конкурса, призывами переслать другу, сделать репост и др. *Да Нет*
7. Общаетесь ли вы в сети Интернет с незнакомцами? *Да Нет*
8. Был ли у вас какой-либо неприятный случай, связанный с общением в информационном пространстве? *Да Нет*
9. Контролируют ли ваши родители ваше использование сети Интернет? *Да Нет*
10. Знаете ли вы правила безопасного поведения в сети Интернет? *Да Нет*

Примечание. Результаты предварительного опроса можно использовать для:

1) организации воспитательной работы с учащимися;
2) организации «родительского университета», консультаций с родителями учащихся.

Приложение 2

Сегодня часто можно слышать слово ***ФЕЙК.*** Оно употребляется на телевидении, радио или просто в межличностном общении.

В самом общем смысле, ФЕЙК — это любая недостоверная информация, размещенная в интернете. Фейк может быть намеренным и ненамеренным, полным или частичным. Фейковой может быть информация любого вида: новость, изображение, видеоролик и даже аккаунт в социальных сетях.

Цели, которые преследуют создатели фейкового контента:

• создание социальной напряженности; вовлечение людей в деструктивные действия;

• дезинформация, предоставление заведомо ложных, сфабрикованных «фактов»; намеренная дезинформация пользователей о каких-либо событиях для так называемого хайпа — привлечения внимания в целях зарабатывания денег;

• реклама определенного продукта или обход лимитов для спама (ведь в большинстве социальных сетей действуют ограничения на добавление друзей и рассылку писем);

• мошенничество;

• повышение трафика в социальных сетях и/или сайтах;

• формирование у потребителя информации определенного взгляда на товары; продвижение товаров и услуг, «накрутка» рейтинга;

• открытое оскорбление определенных лиц;

• троллинг (фейк в таких случаях создается для развлечения и самоутверждения путем участия в спорах, дискуссиях);

• личные мотивы (например, желание закомплексованного пользователя иметь двойника, который отличается другим имиджем) и др.

Как распознать фейковый аккаунт в социальных сетях:

1. Профиль не заполнен вовсе или заполнен частично, лишен индивидуальных черт.
2. Отсутствуют фотографии или присутствуют в незначительном количестве. Фотографии не отображают личность человека и не дают о нем четкого представления.
3. Профиль заполнен от заведомо выдуманного, несуществующего персонажа (например, от имени героя фильмов).
4. На «стене» преобладают репосты, не связанные единством тем и источников, по сути — это спам.
5. Не стоит доверять сайтам, если площадка выглядит подозрительно, появилось много рекламы (баннеров) и визуальных элементов, которых вы раньше не замечали, адрес страницы немного отличается от настоящего, но вас об этом предупредили

и уверяют, что все нормально, так и должно быть. Скорее всего вы столкнулись с фишинговым сайтом. (Фишинг – мошенничество, направленное на кражу данных)

Как распознать фейковое изображение?

1. Проверить уникальность изображения. Для этого скопировать ссылку на изображение, перейти на страницы поиска изображений в популярных поисковиках (https://yandex.ru/images/ и https://www.google.ru/imghp) и, выбрав опцию «Поиск по картинке», указать адрес проверяемого изображения.
2. Изучить результаты поиска, в которых будут как дубликаты проверяемого изображения, так и похожие на него картинки. Таким образом можно узнать, было ли изображение модифицировано (проще говоря, дорисовано).
3. Проверить даты публикаций дубликатов. Если проверяемое изображение подается как свежее и иллюстрирует какую-либо новость (особенно скандальную), а дубликаты были опубликованы значительно ранее, то изображение фейковое. А если изображение было новостным поводом, то фейком является и сама новость.

Как распознать фейковую новость?

