Государственное учреждение образования
«Средняя школа № 12 имени В.В.Бабко г. Гродно»

Номинация
«Разработка внеклассного мероприятия
с применением технологий ИИ в ходе его проведения»

# Музей кибербезопасности

**Подготовила**
Сулима Карина Олеговна,
заместитель директора по учебной работе, учитель математики первой квалификационной категории
karinayakovenko578@gmail.com
+375291223674

***Ключевая идея:*** формирование основ цифровой грамотности и кибербезопасности.

***Целевая аудитория:*** учащиеся 5 – 6 класса.

***Форма проведения:*** командная проектно-творческая мастерская в рамках классного/информационного часа, тематических мероприятий, предметных недель.

***Продолжительность:*** 45 минут

***Актуальность мероприятия:*** с малых лет ребята начинают использовать сеть Интернет, но далеко не всегда обладают необходимым уровнем цифровой грамотности. Традиционные формы обучения: лекции, беседы, рассказы, как правило, не вызывают эмоционального отклика и быстро забываются. Вместе с тем, абстрактные понятия, такие как, «фишинг», «социальная инженерия», «двухфакторная аутентификация», «дипфейк», являются сложными для восприятия. Превращение их в изображения позволяет сформировать запоминающийся образ.

***Обоснование выбора форм и методов работы:*** выбор форм и методов продиктован возрастом учащихся (10–13 лет). В этом возрасте уже не интересны просто «картинки», а сложные лекции ещё не воспринимаются на должном уровне. Ребятам важно общаться друг с другом, чувствовать себя значимыми и видеть результат своих действий. Используемые методы в ходе мероприятия направлены на достижение главной цели: не просто запомнить правила, а пропустить их через себя, через творчество, через командное взаимодействие. Китайская пословица гласит: «Расскажи мне – и я забуду, покажи – и я запомню, дай попробовать – и я пойму».

***Цель:*** сформировать у учащихся представление об основных угрозах в цифровой среде и способах защиты через создание коллективного творческого проекта с использованием технологий искусственного интеллекта.

***Задачи:***

закрепить знания о ключевых понятиях кибербезопасности: фишинг, сложный пароль, двухфакторная аутентификация, социальная инженерия, вирусы, дипфейки;

научить формулировать точные запросы для нейросетей;

развить коммуникативные навыки в ходе командной работы и публичной презентации (экскурсии);

сформировать ответственное отношение к собственной цифровой безопасности.

***Ожидаемый результат:***

учащиеся осознают ценность цифровой безопасности и свою ответственность за сохранность личных данных;

учащиеся могут объяснить смысл понятий: фишинг, социальная инженерия, двухфакторная аутентификация, сложный пароль, дипфейк.

***Используемые инструменты ИИ:***

Графический ИИ (Шедеврум, PixVerse.AI, Leonardo.AI) для генерации экспонатов.

Текстовый ИИ (YandexGPT, GigaChat, ChatGPT) для генерации этикеток.

## Ход мероприятия

***Введение. Организационно–мотивационный этап (5 минут)***

Учитель: Ребята, представьте себе, что мы перенеслись в 2037 год. Открылся новый музей – МУЗЕЙ КИБЕРБЕЗОПАСНОСТИ. Каждый экспонат рассказывает историю о том, какие способы защиты использовали люди в цифровом мире.

Сегодня у нас важная миссия: создать экспонаты для музея, которые помогут посетителям понять, что такое фишинг, почему важен сложный пароль и как работает двухфакторная аутентификация. Помогать нам в работе будет искусственный интеллект (ИИ), он станет нашим графическим дизайнером и редактором. Но помните: ИИ исполняет наши идеи, а не придумывает их за нас. Идейные вдохновители и творческие личности – ВЫ.

***Распределение ролей, вводный инструктаж (5 минут)***

Класс делится на команды по 3 – 4 человека в каждой. Каждая команда получает карточку с темой музейного экспоната (можно использовать жеребьёвку).

