



НИЦМП

Научно-исследовательский центр мониторинга и профилактики деструктивных проявлений  
в образовательной среде ГБУ ДПО ЧИРПО

## **МЕТОДИЧЕСКИЙ КОМПЛЕКС ПО ОБРАЗОВАТЕЛЬНОЙ ИГРЕ «МЕДИАРИНГ»**

### **ПОЯСНИТЕЛЬНАЯ ЗАПИСКА**

Современные обучающиеся – это цифровое поколение, которое знакомо с разными стилями обучения, у этого поколения новое отношение к образовательному процессу и более высокие требования к преподаванию и обучению. Преподаватели сталкиваются с совершенно новыми проблемами и вопросами, связанными с адаптацией учебного процесса к нуждам, предпочтениям и требованиям учащихся, при этом возникает необходимость использовать принципиально новые методы и подходы к обучению, которые формируют у обучающихся более сильную мотивацию и вовлеченность в решение образовательных задач. Одним из таких методов стала технология геймификации, набирающая все большую популярность в связи с тем, что традиционные подходы к образовательной и воспитательной деятельности постепенно устаревают.

Геймификация – это применение игровой механики в неигровом контексте для поощрения желаемого поведения и достижения результатов обучения. Геймификация использует естественные склонности людей к конкуренции, соревнованиям, сотрудничеству и достижениям через использование игрового мышления, подходов и элементов в условиях образовательной и воспитательной деятельности. Одним из инструментов технологии геймификации является методическая разработка «Медиаринг», подготовленная сотрудниками Научно-исследовательского центра мониторинга и профилактики деструктивных проявлений в образовательной среде и направленная на формирование у обучающихся навыков медиаинформационной грамотности и критического мышления.

За основу методической разработки взят принцип телевизионной игры «Брейн-ринг», где две команды игроков одновременно отвечают на один и тот же вопрос, причем правильно ответившая первой команда лишает соперника возможности ответить на этот же вопрос. Игра рассчитана на участие минимум двух команд, при этом количество членов команды может варьироваться – это требует от организатора мероприятия предварительной работы по формированию команд. В эту предварительную работу может входить не только сам факт поиска игроков, но и такие дополнительные действия, как решение вопроса о единой форме или едином элементе одежды, выборы капитана и распределение обязанностей внутри команды, придумывание названия команде, подготовка рассказа о команде в соответствии с имиджем, требуемым правилами и сюжетом игры. В случае проведения «Медиаринга» более чем с тремя командами

необходимы специальные турнирные таблицы, которые потребуют от организатора дополнительных усилий на их изготовление.

В случае если игра рассчитана на две команды, всегда существует опасность того, что командам достанутся разные по степени сложности вопросы, следовательно, необходимо предусмотреть и распределить вопросы по степени схожести, одинаковости. В качестве пожелания можно предложить заранее подготовить все вопросы на отдельных карточках и сложить карточки в отдельные стопки в зависимости от темы и сложности вопросов. Подобная предварительная подготовка ведущего значительно облегчит его работу во время игры. Для максимально эффективного проведения «Медиаринга» организатору и ведущему необходимо подробно изучить правила игры, а также составить письменное описание правил, максимально приближенное к речи ведущего, для объяснения обучающимся в начале предстоящей игры.

Игра разделена на три уровня сложности: теоретический, практический и конкурс капитанов – в каждом из них за правильный ответ либо решенную практическую задачу начисляется балл. Система учета баллов, полученных за правильные ответы, также служит элементом геймификации: используется либо набор выдаваемых за правильные ответы ярких жетонов на основе популярных в молодежной среде мемов и смайлов, либо турнирная таблица, на которой отображается количество баллов.

На первом уровне игры участники отвечают на ряд вопросов, касающихся медиаинформационной грамотности, профилактики IT-мошенничества, формирования навыков критического мышления и фактчекинга. На втором уровне обучающимся предлагается решить ряд практических кейсов по данной тематике, в которые включаются созданные специально либо реально существующие публикации в интернете и социальных сетях с примерами грубых ошибок, ведущих к утечке персональных данных, провоцирующих ситуацию IT-мошенничества; также в состав кейсов входят задачи на формирование критического мышления и навыков фактчекинга.

