V Городской конкурс методических разработок по информатике
«Вернисаж педагогических идей»

Номинация
«Лучшая методическая разработка занятия
в дополнительном образовании»

КИБЕРБЕЗОПАСНОСТЬ: ЗАЩИТА ДАННЫХ

Автор: Наумова Елизавета Алексеевна, студентка,
Сургутский государственный педагогический университет

Введение

В современном мире, где цифровые технологии играют ключевую роль в повседневной жизни, вопросы кибербезопасности становятся всё более актуальными. С развитием Интернета и увеличением количества онлайн-сервисов, защита персональных данных и информационная безопасность становятся неотъемлемой частью жизни каждого человека. Особенно важно формировать у подрастающего поколения понимание основных угроз в сети и навыков их предотвращения.

Данное занятие направлено на то, чтобы познакомить обучающихся с основными понятиями кибербезопасности, научить их распознавать киберугрозы и применять меры защиты своих данных. В ходе занятия обучающиеся смогут не только получить теоретические знания, но и применять их на практике, участвуя в интерактивных играх, среди которых есть ролевая, и обсуждениях.

При разработке методического занятия был учтён тот факт, что тема достаточно актуальна, а само занятие практически значимо. Содержание методической разработки соответствует Федеральному государственному образовательному стандарту основного общего образования (ФГОС ООО) и поставленным целям и задачам. Занятие проводится дистанционно и предполагает совместную работу на онлайн-доске. Представленный материал является авторским и оригинальным. Стиль изложения конспекта доступный, наглядный и логичный. Соблюдено наличие региональной составляющей в ролевой игре. Используются современные информационные ресурсы (Zoom, МТС Link), при чем готовая онлайн-доска является авторской разработкой. Игры носят творческий характер и являются нестандартными решениями педагогической проблемы. Соблюдена культура оформления материалов, разработка соответствует нормам русского языка. Методическая разработка рассчитана на ее применение во внеурочной деятельности (при дополнительном образовании).

Эти критерии легли в основу структуры и содержания занятия, что позволяет рекомендовать его для использования в образовательных учреждениях.

Тема занятия: «Кибербезопасность: защита данных».

Класс: 8.

Цель занятия: формирование понятия информационной безопасности и умения защищать персональные данные.

Задачи занятия:

образовательные:

- ввести понятия кибербезопасности, основных киберугроз (вирусы, спам, фишинг);
- сформировать знания об основных угрозах в Интернете (вирусы, спам, фишинг) и способах защиты от них;

развивающие:

- развить умение взаимодействовать в команде при решении поставленных задач в рамках сетевого общения;
- способствовать развитию умения устанавливать причинно-следственные связи;

воспитательные:

- формировать умение использовать этические нормы и правила при организации сетевого общения;
- учиться слушать и слышать других.

Планируемые результаты:

- *предметные* – знания о кибербезопасности и наиболее распространенных угрозах в Интернете;
- *метапредметные* – решение проблемной ситуации; установление причинно-следственных связей; логическое мышление и способность к анализу информации;
- *личностные* – умение применять этические нормы и правила в общении.

Формы работы: индивидуальная, фронтальная, групповая.

Формат занятия: дистанционное занятие, рассчитанное на 6 человек.

Средства обучения: ПК, презентация MS PowerPoint, онлайн-доска МТС Link, Zoom (или другое средство связи).

Аппаратное обеспечение: системный блок, монитор, клавиатура, компьютерная мышь, микрофон, наушники/колонки.

Программное обеспечение: браузер, Zoom (или другая программа, обеспечивающая видеоконференцию).

ЦОР: заранее заготовленная онлайн-доска МТС Link.