***Тема экспоната и суть угрозы/защиты:***

*«Фишинг»:* злоумышленники могут создать подделку сайта, очень-очень похожую внешне на официальный сайт, а его URL-адрес (символы, которые вводятся в адресную строку браузера) будет отличаться всего на одну букву или цифру. Мошенники надеются, что человек, ничего не подозревая, введет свои данные на таком сайте, а они получат их. Недаром *«*фишинг*»* в переводе с английского значит *«*рыбалка*»*.

*«Сложный пароль»:* разница между простым (легко взломать) и сложным (надежным) паролем;

*«Двухфакторная аутентификация»:* это метод идентификации пользователя в каком-либо сервисе (как правило, в Интернете) при помощи запроса аутентификационных данных двух разных типов, что обеспечивает двухслойную, а значит, более эффективную защиту аккаунта от несанкционированного проникновения. На практике это обычно выглядит так: первый рубеж – это логин и пароль, второй – специальный код, приходящий по SMS или электронной почте.

*«Социальная инженерия»:* способ получения конфиденциальной информации с помощью психологического воздействия на человека. Основной целью социальной инженерии является получение выгоды через доступ к паролям, банковским данным и другим защищенным системам.

*«Дипфейк»:* это результат работы нейросети, которая учится копировать внешность, мимику и голос человека. Для этого используются фотографии,

видео и аудиозаписи, которые есть в открытом доступе: в соцсетях, на видеохостингах или в мессенджерах.

***В ходе совместной работы команды создают продукт, который оформляют в виде презентации в PowerPoint или буклет/листовку. Содержание:***

Экспонат (изображение), созданный с помощью графического ИИ, который передает суть темы.

Этикетка – краткое описание, созданное с помощью текстового ИИ, включающее: название, материал, год создания, описание угрозы и способ защиты.

Устное представление экспоната (экскурсия) продолжительностью до 1 минуты.

***Этап 3. Создание экспоната (работа с графическим ИИ) – 15 минут***

Учитель напоминает правила работы с графическим ИИ: промпт должен быть конкретным, содержать описание объекта, детали, стиль, атмосферу. Учитель оказывает помощь, при необходимости, командам, которые испытывают трудности с формулировкой запроса.

***Памятка для учащихся «Как создать промпт для нейросети»***

Хороший промпт состоит из 4 частей:

1. Что рисуем? (объект, сцена)
2. Какие детали? (что на удочке, какие надписи)
3. Какой стиль? (сюрреализм, мультяшный)
4. Какая атмосфера? (цвета, освещение, настроение)

Плохой промпт: «Нарисуй рыбу».

Хороший промпт: «Нарисуй скульптуру в виде гигантской рыбы из темного металла. Рыба держит удочку, на крючке - смартфон с надписью "Введи пароль". Стиль – темный фон, синяя подсветка».

Команда обсуждает, какой образ лучше всего передаст их тему. Например, для «Фишинга» – рыба с удочкой и телефоном на крючке.

***Примеры промптов для разных тем (Готовые изображения ПРИЛОЖЕНИЕ 1):***

*Фишинг:* Нарисуй музейный экспонат в виде скульптуры: огромная рыба из темного металла держит удочку. На крючке удочки – смартфон с ярким экраном. Вокруг рыбы – волны из цифр.

*Сложный пароль:* Изобрази музейный экспонат: два замка рядом. Один – маленький, ржавый, с надписью "123", он сломан и открыт. Второй – очень большой, состоящий из символов @ # $ и цифр.

*Двухфакторная аутентификация:* Изобрази дверь из стекла и металла. Дверь закрыта на два разных замка: один – обычный замок, второй –светящийся цифровой дисплей с кодом.

*Социальная инженерия:* Изобрази скульптуру в виде театральной маски. Половина маски - улыбающееся, доброе лицо с надписью Выигрыш!. Вторая половина – разорванная, надпись Твои данные.

*Дипфейк:* Изобрази зеркало, в котором отражается человек, но отражение имеет искажения (глаза светятся неестественным светом).

***Этап 4. Создание этикетки (работа с текстовым ИИ) – 8 минут***

Учитель объясняет, что этикетка для экспоната должна быть краткой, но информативной. Она включает: название, «материал» (фантазийный, например, «цифровая сталь», «квантовый пластик»), описание угрозы и способ защиты.