Дополнительным бонусным уровнем игры является конкурс капитанов, где вопросы уже становятся мультимедийными – предусматривают музыкальное либо видеосопровождение. По результатам «Медиаринга» ведется подсчет всех полученных командами баллов и подведение итогов мероприятия, объявляется команда-победитель, которая получает вознаграждение, соблюдая таким образом принцип геймификации.

# СТРУКТУРА И ПРАВИЛА ОБРАЗОВАТЕЛЬНОЙ ИГРЫ «МЕДИАРИНГ»

## Структура мероприятия

1. Приветственное слово преподавателя.
2. Представление команд и жюри.
3. Ознакомление с условиями игры.
4. Образовательная игра «Медиаринг».
5. Подведение итогов.
6. Поздравление победителей.
7. Рефлексия.

## Правила

Распределение по командам возможно несколькими способами в зависимости от количества обучающихся, соответственно, и правила игры также будут разными.

### *1 вариант*

1. Обучающиеся распределяются на шесть команд по пять игроков. Мероприятие делится на два раунда, в которых команды соперничают друг с другом по очереди:

1 раунд – 1, 2, 3 команды (три игры между собой);

2 раунд – 4, 5, 6 команды (три игры между собой);

3 раунд – команды-финалисты соревнуются между собой.

В каждой игре командам задается 10 теоретических вопросов, два практических задания и один медиавопрос в рамках конкурса капитанов. На подготовку ответа к вопросам дается одна минута. Отвечает на вопрос та команда, которая подготовилась первой.

2. Все бои идут до 10 очков.

3. О готовности дать ответ на прозвучавший вопрос команда сигнализирует поднятием зеленой карточки.

4. Отсчет времени начинается после команды ведущего «Время!».

5. Если команда допускает фальстарт, то есть поднимает карточку до сигнала ведущего, она лишается права ответа на данный вопрос.

6. Если обе команды в течение одной минуты не подняли карточку, то команду, которая будет отвечать первой на данный вопрос, определяет ведущий.

7. Если команда, поднявшая карточку первой, ответила неправильно, вторая команда может дать свой ответ на вопрос. Для обсуждения вторая команда может использовать оставшееся игровое время.

8. Команда, которая даст правильный ответ, получает одно очко.

9. Если обе команды не нашли правильный ответ на вопрос, на него может ответить зал. В таком случае 0.5 балла уходят команде, чьи болельщики ответили правильно.

## ***2 вариант***

1. Обучающиеся распределяются на две команды по 5-8 игроков. Мероприятие делится на три этапа: теоретический, практический и конкурс капитанов.

На теоретическом этапе командам задается 15 вопросов, на практическом – три задания и в конкурсе капитанов два медиавопроса, на которые отвечает та команда, которая подготовилась первой.

2. О готовности дать ответ на прозвучавший вопрос команда сигнализирует поднятием зеленой карточки.

3. Отсчет времени начинается после команды ведущего «Время!».

4. Если команда допускает фальстарт, то есть поднимает карточку до сигнала ведущего, она лишается права ответа на данный вопрос.

5. Если обе команды в течение одной минуты не подняли карточку, то команду, которая будет отвечать первой на данный вопрос, определяет ведущий.

6. Если команда, поднявшая карточку первой, ответила неправильно, вторая команда может дать свой ответ на вопрос. Для обсуждения вторая команда может использовать оставшееся игровое время.

7. Команда, которая даст правильный ответ, получает одно очко.

8. Если обе команды не нашли правильный ответ на вопрос, на него может ответить зал. В таком случае 0.5 балла уходят команде, которая ответила правильно.

## ПРИЛОЖЕНИЯ

### Приложение 1. Теоретические вопросы

1. Доступ к каким возможностям вашего телефона не стоит разрешать непрофильным приложениям? Назовите не менее пяти функций, поясните возможные риски. (*контакты, вызовы, sms-сообщения, геолокация, камера, микрофон*).

2. Каким приложениям можно разрешать доступ к геолокации? Назовите не менее трех приложений, поясните возможные риски (*такси, заказ еды, навигаторы и карты*).

3. Назовите пять приложений, кроме социальных сетей и мессенджеров, в которых необходимо установить двухфакторную аутентификацию (*Google, банковские приложения, почтовый ящик, приложения для получения государственных услуг – госуслуги, ПФР, росреестр и т.д.*).

4. Почему при оформлении сим-карты следует сменить пин-код на новый? Назовите стандартный пин-код для сим-карт мобильного оператора Теле-2.

