АНО НЦПТИ

ПРАВИТЕЛЬСТВО
РОСТОВСКОЙ ОБЛАСТИ

Методические указания по проведению классных часов и интерактивных занятий «Защита персональных данных от доступа злоумышленников в сети Интернет»

Ростов-на-Дону
2019

УДК 004.056.5
ББК 32.972.53

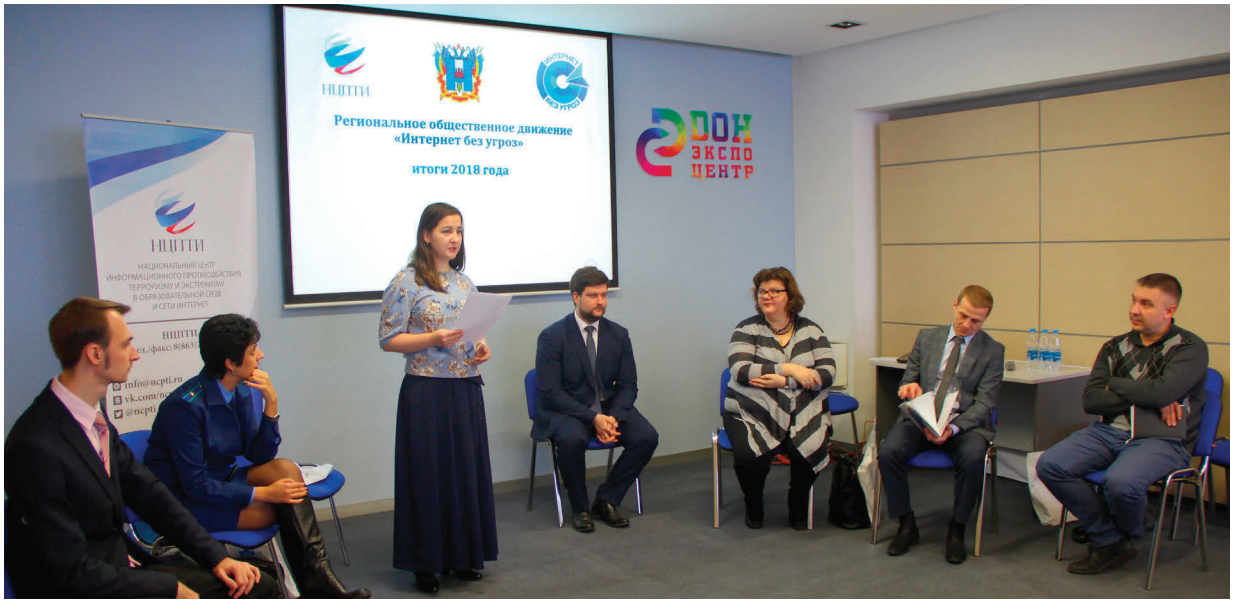
Авторский коллектив: А.С. Быкадорова, Д.Н. Брайко, Е.Р. Валитова, А.Н. Кулик, И.Ю. Насонова, Д.В. Очергоряева, Л.А. Рачеева, А.С. Чунин.
Под редакцией В.С. Жученко

Аннотация: Методические указания разработаны в целях формирования у несовершеннолетних культуры работы с собственными персональными данными в сети Интернет, а также выработки навыков распознавания различных информационных угроз и правильного реагирования на них. Авторами подготовлена серия практических занятий для работы в интерактивном формате и инструкции к их применению.

Методические указания разработаны на средства субсидии Правительства Ростовской области социально ориентированным некоммерческим организациям, договор № 01/04 от 03.07.2019 г.

Гражданский форум Ростовской области: http://civil-society.donland.ru/

Содержание



Авторский коллектив и волонтеры информационно-просветительского проекта «Защита персональных данных от доступа злоумышленников в сети Интернет»

Быкадорова Александра Сергеевна – кандидат филологических наук, директор АНО «НЦПТИ»

Брайко Дарья Николаевна – волонтер регионального общественного движения «Интернет без угроз», преподаватель Института социологии и регионоведения ЮФУ

Валитова Елена Рашидовна – волонтер регионального общественного движения «Интернет без угроз»

Жученко Виктория Сергеевна – волонтер регионального общественного движения «Интернет без угроз»

Чунин Александр Сергеевич – волонтер регионального общественного движения «Интернет без угроз»