Пример промпта для текстового ИИ (для темы «Фишинг»): Напиши этикетку для музейного экспоната фишинг. Экспонат представляет собой скульптуру рыбы с удочкой и смартфоном на крючке. Укажи: название экспоната, материал, описание угрозы (что такое фишинг и как он работает), способ защиты (как не попасться на фишинг).

***Пример результата (сгенерировано в AlisaAI):***

Название экспоната: «Фишинг: улов для неосторожных»

Материал: полимерная глина, металл (элементы удочки), пластик (смартфон-муляж).

Скульптура изображает рыбу, вооружённую удочкой, на крючке которой висит смартфон. Композиция – метафора современного вида мошенничества: злоумышленники «закидывают удочку» в цифровое пространство, а в роли добычи выступают личные данные и финансы пользователей.

*Что такое фишинг и как он работает?*

Фишинг – вид интернет-мошенничества, цель которого – получить доступ к конфиденциальным данным пользователей: логинам, паролям, данным банковских карт и т.д.

*Типичные приёмы:*

срочные предупреждения («ваш счёт заблокирован!»);

предложения «выигрыша» или «подарка»;

ссылки с опечатками в названии домена (например, g00gle.com вместо google.com);

вложения с вредоносным ПО.

*Как не попасться на фишинг?*

Проверяйте отправителя. Внимательно изучите адрес электронной почты или номер телефона. Официальные организации редко пишут с личных адресов.

Не переходите по подозрительным ссылкам. Наведите курсор на ссылку, чтобы увидеть реальный адрес. Если он выглядит странно — не кликайте.

Не вводите личные данные по ссылке из сообщения. Зайдите на сайт организации вручную (через поисковик или сохранённую закладку).

Будьте осторожны с вложениями. Не открывайте файлы из писем от неизвестных отправителей.

Используйте двухфакторную аутентификацию (2FA). Даже если мошенники получат ваш пароль, без второго фактора доступа они не смогут войти в аккаунт.

***Этап 5. Экскурсия – презентация экспонатов (10 минут)***

Учитель объявляет начало экскурсии. Каждая команда делегирует одного «экскурсовода». Учитель может выступать в роли «директора музея», представляя экскурсоводов.

Экскурсовод знакомит с экспонатом, демонстрируя готовый продукт (презентация, буклет). В конце защиты учитель просит добавить 1–2 предложения от себя: почему эта тема важна именно для школьников.

*Пример выступления:* Добро пожаловать в музей безопасности! Перед вами экспонат «Фишинг: улов для неосторожных». Он создан из полимерной глины в 2037 году. Этот экспонат показывает, как мошенники «ловят» пользователей на крючок. Посмотрите: смартфон на удочке – это приманка. А способ защиты очень прост: никогда не переходите по ссылкам из подозрительных сообщений. Даже если очень хочется получить приз!

***Этап 6. Рефлексия и подведение итогов (2 минуты)***

Учитель: сегодня мы создали не просто картинки, а целый музей, который может рассказать о том, как важно быть внимательным в сети Интернет. Искусственный интеллект помог нам, но главные идеи придумали ВЫ. Помните: ИИ – это инструмент, а ваше критическое мышление и креативность – это то, что делает вас настоящими мастерами безопасности.

Учитель проводит рефлексию:

«Какой экспонат вам запомнился больше всего и почему?»

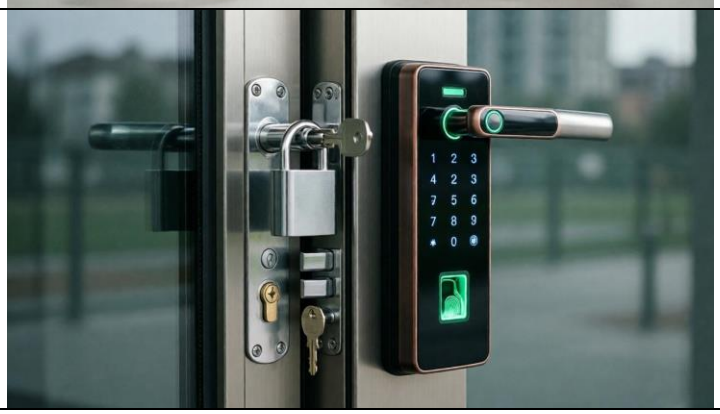
«Было ли сложно придумывать образы для угроз? Что помогало?»