План занятия

Деятельность учителя	Деятельность обучающихся	Используемые методы, приемы, формы, организации	Формируемые УУД (личностные, познавательны, регулятивные, коммуникативные)
1. Вводная часть (5 мин)			
Перед началом занятия готовит демонстрацию презентации и ссылку на онлайн-доску для дальнейшей совместной работы. Создает видеоконференцию и отправляет ссылку обучающимся. Ожидает их подключения и убеждается в том, что всё слышно и видно. – Здравствуйте! Предлагаю начать наше занятие с изображений, которые вы видите на слайде (Приложение 1). Можете назвать слово, которое объединяет их? Вводит тему занятия. – Сегодня мы поговорим о кибербезопасности и защите данных (Приложение 2). Знакомо ли вам данное слово? – А важна ли вообще кибербезопасность в наше время? Почему? – В таком случае, нужна ли она в повседневной жизни обычного человека? – А почему? Кибербезопасность, в основном, приписывают как деятельность технических специалистов. Зачем она нужна обычному человеку? – Вы действительно правы. Например, в 2023 году неизвестный хакер выложил в открытый доступ	Подключаются к видеоконференции по ссылке, предоставленной учителем. Включают видео и микрофон, убеждаются в том, что всё слышно и видно. Приветствуют учителя. Отвечают на вопросы учителя. – Кибербезопасность. – Да. / Нет – Важна, потому что везде есть риски взлома нашего аккаунта и мы должны знать, как обезопасить себя. / Не важна, потому что даже самые сложные системы кибербезопасности могут быть взломаны. – Да, нужна. – Нужна, потому что аккаунт любого человека уязвим к различным взломам. Каждый из нас должен быть готовым к ним и знать, как предотвратить их. Слушают учителя и осознают важность кибербезопасности. – Поговорим о кибербезопасности, о правилах информационной безопасности.	Фронтальная форма работы, постановка задачи, приведение реальных ситуаций.	*Личностные*: формирование учебной мотивации и целенаправленной познавательной деятельности. *Познавательные*: умение получать необходимую информацию. *Регулятивные*: предвосхищение результата и уровня усвоения знаний. *Коммуникативные*: умение формулировать грамотные речевые выражения.

личные данные около 3 млн пользователей Глория Джинс. Также это коснулось и пользователей магазинов «Твое», «Читай-город» и др. И такие случаи происходят всё чаще. – Исходя из этого, как думаете, чем мы займемся с вами на занятии? – Так и есть. Занятие будет посвящено кибербезопасности и информационной безопасности.			
2. Теоретическая часть (5 мин)			
– Можете сказать, что такое «кибербезопасность»? – Кибербезопасность – это совокупность методов и практик защиты от атак злоумышленников для компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных (Приложение 3). Стоит отметить, что это не просто технические меры, но и ответственное поведение в интернете. Среди распространенных киберугроз встречаются вирусы, спам, фишинг. Знакомы ли они вам? – Компьютерный вирус – это вредоносная программа, способная самостоятельно распространяться и заражать компьютеры, системы или сети. Он может выполнять различные вредоносные действия, такие как уничтожение, изменение или кража данных, блокировка работы компьютера или сети, перехват информации, нарушение работы аппаратной части и т. д. – Спам – это массовая рассылка сообщений без согласия получателя, а также размещение опасных	Отвечают на вопрос учителя. – Кибербезопасность – это безопасность в Интернете. – Да, знакомы. / Нет, не знакомы.	Фронтальная форма работы, работа с презентацией MS PowerPoint.	*Личностные*: выражение положительного отношения к процессу познания. *Регулятивные*: умение слушать в соответствии с целевой установкой; умение высказывать своё предположение. *Коммуникативные*: умение формулировать грамотные речевые выражения; умение выражать свои мысли, аргументировать свое мнение, убеждать и уступать, слушать собеседника. *Познавательные*: умение получать необходимую информацию.

