Информационная безопасность детей:

эффективная система обучения педагогов и детей основам информационной безопасности в дополнительном образовании

Программа стажировки

День 1 | 30 сентября

10:30 – 11:30

Теоретическая часть: Актуальные угрозы и роль педагога в цифровой безопасности

11:40 – 13:00

Практикум: Формы и методы работы с детьми: квесты, игры, проекты

День 2 | 1 октября

10:30 – 11:10

Мастер-класс: Инфографика как инструмент педагога

11:20 – 12:30

Практикум: Создание авторской инфографики

12:30 – 13:00

Рефлексия: Итоги стажировки и планы внедрения

Джума Татьяна Александровна
методист, педагог дополнительного образования

Гончарова Алёна Юрьевна
педагог-организатор, педагог дополнительного образования

Голубятников Сергей Юрьевич
педагог дополнительного образования

Обзор актуальных угроз

Голубятников Сергей Юрьевич

педагог дополнительного образования

Классификация угроз

Угрозы, нацеленные на человека
Социальная инженерия, фишинг

Угрозы, нацеленные на устройство
Вредоносное ПО

Угрозы, нацеленные на данные и аккаунты
Взлом, утечки

Угрозы, нацеленные на каналы связи
Сетевые атаки

Угрозы, нацеленные на человека

Социа́льная инженерия – психологическое манипулирование людьми с целью совершения ими определенных действий или разглашения конфиденциальной информации.

От традиционного «мошенничества» отличается тем, что зачастую является одним из многих шагов в более сложной схеме мошенничества. Также может быть определена как побуждение другого человека к действию в чьих-либо интересах.

Угрозы, нацеленные на человека

- Фишинг
(текстовые способы подмены ссылок на вредоносные)
- Вишинг
(голосовой фишинг)
- Претекстинг
(“с подготовкой претекста” – злоумышленник придумывает легенду)
- Quid pro quo – “услуга за услугу”
(выгода или помощь в обмен на информацию)
- “Дорожное яблоко”
(носители, которые как бы случайно оставлены в общественном месте)
- Плечевой серфинг
(подглядывать из-за плеча)

Фишинг

Фи́шинг (англ. phishing от fishing «рыбная ловля, выуживание») – это способ интернет-мошенничества. Хакеры используют его, чтобы получить доступ к конфиденциальной информации других людей, например их учетным записям и данным банковских карт.

Фишинг

- общее или неофициальное приветствие;
- неожиданно выгодное предложение;
- подозрительные домен или почта отправителя;
- угрозы и запугивания;
- просьба действовать быстрее;
- ошибки в сообщениях;
- запрос личной информации.