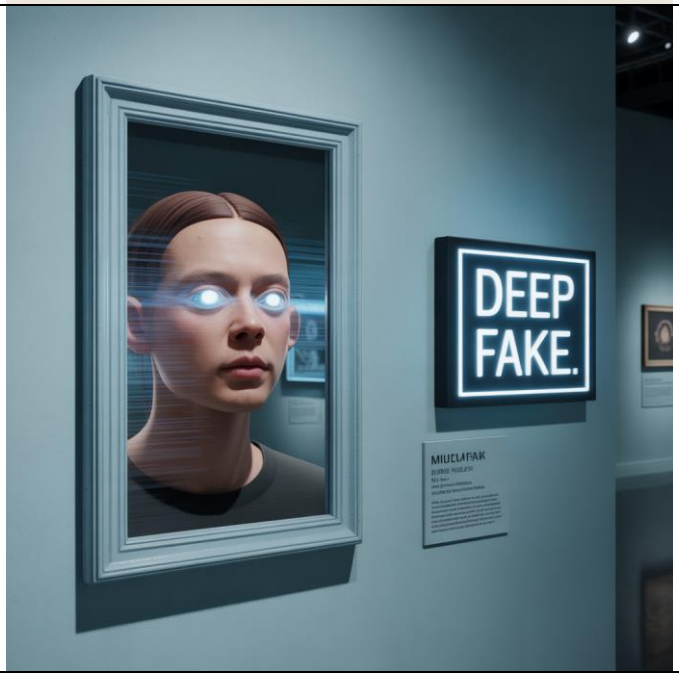
«Как вы думаете, почему важно уметь правильно формулировать запросы для ИИ?»

«Какое правило кибербезопасности запомнилось каждому из вас?»

ПРИЛОЖЕНИЕ 1

***Примеры готовых изображений экспонатов***

| | | |
|---|---|---|
| Фишинг |  | Изображение создано с помощью PixVerse.AI |
| Сложный пароль |   | Изображение создано с помощью PixVerse.AI |
| Двухфакторная аутентификация |  | Изображение создано с помощью PixVerse.AI |

| | | |
|---|---|---|
| Социальная инженерия |  | Изображение создано с помощью Leonardo.AI |
| Дипфейк |  | Изображение создано с помощью Leonardo.AI |

**Список используемой литературы**


1. Промты для нейросети: полезные советы по созданию запроса. – [Электронный ресурс]. Режим доступа: https://hi-tech.mail.ru/review/109596-promty-dlya-neyroseti/#anchor171508230954260805 – Дата доступа: 20.03.2026.
2. Фишинг – [Электронный ресурс]. Режим доступа: https://www.fingramota.by/ru/guide/anti-fraud/phishing – Дата доступа: 20.03.2026.
3. Двухфакторная аутентификация: что это и зачем оно нужно? – [Электронный ресурс]. Режим доступа: https://www.kaspersky.ru/blog/what_is_two_factor_authenticatio/4272/ – Дата доступа: 20.03.2026.
4. Что такое социальная инженерия? – [Электронный ресурс]. Режим доступа: https://www.fingramota.by/ru/guide/practical/breaking-into – Дата доступа: 20.03.2026.
5. Дипфейки: как не попасться на цифровую подделку – [Электронный ресурс]. Режим доступа: https://media.mgddm.by/%D0%BC%D0%B5%D0%B4%D0%B8%D0%B0%D1%88%D0%BA%D0%BE%D0%BB%D0%B0/%D0%BC%D0%B5%D0%B4%D0%B8%D0%B0%D0%B3%D1%80%D0%B0%D0%BC%D0%BE%D1%82%D0%BD%D0%BE%D1%81%D1%82%D1%8C/%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C/document-75403.html – Дата доступа: 20.03.2026.