Кулик Анна Николаевна – педагог-организатор МБУ ДО Центр творчества детей и молодежи Аксайского района Ростовской области

Насонова Ирина Юрьевна – заведующая МБДОУ детский сад № 9 «Солнечный» Каменского района Ростовской области

Очергоряева Джиргал Викторовна – волонтер регионального общественного движения «Интернет без угроз»

Рачеева Лилия Анатольевна – преподаватель русского языка, литературы, права ГБПОУ РО «Ростовский технологический техникум сервиса»

От авторов

В современном обществе сложно представить организацию профессиональной или повседневной коммуникации, а также получение или оказание ряда услуг без каналов интернета. Однако обмен информацией через телекоммуникационные системы, кроме определенного удобства, привносит в нашу жизнь и дополнительные риски, связанные с потерей ценной информации. Наибольшую угрозу представляет утечка персональных данных.

Интернет-пользователи постоянно совершают различные действия, связанные с использованием персональных данных: от регистрации в социальных сетях до совершения онлайн-покупок. Каждое действие требует раскрытия тех или иных персональных данных (ФИО, паспортных данных, номера телефона, реквизитов банковской карты и др.). В этой связи актуальной становится проблема защиты собственных персональных данных в сети Интернет как от доступа злоумышленников, так и от собственноручной неосознанной передачи их третьим лицам.

Проблема актуальна для пользователей сети Интернет всех возрастов, однако наиболее уязвимыми являются несовершеннолетние, поскольку именно они являются самыми активными интернет-пользователями и, в то же самое время, самыми раскованными и неосведомленными о потенциальных угрозах.

Цель данных методических указаний – разработать серию практических материалов и методическое сопровождение к ним для работы сотрудников образовательных организаций с несовершеннолетними в сфере формирования культуры использования и распространения персональных данных.

Задачи методических указаний:

1. Выявить наиболее актуальные угрозы в сфере использования персональных данных в сети Интернет.

2. Выработать эффективные алгоритмы действий для несовершеннолетних при столкновении с одной из угроз в сети Интернет.

3. Сформировать у несовершеннолетних основные принципы обращения с собственными персональными данными в интернет-пространстве.

В силу возрастных, психоэмоциональных и ценностных различий, практические материалы были подготовлены для различных возрастных групп несовершеннолетних:

- 1–4 классы;
- 5–6 классы;
- 7–9 классы;
- 10–11 классы, студенты средних профессиональных образовательных учреждений.

Учебно-практическая ценность методических указаний заключается в уникальности и узконаправленности подготовленных практических материалов и методического сопровождения к ним.

Методические указания «Защита персональных данных от доступа злоумышленников в сети Интернет» разработаны в помощь сотрудникам образовательных организаций в исполнение Указа Президента РФ от 01.06.2012 № 761 «О Национальной стратегии действий в интересах детей», Комплексного плана противодействия идеологии терроризма на 2019–2023 гг.

Методические указания будут полезны классным руководителям, специалистам по учебно-методической и воспитательной работе, учителям по информатике и ОБЖ, педагогам-организаторам, старшим вожатым, психологам образовательных организаций, педагогам дополнительного образования, родителям несовершеннолетних детей.

Методические указания разбиты на 4 подраздела, каждый из которых содержит сами практические задания и инструкции к их проведению. Для точного и единообразного определения терминов приводится словарь.

Главная особенность использования методических указаний заключается в том, что педагог выступает в качестве модератора интерактивного занятия, в котором главную роль должны играть сами школьники или студенты. Кроме того, необходимо учитывать уровень подготовленности аудитории, в которой проводятся занятия: если он низкий, то следует адаптировать предложенные материалы или использовать задания для младших классов, и наоборот, если ситуация противоположная.

Формат проведения классного часа (другого занятия) предполагает групповую работу, поэтому перед началом рекомендуется распечатать предложенные практические материалы в необходимом количестве (соотносится с количеством микрогрупп).

Для удобства работы все представленные в методических указаниях материалы можно скачать по ссылке: культ-просвет.нцпти.рф или на официальном сайте НЦПТИ.

Словарь

Защита персональных данных – это действия, направленные на предотвращение неконтролируемого распространения персональных данных в результате их разглашения и несанкционированного доступа к ним.

Медиабезопасность – это защищенность от недостоверной информации и информации, наносящей вред личному и общественному благополучию.