5. Можно ли при входе в разные аккаунты использовать один и тот же пароль? Назовите не менее трех рекомендаций по составлению безопасного пароля (*чередовать строчные и прописные буквы латинского алфавита, использовать цифры и символы, в пароле должно быть не менее восьми символов*).

6. Как не забыть и наиболее безопасно хранить пароли от различных аккаунтов? (*использовать менеджер паролей*).

7. Что такое кэш и cookie? Почему их нужно периодически очищать? (*файлы, создаваемые веб-сайтами, которые посещали. В кеш-памяти сохраняется определенная информация с веб-страниц (например, изображения), чтобы в следующий раз они открывались быстрее*).

8. Как обезопасить свой аккаунт в социальной сети, если пришлось авторизоваться на чужом устройстве? (*поставить галочку «не сохранять пароль» при входе, очистить после себя кэш*).

9. По какому принципу следует выбирать контрольный вопрос для восстановления доступа к своим аккаунтам в социальных сетях? Назовите не менее трех примеров небезопасных контрольных вопросов (*такой, ответ на который не найти в общем доступе. Небезопасными контрольными вопросами могут быть девичья фамилия ваша либо вашей матери, кличка питомца, даты рождения ближайших родственников*).

10. Что такое фишинг? (*англ. phishing, от fishing – рыбная ловля, выуживание и password – пароль. Вид интернет-мошенничества, цель которого получить идентификационные данные пользователей. Сюда относятся кражи паролей, номеров кредитных карт, банковских счетов и другой конфиденциальной информации*).

11. Назовите два способа обезопасить свои деньги при бесконтактной оплате смартфоном (*установить пароль или отпечаток пальца при оплате смартфоном*).

12. В каком случае можно передавать в чужие руки свои документы, например, паспорт? (*только при получении банковских либо государственных услуг*). Чем грозит передача документов в чужие руки? (*случаями мошенничества с использованием ваших личных данных: оформление кредита, поддельных документов, подлог*).

13. Назовите не менее трех способов, которыми можно оградить денежные средства на ваших банковских картах от похищения (*не держать большие суммы на картах, ограничить лимит суточных трат, основные сбережения хранить на счетах, к которым не подключено дистанционное управление*).

14. Назовите не менее трех вариантов данных, относящихся к вашей банковской карте, которые должны быть полностью конфиденциальны. Имеют ли право сотрудники банка запрашивать эти данные у вас? (*сvv-код, пин-код, пароль*).

15. Что делать, если вам написал в социальных сетях знакомый с просьбой срочно одолжить небольшую сумму? (*ничего не переводить, позвонить, задать проверяющий вопрос*).

16. Каким словом называют интернет-контент, главная цель которого – накручивать количество просмотров, используя «желтые» заголовки для привлечения внимания? (*кликбейт*).

17. Назовите не менее трех способов проверить публикацию в социальных сетях на правдивость информации (*проверить аккаунт автора публикации – время создания, количество друзей, подписок и постов; проверить фото через различные сервисы на подлинность; поискать другие источники, подтверждающие информацию*).

18. Один из ключевых навыков 21 века – система суждений, которую применяют для анализа вещей и информации, интерпретации явлений, оценки событий, а также для последующего составления объективных выводов (*критическое мышление*).

19. Каково англоязычное название проверки информационных фактов, публикуемых в социальных сетях или медиаисточниках, на подлинность и достоверность? (*фактчекинг*).

## Приложение 2. Практические задания

### Карточка № 1

#### Угроза

- По государственному номеру автомобиля можно выяснить некоторые персональные данные владельца, например, узнать номер телефона или адрес проживания.

- Злоумышленники могут изготовить такие же номера и установить их на другой автомобиль, при этом штрафы за нарушения ПДД будут приходить настоящему владельцу номеров.

- Фотографии дорогого автомобиля могут сигнализировать злоумышленникам, что им есть чем поживиться.

#### Рекомендации

1. Если все же возникла острая необходимость выложить фото автомобиля в общий доступ, следует помнить – даже если закрасить важную информацию в графическом редакторе, специальными программами можно восстановить ее.

2. Следует учитывать, что госномера не являются персональными данными и не подлежат защите закона, следовательно, контролировать распространение и использование таких фотографий невозможно.



## Карточка № 2

### Угроза

- Утечка персональных данных в сеть Интернет. Зачастую та информация, которую о себе предоставляют пользователи в такой ситуации, утекает к злоумышленникам, которые не преминут ей воспользоваться в противоправных целях.