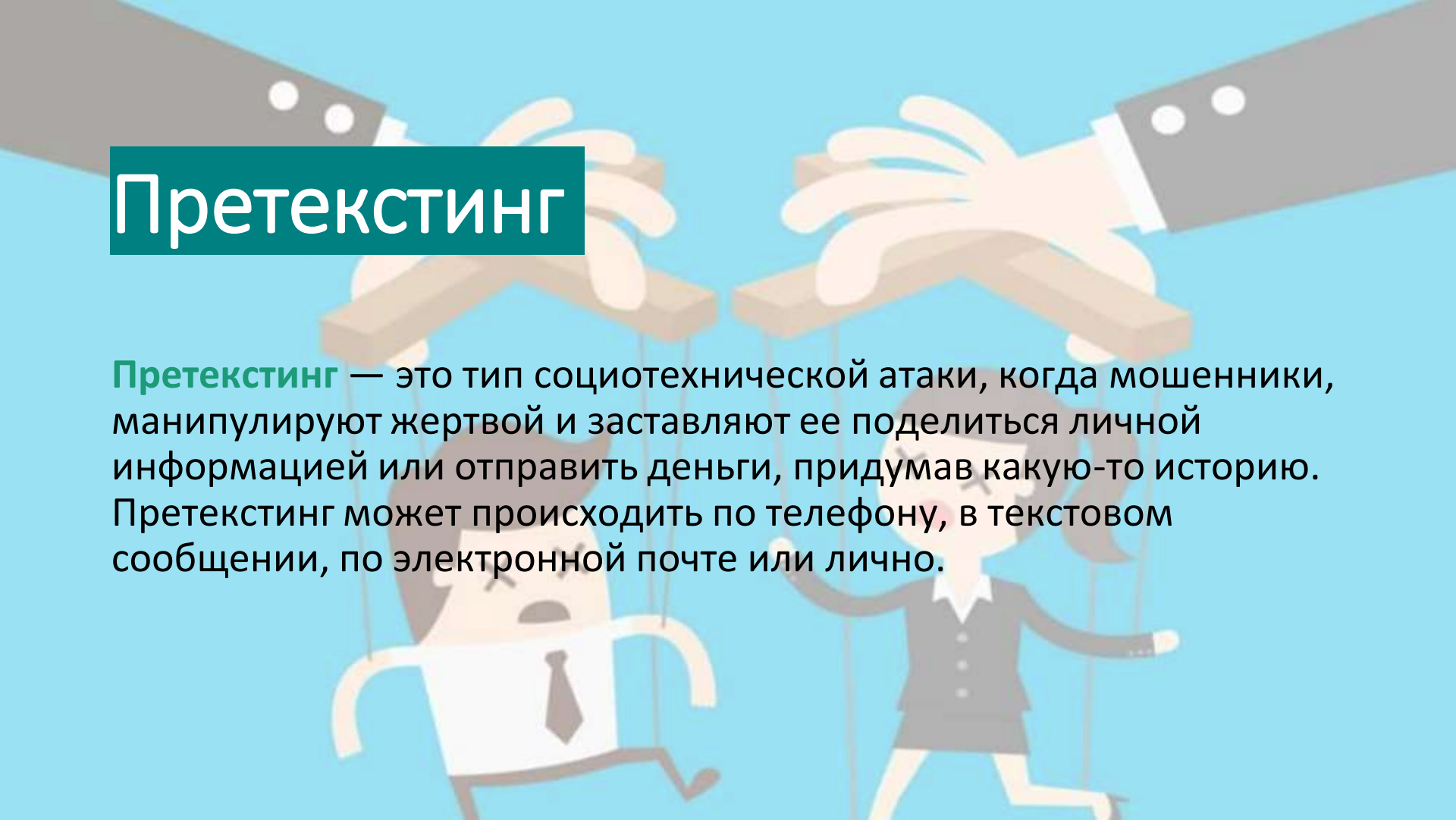
Вишинг

Телефонный фишинг – Вишинг (англ. vishing – voice fishing) назван так по аналогии с фишингом. Данная техника основана на использовании системы предварительно записанных голосовых сообщений с целью воссоздать «официальные звонки» банковских и других систем.

Вишинг

- маскировка мошенников под определенную организацию – банк, поставщика услуг, государственную организацию, сотрудника ИТ-службы;
- создание ощущения срочности или страха – угрозы, давление авторитетом, нагнетание обстановки.

Претекстинг



Претекстинг — это тип социотехнической атаки, когда мошенники, манипулируют жертвой и заставляют ее поделиться личной информацией или отправить деньги, придумав какую-то историю. Претекстинг может происходить по телефону, в текстовом сообщении, по электронной почте или лично.

Претекстинг

- внезапные и срочные запросы на получение личной информации или денег;
- предложения, слишком хорошее, чтобы быть правдой (деньги, отпуск, подарки, предложения о работе и т. д.);
- нежелательные телефонные звонки, особенно из государственного учреждения;
- грамматические и орфографические ошибки.

Quid pro quo

Квид про кво (от лат. Quid pro quo — «то за это») — в английском языке это выражение обычно используется в значении «услуга за услугу».

Данный вид атаки подразумевает обращение злоумышленника в компанию по корпоративному телефону или электронной почте. Зачастую злоумышленник представляется сотрудником, который сообщает о возникновении каких-либо проблем на рабочем месте сотрудника и предлагает помощь в их устранении.

Quid pro quo

- Предложение помощи – мошенник представляется IT-специалистом, сотрудником службы поддержки или даже коллегой.
- Создание доверия – предлагает «решить проблему» (например, «обновить ПО», «исправить ошибку в системе»).
- Требование взамен – просит логин/пароль, доступ к компьютеру (удалённый доступ, демонстрация экрана) или личные данные.

Дорожное яблоко

Этот метод атаки представляет собой адаптацию троянского коня, и состоит в использовании физических носителей. Злоумышленник может подбросить инфицированный CD, или флэш, в месте, где носитель может быть легко найден (туалет, лифт, парковка). Носитель подделывается под официальный,
и сопровождается подписью, призванной вызвать любопытство.

Плечевой серфинг

Плечевой серфинг (англ. shoulder surfing) включает в себя наблюдение личной информации жертвы через её плечо. Этот тип атаки распространён в общественных местах, таких как кафе, торговые центры, аэропорты, вокзалы, а также в общественном транспорте.

Плечевой серфинг

Плечевой серфинг (англ. shoulder surfing) включает в себя наблюдение личной информации жертвы через её плечо. Этот тип атаки распространён в общественных местах, таких как кафе, торговые центры, аэропорты, вокзалы, а также в общественном транспорте.