1. Читать дальше заголовка. Нередко сама новость практически никак не связана с громким заголовком, единственная цель которого – увеличить посещаемость.
2. Изучить историю новости. Есть ли у нее первоисточник? Ссылается ли прочитанная вами новость на какие-либо иные источники? Подтверждается ли приведенная информация из иных независимых источников?
3. Есть ли у информации, приведенной в новости, персонифицируемый источник, или она подается анонимно, абстрактно (например, «большинство наших читателей считает...», «как заявляют многие ученые...»). Если у информации источник есть, то насколько он компетентен именно в той области, которой посвящена статья (например, мнение архитектора о развитии медицины вряд ли может считаться экспертным).
4. Если один и тот же новостной повод «обрушился» на вас из множества источников сразу, тем более, в однообразной подаче, то речь идет о вбросе фейка.
5. Подвергайте информацию критическому анализу: какой может быть цель ее опубликования? Какой реакции на нее ждут от вас лично? Кому и зачем необходимо вызвать именно такую массовую реакцию?

Как проверить информацию?

1. «Правило трех». Прежде чем принять за истину какую-либо информацию в Интернете, необходимо проверить ее еще, как минимум, в двух, не зависимых друг от друга, источниках. Если «важная новость» опубликована лишь на одном ресурсе, и информацию о ней не распространяют другие, в частности, крупные информационные агентства, то, скорее всего, это фейк.

2. Обратить внимание на веб-адрес страницы: порой крупные новостные сайты имитируются сайтами-подделками. Найдите первоисточник информации (какое издание или ресурс её опубликовали, кто автор, какова дата публикации.

3. Сравнить полученную информацию с уже известной по этой теме. В поисках какого-либо материала не стоит полагаться на первые попавшиеся источники.

4 Проверить достоверность полученной информации у авторитетных экспертов в данной области (специалистов).

Приложение 3

Вопросы-ситуации для обсуждения в группах

1. Дополните список признаков фейков:

новость содержит призыв к распространению: «отправь другу, сделай репост, отнесись серьёзно, расскажи тем, кого ты действительно любишь...»;

кликбейтный заголовок;

эмоциональность изложения (акцент на том, что вызывает чувство страха или гнева; касается денег, здоровья, вас, вашей семьи, друзей);

срочность (например, вас просят немедленно отреагировать и распространить информацию).

2. Как действовать, если приходит смс, в котором говорится об ошибочном переводе и просьбе вернуть якобы переведенные средства?

3. Как действовать, если пришло сообщение или уведомление от онлайн-банка о снятии денег в банкомате или оплате онлайн-покупки, а вы этого не делали?

4. Что делать, если какое-то действие вас просят совершить немедленно или дают небольшое количество времени на обдумывание (например, принять участие в лотерее, но сделать это можно только в течение ограниченного времени)?

5. Как действовать, если вас просят срочно помочь, например, переводом денег?

Приложение 4

Как обеспечить свою безопасность в Интернете?

Безопасность персональных данных в компьютерных играх.

1. Придумайте сложный и уникальный пароль для игрового аккаунта. Он должен быть больше 12 символов и содержать буквы, цифры и специальные символы.

2. Удалите всю личную информацию из своего игрового аккаунта. Лучше максимально абстрагироваться от любых ассоциаций с персональными данными, в том числе и с аккаунтами в социальных сетях.

Безопасность в социальных сетях

1. Сделать свой аккаунт приватным. Закройте свой аккаунт, чтобы быть уверенным: контент, который вы публикуете, доступен только друзьям и знакомым. Некоторые незнакомцы могут оказаться злоумышленниками. Они могут узнать у вас личную информацию или прислать фишинговые ссылки на сервисы, чтобы украсть личные данные. Запретите отправку сообщений от незнакомых вам людей.

2. Использовать антивирусные решения на всех своих устройствах. Технические меры защиты, установленные на ваших устройствах, помогут вам уберечь свои данные от действий зловредного программного обеспечения (вирусов, троянов, шифровальщиков и др.).

Кроме того, стоит позаботиться и о том, чтобы регулярно устанавливать обновления для вашей операционной системы, мобильных приложений и защитных решений. Зачастую этого может оказаться недостаточно, ведь о существовании уязвимости знают не только разработчики, но и злоумышленники, которые могут эти уязвимости эксплуатировать в своих целях. Например, они могут получить доступ к данным, которые хранятся на вашем устройстве (фото, видео, переписка).