вредоносных ссылок на веб-ресурсах. Сообщения распространяют через электронную почту, мессенджеры, SMS, сайты, форумы и соц. сети. – Фишинг – атаки, цель которых – обманом заполучить конфиденциальную информацию пользователя (например, данные банковских карт или пароли). Часто в ходе таких атак преступники отправляют жертвам электронные письма, представляясь официальной организацией.			
3. Ролевая игра «Охота за угрозами» (7 мин)			
– После того, как вы узнали о киберугрозах, предлагаю вам побыть в роли «экспертов» в игре «Охота за угрозами». Осуществляет переход на онлайн-доску. Делится ссылкой с обучающимися. Объясняет при необходимости особенности работы на ней. – Перед вами 3 ситуации, в каждой из которых предстоит выяснить, какая киберугроза была задействована, и предположить, как ее «устранить» (Приложение 4). Предлагаю совместно разобрать 1 ситуацию. Пока обучающиеся читают ситуацию, учитель кратко обозначает ее. Просит озвучить киберугрозу, как ее определили, и назвать действия, которые можно предпринять в данной ситуации для предотвращения киберугрозы. Убеждается в том, что все согласны. – Теперь вам предстоит в двух группах разобрать ситуации 2 и 3.	Осуществляют переход на онлайн-доску по ссылке. Слушают учителя, задают вопросы при необходимости. – Киберугроза в 1 ситуации – вирус, т. к. из-за него перестал нормально функционировать компьютер. Правильные стикеры: сообщить о проблеме системному администратору; установить антивирус; не заходить на незнакомые сайты / проверить соответствие официальному сайту. Делятся на две группы. Слушают инструкцию учителя. Выполняют задание в течение 3 минут. – Киберугроза во 2 ситуации: спам, т. к. это массовая рассылка сообщений без согласия получателя. Правильные стикеры: не переходить по ссылкам; подать жалобу; использовать спам-фильтры; не заходить на	Фронтальная, групповая формы работы, работа на онлайн-доске МТС Link, ролевая игра.	*Личностные*: выражение положительного отношения к процессу познания. *Коммуникативные*: умение формулировать грамотные речевые выражения. *Познавательные*: умение получать необходимую информацию; умение устанавливать причинно-следственные связи, строить логичные рассуждения и делать выводы, обобщать факты и понятия. *Регулятивные*: умение слушать в соответствии с целевой установкой; умение высказывать своё предположение.

Если у обучающихся есть пожелания по делению на группы, то учитель учитывает их. Иначе распределяет самостоятельно. – Выполняете по такому же принципу: читаете ситуацию, выясняете, что за киберугроза здесь представлена, и передвигаете в свое поле те стикеры, которые, как вам кажется, помогут устранить эту киберугрозу. Рекомендую воспользоваться функциями копировать-вставить, чтобы стикеры были в вашем поле. На это задание у вас 3 минуты. Сообщить о готовности вы можете с помощью реакций на этой доске.	незнакомые сайты / проверить соответствие официальному сайту. – Киберугроза в 3 ситуации: фишинг, т. к. здесь обманом хотят заполучить конфиденциальную информацию пользователя. Правильные стикеры: не переходить по ссылкам; использовать спам-фильтры; включить двухфакторную аутентификацию; использовать разные пароли.		
4. Игра «Киберпроверка» (10 мин)			
– Отлично! Вы умеете определять и устранять киберугрозу. Поэтому вы успешно справитесь со следующей игрой «Киберпроверка» (Приложение 5). Перед вами плакат по кибербезопасности, подготовленный обучающимися 8 класса. Но дело в том, что у них еще не было занятия по данной теме. Поэтому они создали плакат с ошибками. С помощью реакции обозначьте, где вы нашли ошибку. Обращает внимание на реакции обучающихся. Уточняет у них, что не так в отмеченных местах. Выборочно просит исправить ошибки на правильные предложения. Убеждается в том, что все согласны с исправлениями.	Слушают инструкцию учителя. Отмечают реакцией места, где допущены ошибки. По просьбе учителя комментируют их и исправляют на правильные утверждения. Убеждаются в том, что все ошибки исправлены и плакат носит правильную информацию.	Фронтальная, индивидуальная формы работы, работа на онлайн-доске МТС Link.	*Личностные*: выражение положительного отношения к процессу познания. *Коммуникативные*: умение формулировать грамотные речевые выражения. *Познавательные*: умение получать необходимую информацию; умение устанавливать причинно-следственные связи, строить логичные рассуждения и делать выводы, обобщать факты и понятия. *Регулятивные*: умение слушать в соответствии с целевой установкой; умение высказывать своё предположение.