Медиаграмотность – возможность личности противостоять информационным угрозам и воздействиям.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Традиционно персональные данные подразделяют на 3 основные группы: общие (ФИО, дата рождения, паспортные данные и др.), специальные (раса, религия, этническая принадлежность и др.) и биометрические (цвет глаз, вес, рост и др.).

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Утечка персональных данных – неконтролируемое распространение персональных данных в результате их разглашения, несанкционированного доступа к персональным данным.

1–4 классы

Есть много важных тем, в которые нельзя не посвящать детей только потому, что они еще «слишком маленькие, чтобы понять». Задача взрослых — не только оберегать, но и своевременно научить детей распознавать угрозы и правильно на них реагировать, тем более сейчас, когда дети осваивают смартфон или планшет быстрее, чем ходьбу. Однако очень важно правильно подать информацию, чтобы ребенок не просто понял ее, но и воспринял.

В 1–4 классах дети еще не являются активными интернет-пользователями, однако у многих уже есть мобильные телефоны с выходом в Интернет, а у некоторых — аккаунты в социальных сетях, поэтому профилактическая работа по проблеме защиты персональных данных должна начинаться уже с этой возрастной группы. Авторы предлагают сосредоточиться на этапе ознакомления и введения в проблему: пояснения самого термина «интернет», «персональные данные», обозначения круга потенциальных угроз. Наиболее эффективными форматами признаны интерактивные уроки-беседы, игры.

Настольная игра «Путешествие по интернету»

Цель: привить школьникам младших классов культуру работы в интернете, а также основные правила защиты персональных данных, публикуемых в сети.

Задачи:

1. Ознакомить школьников с основными аспектами безопасного использования интернета.
2. Провести тематическую игру для контроля выработки у школьников необходимых компетенций, связанных с культурой пользования интернетом.

Время проведения: 30–60 минут.

Правила игры:

Количество участников: 2 и больше.

Для проведения игры необходимы: игровое поле (вкладка), фишки, шестигранный кубик.

Определите жребием, кто будет ходить первым. Все игроки начинают игру на шаге «СТАРТ».

Игроки по очереди бросают кубик, и передвигают свою фишку на столько шагов вперед, сколько очков выпало.

В игре есть 12 карточек, которые раскладываются перед участниками игры возле игрового поля. На поле игры находятся в кружке ходы: 1, 3, 4, 7, 8, 9, 13, 15, 17, 21, 22, попадая на эти номера, участники отвечают на вопросы.

Выигрывает тот, у кого первого на кубике выпадает точное количество очков до финиша.

Вводное слово:

Перед тобой открывается необычный мир – мир интернета. В этом чудесном и увлекательном мире есть всё: информация для учебы, чтобы получать хорошие оценки, много иностранных слов, позволяющих пополнить твой словарный запас, здесь можно найти друзей, и, конечно же, в интернете есть много опасностей, которые затаились и ждут тебя. С этими опасностями тебя познакомят два школьника – это пятиклассники: мальчик Бук и девочка Варя. Мальчик вечно хмурый и сидит за компьютером. Правда, он хорошо учится. Он хорошист, но только тогда, когда захочет и интернет его не отвлекает. А девочка Варя – веселая и задорная! Она староста в классе, отличница. Варя Бука знает давно! Еще бы не знать своего одноклассника Бука, а точнее его зовут по-другому – Даниил. С первого класса его прозвали Буком из-за молчаливости и серьезности. Однажды в гости пришла Варя и заявила, что хочет, чтобы Бук был отличником и вышел на улицу погулять, а не сидел за компьютером, но Бук сказал, что интернет безопасный и интересный! Помоги Буку и Варе помириться и поиграй с ними в игру. Побежали!

Карточки для настольной игры «Путешествие по Интернету»:

Ход 1	Ход 1	Ход 3	Ход 3
Что такое Интернет?	Internet («межсетевой») — всемирная система объединённых компьютерных сетей для хранения и передачи информации.	Что такое персональные данные?	Персональные данные — информация о человеке, которая позволяет отличить его от других.
Ход 4	**Ход 4**	**Ход 7**	**Ход 7**
В чем может помочь тебе Интернет?	Возможные варианты ответа: 1. Выполнять домашнее задание. 2. Смотреть познавательные фильмы. 3. Общаться с друзьями.	Как думаешь, как много людей пользуются Интернетом?	По приблизительным оценкам, к Интернету подключено свыше 3 миллиардов человек, а это половина всех жителей нашей планеты!
Ход 8	**Ход 8**	**Ход 9**	**Ход 9**
Правила безопасности в Интернете! Правило № 1 Какое бы правило назвал ты?	В социальных сетях (например, «Вконтакте»), в комментариях, на форумах, в анкетах не указывай, как свои, так и персональные данные твоих родственников и друзей (фамилию, имя, отчество, номера телефонов).	Правила безопасности в Интернете! Правило № 2 Какое бы правило назвал ты?	НЕ выкладывай фотографии друзей и знакомых без их согласия! Фотографии человека могут быть его персональными данными! Будь осторожен, выкладывая в соцсети и свои фото.