Угрозы, нацеленные на устройство

Вирусы и черви: Самораспространяющиеся программы.

Трояны: Маскируются под легитимный софт.

Программы-шпионы (Spyware): Крадут данные без ведома пользователя.

Рекламное ПО (Adware): Показывают навязчивую рекламу.

Рансомвер (Ransomware): Шифруют данные и требуют выкуп.

Кейлоггеры (Keyloggers): Записывают все нажатия клавиш.

Источники

- **Фишинговые электронные письма:** Злоумышленники рассылают письма, маскирующиеся под сообщения от известных отправителей, с вредоносными вложениями или ссылками.
- **Вредоносная реклама:** Появление рекламы на веб-сайтах, ведущей на зараженные ресурсы или предлагающей установить вредоносное ПО.
- **Поддельные сообщения и предупреждения:** Всплывающие окна или сообщения, имитирующие системные оповещения, предлагающие загрузить ложные "антивирусы" или обновления.
- **SMS и мессенджеры:** Заражение через сообщения, которые содержат вредоносные ссылки или вложения.

Угрозы, нацеленные на данные и аккаунты

- Взлом учетных записей
- Утечка данных

Подбор паролей, использование утекших данных

Брутфорс
— это метод взлома, при котором злоумышленник систематически перебирает все возможные комбинации символов (пароли, ключи, логины), пока не найдет правильную.

Этот метод является одним из старейших и наиболее простых, но может занять много времени, которое зависит от сложности пароля.

Перехват сеансов

- **Перехват сеансов** – это кибератака, в ходе которой злоумышленники перехватывают и крадут идентификатор сеанса, также называемый токеном сеанса, который передается между пользователем и веб-сайтом. С помощью украденного идентификатора сеанса злоумышленники могут выдать себя за пользователя и получить доступ к учетной записи.

Угрозы, нацеленные на каналы связи

- Атаки "человек посередине" (Man-in-the-Middle): Перехват трафика между жертвой и сайтом/сервисом (например, в публичных Wi-Fi).
- Поддельные Wi-Fi точки доступа (Evil Twin).
- Отказ в обслуживании (DDoS-атаки): Наводнение сайта или сервера мусорным трафиком, чтобы сделать его недоступным.

Противостояние киберугрозам

Используйте надежные и уникальные пароли для каждой учетной записи

1. Используйте длинные и сложные пароли (лучше 14+ символов);
2. Используйте менеджеры паролей для генерации и хранения вместо сохранения в браузере (если браузер не поддерживает мастер-пароль);
3. Придумывайте уникальные пароли (так один «утекший» аккаунт не повлияет на десятки или даже сотни других), не содержащие личной информации, например имени или даты рождения питомца, вы значительно усложните злоумышленникам доступ к вашим учетным записям.

Современные видеокарты могут проверять миллионы паролей в секунду, а ниже небольшая оценка классического перебора для разных вариантов:

- подбор пароля **123456** (10^6, миллион вариантов) происходит **мгновенно**,
- пароль **password123** (10^{12}) займёт пару секунд **2 секунды**,
- **p@ssW0rD!2024** (10^{20}) порядка **5 лет** (хотя выглядит так, будто мог попасть в базу готовых словарей),

а вот пароль вроде **u6$F1g!rL$93*k** (10^{32}) будет взламываться **миллионы или миллиарды лет**.

Противостояние киберугрозам

Включите многофакторную аутентификацию там, где это возможно

Многофакторная аутентификация (MFA) — это дополнительная мера безопасности, которую следует принять для защиты учетных записей в Интернете. Если включена многофакторная аутентификация, необходимо предоставить дополнительное подтверждение личности для доступа к учетным записям. Это затруднит доступ к вашим учетным записям мошенникам, даже если у них будут ваши учетные данные для входа в систему, поскольку у них будет отсутствовать дополнительная форма аутентификации.

Противостояние киберугрозам

Не предоставляйте личную информацию

Не сообщайте свою (или чужую) личную информацию ни по телефону, ни в сообщениях. Даже если вы считаете, что человек, с которым вы говорите, заслуживает доверия, как это обычно бывает в случае мошенничества с пожилыми людьми, всегда следует соблюдать осторожность.

Кроме того, стоит помнить, что безопасность персональных данных защищает ФЗ 152 – это закон РФ «О персональных данных», который устанавливает правила их обработки, хранения и защиты для всех организаций и граждан. Основные требования включают получение согласия на обработку, обеспечение безопасности данных, их регистрацию в Роскомнадзоре как оператора данных и ответственность за их защиту от утечек и несанкционированного доступа.