Антивирус помогает быстро «отловить» все опасности, которые могут угрожать вашим данным. Например, обнаружить зловредное программное обеспечение, заблокировать переход по фишинговой ссылке или отфильтровать спам-письмо в электронной. Устанавливать защитные решения нужно не только на персональные компьютеры, но и на мобильные устройства.

3. Использовать надежный пароль. Правило такое: один сервис, один пароль. Не самой хорошей идеей будет авторизация в социальной сети при помощи аккаунта другой социальной сети, т.к. в случае утечки данных обе учетных записи будут скомпрометированы.

4. Не открывать подозрительные ссылки. Если вы получили сообщение с такой ссылкой, даже от человека из вашего списка контактов, не торопитесь по ней переходить. Обращайте внимание на подозрительные словосочетания в обращении собеседника. Например, обычно ваш друг даже не здоровается, а сразу переходит к сути вопроса. А в этот раз пишет «доброе утро!» и «как дела?». Сообщение от мошенников может начинаться словами «Дорогой друг…» в начале, вместо обращения по имени и др. В этом же сообщении вас могут просить что-то сделать: проголосовать за рисунок, видеофрагмент, оценить работу художника и т.п. Не спешите это делать, свяжитесь со своим другом, например, по телефону и уточните детали. Или задайте вопрос, ответ на который можете знать только вы вдвоем.

5. Очень внимательно относиться к тому, в какие группы вас приглашают. Некоторые сайты, web-страницы, интернет-сообщества могут приглашать детей и молодых людей входить в разные группы по интересам, увлечениям (по музыкальному направлению, творческой деятельности (вокалу, рисованию и др.), могут быть посвящены определенному фильму, сериалу, творчеству музыкального исполнителя, актера и т.д.). Такие группы оказывают положительное влияние, способствуют углублению знаний в определенной сфере, организации общения с единомышленниками.

Но! Среди таких групп могут быть *группы, которые оказывают вредное, негативное влияние:*

- экстремистские (обучают использованию оружия, нанесению вреда зданиям, сооружениям, технике, в том числе посредством граффити и неуважительных надписей, призывают к убийствам и проведению выступлений протеста, террористических акций);
- религиозно-сектантские (призывают к вступлению в религиозные группы, которые считают себя исключительными, избранными, готовыми лишать жизни себя или других людей, разрушать памятники культуры, сооружения и имущество людей других религиозных взглядов);
- призывающие к причинению вреда собственному здоровью и организму;
- фанатские, нацистские и иные группы, призывающие к агрессивным, разрушительным действиям в отношении материальных объектов, людей других групп и др.

Подобные группы называют *деструктивными* (опасными, наносящими вред, уничтожающими, разрушающими само общество, его культуру, нарушающими благополучие, права, здоровье граждан).

В деструктивных группах происходит изменение норм, правил, привычного поведения. Человек начинает по-другому относиться к другим людям, событиям, своей жизни, не ценит то, что дает общество – право развиваться, учиться, общаться, реализовывать себя с пользой для себя, других людей, своей страны. Попасть под такое негативное влияние можно легко – если человек много читает в сети соответствующую информацию, смотрит видео и фото, участвует в играх, выполнении специальных заданий, общается с членами группы.

Ежедневно в социальных сетях службы информационной безопасности выявляют тысячи сообществ с участием несовершеннолетних, пропагандирующих деструктивные формы поведения (агрессия, употребление наркотических средств, терроризм, причинение себе вреда и прочее).

Будьте очень внимательны! Подавляющее большинство подростков и молодежи уверены, что лично с ними, никогда ничего плохого в сети интернет не произойдет. Но, к сожалению, они ошибаются, так как подход к каждому человеку подбирается индивидуально.

Что делать, если попались в ловушку?