- Потеря денежных средств. Любые предложения в Интернете быстро заработать, не прикладывая никаких усилий, исходят от мошенников, которые выманивают деньги.

### Рекомендации

1. Никогда не отправляйте незнакомцам, которые первыми вышли с вами на контакт через сеть Интернет, свои персональные данные.

2. По всем законам экономики такая крупная прибыль за настолько короткий срок невозможна. Задумайтесь, почему настолько выгодные условия предлагают именно вам – «включите» навыки критического мышления.

3. Если все еще сомневаетесь, мошенники ли вам написали, обязательно следует проверить и написавшего вам человека, и компанию, от лица которой было сделано предложение. Добропорядочные бизнесмены обязательно имеют официальные сообщества в социальных сетях, сайты, везде будут указана достоверная информация и правильные контакты, по которым всегда можно связаться.



**Евгений** 10:57

Привет! Есть идея неплохо заработать. Не хочешь поучаствовать?



**Илья** 10:57

Привет!

Ну можно



**Евгений** 11:02

Идея проста: мы - небольшая компания, специализирующаяся на продажах. В данный момент, я набираю группу инвесторов, которые в будущем могут стать моими партнерами. Все, что от вас требуется - это вложение 3000 рублей. На выходе вы сможете получить целых 15000 рублей, и это все лишь за неделю. Вам ничего даже делать не придется. Все хлопоты я беру на себя. Всем инвесторам предоставляю гарантии.