Противостояние киберугрозам

Сохраняйте цифровой след в чистоте

Чтобы сохранить свой цифровой след в чистоте, можно выполнить ряд простых действий, которые уменьшат риск стать мишенью для мошенников:

- Удалите все учетные записи, которые больше не используются
- Избегайте чрезмерного распространения информации в социальных сетях
- Обновите настройки конфиденциальности, чтобы уменьшить цифровой след в различных учетных записях или приложениях

Противостояние киберугрозам

Использование актуальных антивирусных программ

Не пренебрегайте установкой антивирусных программ и своевременным обновлением их баз для обнаружения новых угроз, поскольку они обеспечивают защиту в реальном времени, используют поведенческий анализ и защиту от фишинга/веб-угроз, а также блокируют и удаляют вредоносное ПО до нанесения ущерба системе.

Без актуальных обновлений антивирус теряет эффективность против новых, быстро распространяющихся угроз.

Противостояние киберугрозам

Избегайте общедоступных сетей Wi-Fi

Общедоступная сеть Wi-Fi небезопасна, и злоумышленники могут легко перехватить сеансы с помощью атак через посредника. Постарайтесь вообще не пользоваться общедоступными сетями Wi-Fi.

Не открывайте подозрительные сообщения и сайты

Контролируйте активность своих банковских и кредитных счетов

Регулярно проверяйте свои счета на наличие подозрительной деятельности. Это может помочь обнаружить деятельность злоумышленников, прежде чем они нанесут значительный финансовый ущерб или навредят вашей репутации. Установите лимиты для различных операций, чтобы предотвратить любые злонамеренные действия с вашими деньгами.

А как проверить?

🔍 Have I Been Pwned

Этот бесплатный сервис подскажет, не попали ли ваши данные в общий доступ. Все, что нужно сделать, — ввести свою почту.

https://haveibeenpwned.com

🔐 Mozilla Monitor

Сервис проанализирует все слитые в сеть базы данных и предупредит, если ваша почта и аккаунты в соцсетях скомпрометированы. Чтобы это узнать, понадобится зарегистрироваться. Работает бесплатно.

https://monitor.mozilla.org

 Safe Surf

Бесплатно покажет, попали ли ваша почта, номер телефона и логин в свободный доступ, а также по чьей вине это произошло.

https://chk.safe-surf.ru

Кибербуллинг: онлайн-травля и как с ней бороться

- Кибербуллинг – это форма травли, которая происходит в цифровом пространстве. Это может быть оскорбление, угрозы, распространение личной информации, создание фейковых аккаунтов и многое другое.

- Почему кибербуллинг так опасен? Потому что он может преследовать жертву 24/7, затрагивая ее психологическое состояние, самооценку и даже физическое здоровье.

Кибербуллинг

Как распознать кибербуллинг? Обратите внимание на признаки:

- Ребенок/подросток становится более замкнутым и раздражительным.
- Он избегает использования компьютера или телефона.
- Он испытывает трудности со сном и аппетитом.
- Он получает странные сообщения или звонки.

Что делать, если вы стали жертвой кибербуллинга?

- Не отвечайте обидчику.
- Сохраните все доказательства.
- Сообщите о случившемся родителям, учителям или другим доверенным лицам.
- Заблокируйте обидчика.
- Обратитесь за помощью к психологу.

Обзор актуальных угроз

Голубятников Сергей Юрьевич

педагог дополнительного образования

Роль педагога в цифровой безопасности детей

Гончарова Алёна Юрьевна,
педагог-организатор,
педагог дополнительного образования


ИНФОРМАЦИОННАЯ
БЕЗОПАСНОСТЬ
И
ЦИФРОВАЯ ГИГИЕНА

Департамент образования и науки города Москвы

Государственное бюджетное
образовательное учреждение дополнительного образования города Москвы
«Центр детского творчества «Ново-Переделкино»

Методическая разработка для педагогов

«Цикл семинаров-практикумов по обучению детей основам информационной безопасности»

1. Создание безопасного профиля

Целевая аудитория: дети от 12 до 17 лет.

Формат: семинар.

Цель: формирование сознательного использования личной информации.

Задачи:

- объяснить важность защиты личной информации в сети Интернет и ограничить ее распространение;

- рассказывать о рисках предоставления личной информации незнакомцам в сети Интернет.

Оборудование: флипчарт, бумага для флипчарта, бумага по количеству присутствующих, пишущие принадлежности.