- СПОКОЙСТВИЕ! Даже если с тобой случилась неприятность в сети ты можешь довериться взрослым, которые рядом с тобой. Они помогут тебе справиться!
- ГОВОРИМ РОДИТЕЛЯМ! Так они смогут тебе помочь. Не поддавайся на манипуляции обманщиков в сети, их задача – не дать тебе подключить взрослых, поэтому они могут угрожать, шантажировать, брать тебя «на слабо».
- МЕНЯЕМ ВСЕ ПАРОЛИ! Для того, чтобы обезопасить свою личную информацию, сделай это как можно скорее. Это поможет тебе ограничить влияние обманщика из интернета.
- ПРЕДУПРЕЖДАЕМ ДРУЗЕЙ В ИНТЕРНЕТЕ! Для того, чтобы не попасть в неловкую ситуацию и не дать злоумышленникам использовать твои данные для обмана других сообщи всем, с кем общаешься, что твои данные украдены, говорить какие именно не стоит.
- СООБЩИТЬ МОДЕРАТОРАМ РЕСУРСА! Это даст тебе дополнительную поддержку и поможет не допустить нового обмана.

Приложение 5

Викторина «Что я знаю о безопасной работе в Интернете»

1. Ты зашёл на незнакомый сайт. Вдруг на экране компьютера появились непонятные тебе сообщения. Что ты сделаешь?

1) Быстро закроешь сайт.

2) Обратишься к родителям за помощью.

3) Сам устранишь неисправность.

***Комментарий**: всегда спрашивай родителей о незнакомых вещах в Интернете. Они расскажут, что безопасно делать, а что нет.*

2. На адрес твоей электронной почты пришло сообщение: файл с игрой от неизвестного тебе пользователя. Как ты поступишь?

1) Скачаешь файл и начнешь играть.

2) Не откроешь файл.

3) Отправишь файл своим друзьям.

Комментарий: *не скачивай и не открывай неизвестные тебе или присланные незнакомцами файлы из Интернета. Убедись, что на твоем компьютере установлено антивирусное программное обеспечение. Помни о том, что эти программы должны своевременно обновляться.*

3. Ты захотел скачать картинку в Интернете, нажал кнопку "скачать", на экране появилось сообщение отправить SMS на указанный номер в Интернете. Как тебе поступить?

1) Отправить SMS на указанный номер в Интернете.

2) Проверить этот номер в Интернете.

3) Не скачивать больше картинки.

Комментарий: *если хочешь скачать картинку или мелодию, но тебя просят отправить смс — не спеши! Сначала проверь этот номер в интернете — безопасно ли отправлять на него смс и не обманут ли тебя. Сделать это можно на специальном сайте.*

4. Ты познакомился в Интернете со сверстником, который приглашает тебя встретиться с тобой. Что ты будешь делать?

1) Пойдешь на встречу.

2) Пойдешь на встречу вместе с родителями.

3) Не пойдешь на встречу.

Комментарий: *не встречайся без родителей с людьми из Интернета вживую. В Интернете многие люди рассказывают о себе неправду.*

5. Новый друг, с которым ты познакомился вчера в Интернете, попросил тебя срочно сообщить ему такую информацию: номер телефона, домашний адрес, кем работают родители. Как ты поступишь:

1) Сообщишь ему нужные сведения.

2) Не сообщишь

3) Посоветуешься с родителями.

Комментарий: *никогда не рассказывай о себе незнакомым людям: где ты живешь, учишься, свой номер телефона. Это должны знать только твои друзья и семья!*

6. Ты решил опубликовать в Интернете свою фотографию и фотографии своих одноклассников. Можно ли это сделать?

1) Нет, нельзя.

2) Можно, с согласия одноклассников.

3) Можно, согласие одноклассников не обязательно.

7. У тебя появилось много друзей в Интернете. Вдруг стали приходить сообщения с неприятным, грубым содержанием. Что ты должен сделать?

1) Оскорбить обидчика.

2)Не отвечать обидчику тем же, а продолжить с ним общение.

3) Сообщить об этом взрослым.

8. На адрес твоей электронной почты стали часто приходить письма, многие из которых называются “спам”. Что это за письма?

1) Обычные письма, их можно открывать и читать.

2) Письма, в которых находится важная информация.

3) Письма, которые нельзя открывать и читать.