**Илья** 11:02

О, классно, я в деле



### Карточка № 3

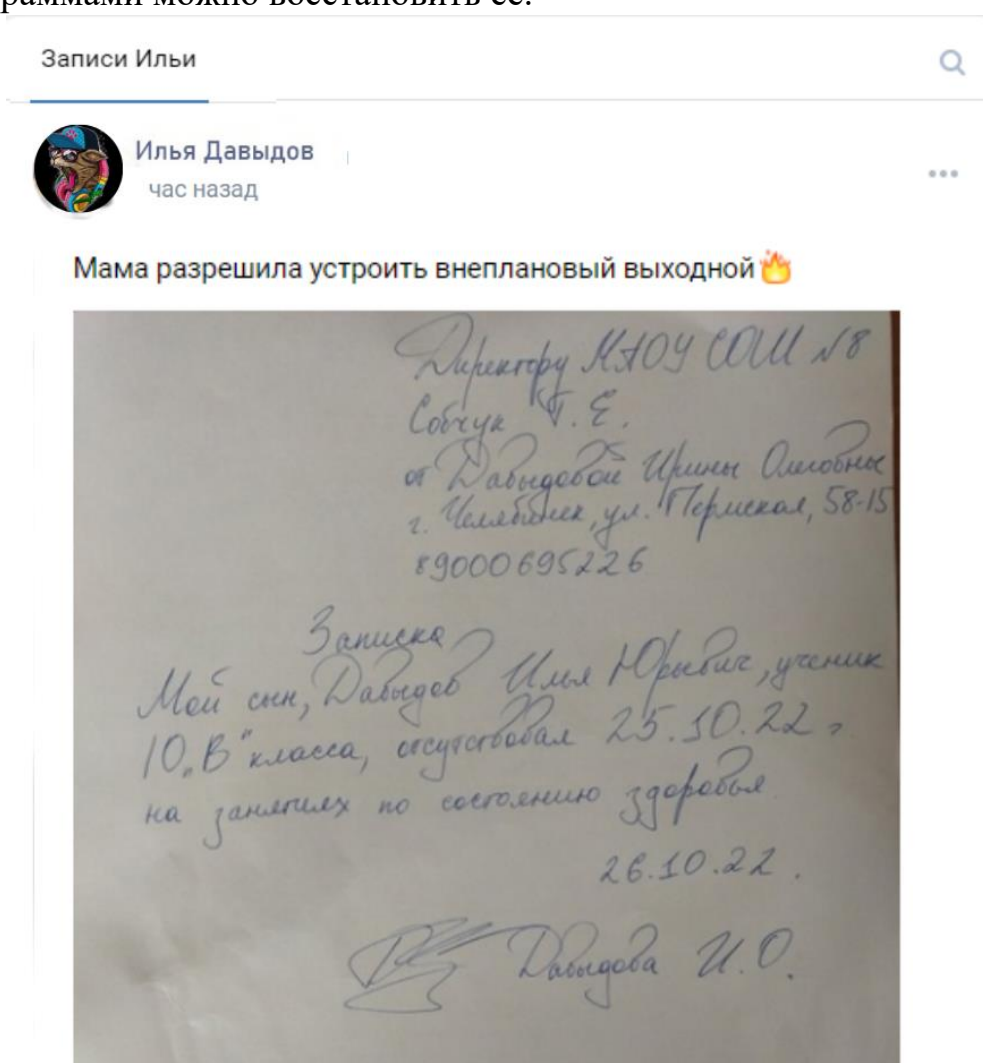
#### Угроза

- Опубликованные в общем доступе персональные данные третьего лица, такие как ФИО матери, номер телефона, адрес проживания, ее подпись, могут попасть к мошенникам. Полученные сведения позволят злоумышленникам подделать некоторые документы, связанные с личной подписью указанного лица.

#### Рекомендации

1. Нельзя выкладывать в открытый доступ персональные данные других людей без их согласия, за это предусмотрена ответственность вплоть до уголовной.

2. Если все же возникла такая необходимость, следует помнить – даже если закрасить важную информацию в графическом редакторе, специальными программами можно восстановить ее.



## Карточка №4.

### Угроза

- Опубликованные в общем доступе документы и важные файлы. Многие пользователи зачастую используют социальные сети для пересылки различных файлов, в том числе содержащих персональные данные, забывая при этом, что вся информация остается в разделе «Документы» и может быть доступна другим пользователям.

### Рекомендации

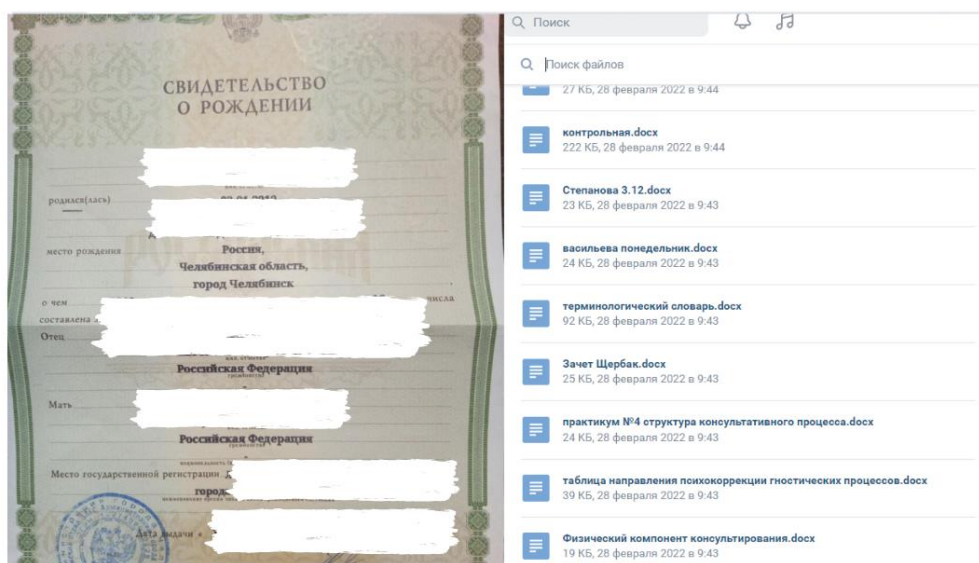
1. Если все же необходимо срочно использовать данный канал для отправки документа, важно сразу же после этого удалить его из раздела «Документы».

2. Важно понимать, что файл будет удален только со страницы. Все, что попадает в Интернет, там остается – следовательно, необходимо все же ограничить пересылку персональных данных посредством сети Интернет.



Илья Давыдов  
только что

Друзья! Узнал новый способ, как сохранять облачно документы. Просто закидываете в свои документы ВК и они всегда под рукой. Удобненько)



## Карточка №5.

### Угроза

- Потеря денежных средств вследствие мошенничества. Очень часто объявляются конкурсы с очень соблазнительными призами за простейшие действия вроде репоста или отзыва, далее пользователям рассылаются сообщения о выигрыше и просьба оплатить стоимость пересылки приза, налог либо другие расходы – а после оплаты пользователь просто блокируется. И уж тем более не стоит верить подобным сообщениям, если вы в таком конкурсе даже не участвовали.