Ход мероприятия:


БЕЗОПАСНОЕ ОБЩЕНИЕ
В ИНТЕРНЕТЕ
И СОЦИАЛЬНЫХ СЕТЯХ


ТЕХНОЛОГИЧЕСКИЕ АСПЕКТЫ
ЗАЩИТЫ ДЕТЕЙ ОТ
НЕЖЕЛАТЕЛЬНОГО КОНТЕНТА В
СЕТИ ИНТЕРНЕТ


CYBERHUB
PHDAYS FEST
PHDAYS FEST


28 ЛЕТ
ОБУЧАЕМ:
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ИНФОРМАЦИОННЫМ ТЕХНОЛОГИЯМ
КОРПОРАТИВНОЙ БЕЗОПАСНОСТИ
ЭЛЕКТРОННОМУ ДОКУМЕНТООБОРОТУ
ИМПОРТОЗАМЕЩЕНИЮ
АИС


PHDAYS FEST
МЫ ДОЛГО НЕ ВИДЕЛИ ПРОБЛЕМЫ

kaspersky

Что прячется в смартфоне: исследуем мобильные угрозы

ПРОХОЖДЕНИЙ: 2 086 379

Ученику | Учителю | Роди

kaspersky

Кибербезопасность будущего

ПРОХОЖДЕНИЙ: 3 615 532

Отправляйтесь в 2050 год и помогите героям обезопасить умный дом и даже умный город! Узнайте, как противостоять самым разным кибератакам, которые нас могут ожидать в будущем и встречаются уже сейчас.

Ученику | Учителю | Родителю

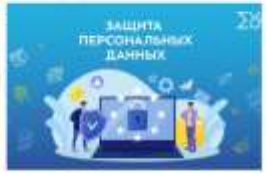
ТРЕ

1–
5–
9–

ВИДЕО

Анонимность в интернете | Кибербезопасность

Виды мошенничества | Кибербезопасность



Защита персональных данных | Кибербезопасность

БОЛЬШЕ ВИДЕО

Роль педагога в цифровой безопасности детей

Гончарова Алёна Юрьевна,
педагог-организатор,
педагог дополнительного образования

Формы и методы работы с детьми

Джума Татьяна Александровна

методист, педагог дополнительного образования

Практикум
Анализ и адаптация форм работы по информационной безопасности

Цель: Проанализировать предложенные форматы образовательной деятельности и предложить варианты их улучшения для разных возрастных групп детей.

Формат работы: Работа в парах.

Время на выполнение: 30 минут.

Время на презентацию: 2-3 минуты для каждой пары.

Задание

1. **Определите целевую аудиторию.**
   Проанализируйте каждую из предложенных форм и определите, для какой возрастной группы она подходит лучше всего:
   1. Младшие школьники (1-4 класс)
   2. Средние школьники (5-8 класс)
   3. Старшие школьники (9-11 класс)
2. **Сформулируйте образовательную задачу.**
   Ответьте на вопрос: Какую **конкретную задачу по информационной безопасности** решает данный сценарий?
   Например: «Научить распознавать фишинговые ссылки», «Сформировать навык создания надежного пароля», «Отработать алгоритм действий при столкновении с кибербуллингом».
3. **Предложите улучшение.**
   Придумайте и запишите **одно небольшое изменение** в сценарий. Это изменение должно:
   1. либо повысить его эффективность для заявленной аудитории,
   2. либо адаптировать его для другой возрастной группы.

Пример карточки и её решения

- **Форма:** Квест «Тайна цифрового города»
- **Сценарий:** Дети, проходя станции, разгадывают головоломки: определяют мошеннические сайты, придумывают сложные пароли, расшифровывают сообщения с правилами сетевого этикета.
- **Целевая аудитория:** Средние школьники (5-8 класс)
- **Образовательная задача:** Сформировать практические навыки распознавания фишинговых сайтов, создания стойких паролей и применения базовых правил сетевого этикета.
- **Предлагаемое изменение:** Для адаптации под старших школьников (9-11 класс) можно добавить станцию, посвященную основам двухфакторной аутентификации и биометрии, где нужно будет выбрать наиболее безопасный метод защиты для разных ситуаций (соцсеть, банкинг, почта).

Формы и методы работы с детьми

Джума Татьяна Александровна
методист, педагог дополнительного образования

Программа стажировки

День 1 | 30 сентября

10:30 – 11:30

Теоретическая часть: Актуальные угрозы и роль педагога в цифровой безопасности

11:40 – 13:00

Практикум: Формы и методы работы с детьми: квесты, игры, проекты

День 2 | 1 октября

10:30 – 11:10

Мастер-класс: Инфографика как инструмент педагога

11:20 – 12:30

Практикум: Создание авторской инфографики

12:30 – 13:00

Рефлексия: Итоги стажировки и планы внедрения