– Вы большие молодцы! Надеюсь, информацию в данном плакате вы будете применять в жизни и не сталкиваться с киберугрозами.			
5. Подведение итогов (3 мин)			
– Подведем итоги и сформулируем правила информационной безопасности. Что нужно делать, чтобы обезопасить себя и свои личные данные? – Давайте я начну. Необходимо использовать надежные пароли и периодически их менять. Слушает ответы обучающихся. Отмечает их правильность. – Следуйте этим правилам и будьте бдительны. Ответственно подходите к тому, что выкладываете, ведь информация в Интернете остается и никуда не пропадает. – Как вы считаете, справились ли мы с поставленными в начале занятия задачами? – Хочу еще раз отметить тот факт, что кибербезопасность очень важна. Особенно в наше время. Это подтверждается тем, что правительство нашей страны предпринимает меры по внедрению курса Кибербезопасности в качестве урока в школах и других образовательных учреждениях. – На этом я завершаю занятие. Спасибо всем за работу! До свидания!	Слушают учителя и по очереди отвечают на его вопрос. – Не стоит разглашать личную информацию в Интернете; следует использовать антивирусные программы; нельзя полностью верить рекламным объявлениям; нужно опасаться незнакомцев; стоит использовать только официальные сайты; важно уметь распознавать злоумышленника и т. д. – Да. Слушают учителя и повторно осознают важность кибербезопасности. Прощаются с учителем.	Фронтальная формы работы, диалог.	*Личностные*: понимание значения знаний для человека и принятие его; способность к самооценке на основе критерия успешности учебной деятельности. *Регулятивные*: прогнозирование результатов уровня усвоения изучаемого материала; умение осуществлять итоговый контроль деятельности («что сделано») и пооперационный контроль («как выполнена каждая операция, входящая в состав учебного действия»); формирование адекватной самооценки. *Познавательные*: умение устанавливать причинно-следственные связи, строить логичные рассуждения и делать выводы, обобщать факты и понятия. *Коммуникативные*: умение формулировать грамотные речевые выражения.

Заключение

Представленная методическая разработка занятия по теме «Кибербезопасность: защита данных» обладает значительным потенциалом для интеграции в образовательный процесс. Её использование позволяет не только формировать у обучающихся знания о современных киберугрозах, но и развивать навыки безопасного поведения в цифровой среде.

Для эффективного применения разработки рекомендуется упрощать или усложнять задания в зависимости от уровня подготовки обучающихся, связать тему с другими дисциплинами, например, обществознанием или правом, чтобы занятие носило метапредметный характер. Немало важно обучить учителей работе с цифровыми инструментами и методике преподавания кибербезопасности. Также возможно использование различных средств связи, помимо Zoom. Онлайн-доска может быть любая другая, но предполагающая совместную работу на ней и с возможностью реакции.

Таким образом, методическая разработка занятия успешно формирует у обучающихся навыки безопасного поведения в цифровой среде. Разработка адаптивна и практикоориентирована.

Список использованной литературы:

1. УРОК ЦИФРЫ — всероссийский образовательный проект в сфере цифровых технологий. — Текст : электронный // Урок Цифры : [сайт]. — URL: https://урокцифры.рф/.

2. Федеральный государственный образовательный стандарт основного общего образования (Утвержден приказом Министерства образования и науки Российской Федерации от 17 декабря 2010 г. № 1897).

3. Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных».

4. Что такое кибербезопасность?. — Текст : электронный // Kaspersky : [сайт]. — URL: https://www.kaspersky.ru/resource-center/definitions/what-is-cyber-security.