- Утечка персональных данных. Злоумышленники требуют фото вашего паспорта или иных документов якобы для подтверждения личности при получении приза, а после также блокируют.


### Рекомендации

1. Никогда и никому не следует переводить деньги заранее. Важно понимать, что добросовестные организации и сообщества всегда берут расходы по пересылке призов на себя. Если требуют оплатить налог на приз, вы можете это сделать после его получения.


2. Не верьте фотографиям якобы организатора конкурса на фоне приза, паспорта и иных документов – никто не может гарантировать их подлинность, возможно, эти фото уже давно «гуляют» по Интернету.


3. Используйте навыки критического мышления и проведите проверку фактов. Проверьте дату создания аккаунта, с которого вам писали, открыты ли комментарии к постам, посмотрите, кто в друзьях у аккаунта, сделайте поиск по фотографиям на странице. «Включите» логику и здравый смысл.

сегодня


 **Сергей** 13:19  
Здравствуй! Меня зовут Сергей. Я администратор группы «Отдай даром».

Вы выиграли в конкурсе! Вам достаётся новенький iPhone 14! От вас потребуются только написать отзыв о нашей продукции после получения подарка. Вы согласны?


 **Илья** 13:20  
Здравствуй! Круто, спасибо! Конечно, согласен)))


 **Сергей** 13:22  
Для оформления доставки нам нужны следующие данн ФИО, адрес, номер вашего контактного телефона

Также необходимо оплатить стоимость пересылки в размере 800 рублей

 **Илья** 13:22  
Скиньте, пожалуйста, реквизиты, сейчас оплачу

А что за конкурс? Я просто не помню, вроде нигде не участвовал


 **Сергей** 13:27  
Программа сама выбирала случайного пользователя

 **Отдам даром**  
13 сен в 18:00

Только Россия  
Здравствуй дорогие участники группы  
Группе исполняется 3 года и в честь этого мы разыграем много продукции APPLE (32 ПОБЕДИТЕЛЯ)

- 1 Нужно написать МНЕ в лс "+"
- 2 ДОСТАВКУ ПРИЗА ОПЛАЧИВАЕТ САМ ПОБЕДИТЕЛЬ
- 3 Все гарантии можете посмотреть ТУТ

✓ Данный розыгрыш прошёл полную проверку Администрацией и Гарантом и имеет полное доверие как и к розыгрышу так и к его ведущему.



## Карточка №6.

### Угроза

- Утечка персональных данных. Номер электронного билета, код бронирования (PNR-код), номер карты лояльности, штрих коды и QR коды на посадочном талоне представляют интерес для злоумышленников, так как с их помощью реально получить доступ для входа в аккаунт. На странице бронирования возможно изменить данные: фамилию, место в самолете, паспортные данные (например, на имя террориста из базы Интерпола) или даже аннулировать билет. Там же можно найти последние четыре цифры банковской карты, дату и сумму платежа.

- Злоумышленники могут достоверно узнать, сколько вы будете отсутствовать дома, и таким образом спланировать какие-либо противоправные действия против вас.

### Рекомендации:

Не стоит выкладывать в общий доступ фотографии билетов, на которых видно имя пассажира, дата рождения, PNR-код или штрих-код. Помните – даже если закрасить коды в графическом редакторе, специальными программами можно восстановить их.



Илья Давыдов  
7 секунд назад

Ура, летим погостить к любимой бабуле ! Целую неделю буду лопать от пуза домашние пирожки и блины 🍷



### Приложение 3. Задания для конкурса капитанов.

В рамках конкурса капитанов предлагаются 2 развлекательных задания на общую эрудированность участников: музыкальное и видеовопрос.

#### ***Музыкальное:***

Необходимо угадать, что за мелодии воспроизводятся, и к какому компьютерному процессу они относятся. Участникам предлагается прослушать короткие музыкальные заставки на включение/выключение ОС Windows, звук работы матричного принтера, чтения дискеты, работы модема, звонок в Skype, оповещение в ICQ, музыкальная заставка Asus и звук обнаружения вируса в программе «Антивирус Касперского».

#### ***Видеовопрос:***

1. Необходимо угадать, чем известно видео «Baby Shark Dance» (самое просматриваемое видео на YouTube).

2. Необходимо угадать, какое видео раньше всех перешагнуло отметку в миллиард просмотров (PSY – Gangnam Style).