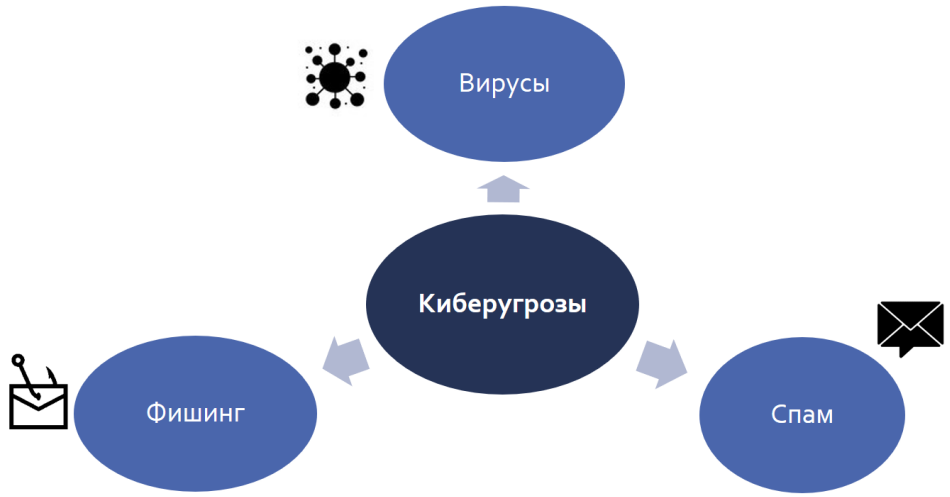
Приложения

Приложение 1

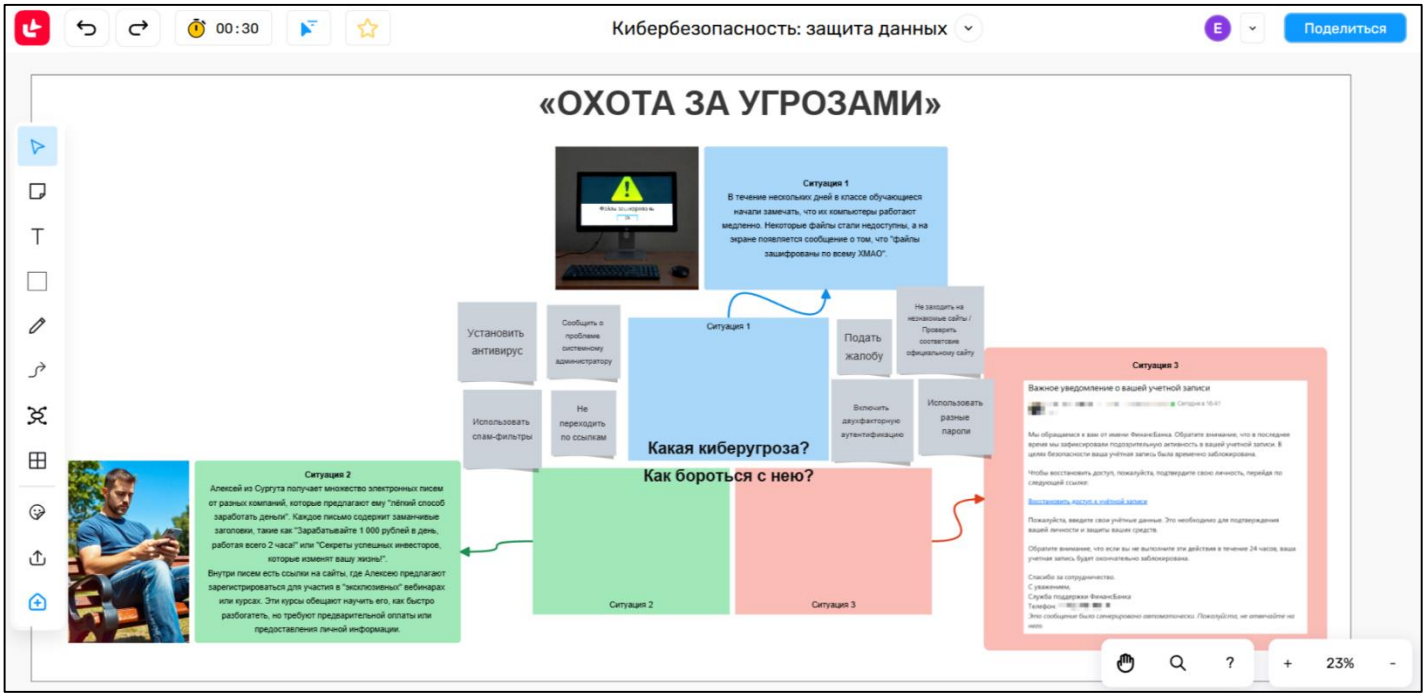
Приложение 2

Приложение 3

КИБЕРБЕЗОПАСНОСТЬ – это совокупность методов и практик защиты от атак злоумышленников для компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных.



Приложение 4



Приложение 5