Ход 13	Ход 13	Ход 15	Ход 15
Правила безопасности в Интернете! Правило № 3 Какое бы правило назвал ты?	Никогда не отправляй со своего телефона sms-сообщения по объявлениям, которые ты увидел в интернете. Даже если там будут такие фразы: «Выиграй деньги», «Отправь смс и поучаствуй в игре» и т.д. Всегда спрашивай взрослых, прежде чем вступить в игру!	Правила безопасности в Интернете! Правило № 4 Какое бы правило назвал ты?	Без разрешения родителей не встречайся в жизни с друзьями, с которыми ты познакомился в Интернете!
Ход 17	**Ход 17**	**Ход 21**	**Ход 21**
Правила безопасности в Интернете! Правило № 5 Какое бы правило назвал ты?	НЕ переходи по сомнительным с сылкам на другие непроверенные сайты! Будь осторожен, так как там могут быть компьютерные вирусы, которые могут уничтожить все документы на компьютере!	Правила безопасности в Интернете! Правило № 6 Какое бы правило назвал ты?	Не рассказывай в соцсетях много о себе! Куда поедешь отдыхать, что купил нового! Любая твоя информация может быть использована мошенниками! Интернет предназначен для временного пользования: скачать книги, фильмы, договориться о встрече, найти полезную информацию.
Ход 22	**Ход 22**	**ФИНИШ**	**ФИНИШ**
ОТВЕТЬ НА ВОПРОСЫ И ПЕРЕЙДИ НА ФИНИШ!	1. Почему нельзя указывать в социальных сетях номер банковской карты родителей или номер их телефона? 2. Для чего нужны антивирусники? 3. Как надо поступить, если в соцсетях тебе написал незнакомый человек и пригласил погулять?	ТЫ ВЫИГРАЛ!	Спасибо! ТЫ ПОМИРИЛ ВАРЮ И ДАНИИЛА!

Интерактивный урок-беседа «Что такое персональные данные?»

Задача: рассказать, что такое персональные данные и объяснить их значимость в пространстве Интернета.
Формат: беседа.
Время проведения: 20–30 минут.

Педагог: «Перед тем как мы начнем, поднимите руки те, кто когда-нибудь слышал словосочетание «персональные данные»?».

Пусть дети расскажут то, что они уже слышали об этом термине. Если таких не окажется, то они могут интуитивно предложить свои варианты. При возникновении затруднений, можно предложить поразмышлять над словосочетанием «личная информация», которое может быть более знакомо и привычно детям данного возраста. Итогом диалога должен стать сформулированный термин:

Персональные данные — информация, позволяющая отличить одного человека от другого.

Педагог: «Посмотрите на двух мальчиков. Скажите, что мы должны о них знать, чтобы отличить одного ребенка от другого?» (Рис. 2).

Возможные варианты ответа:
1. Имя.
2. Фамилия.
3. Отчество.
4. Возраст.
5. Адрес места жительства.
6. Дата рождения.

Рис. 2

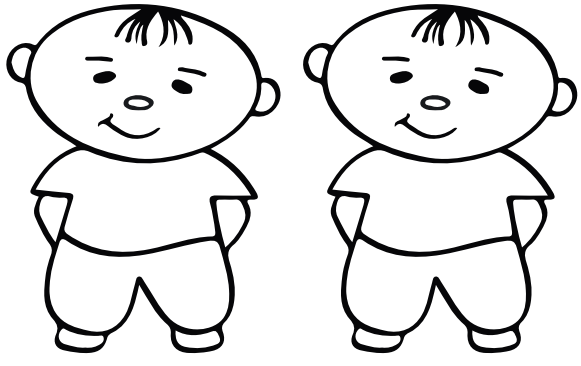
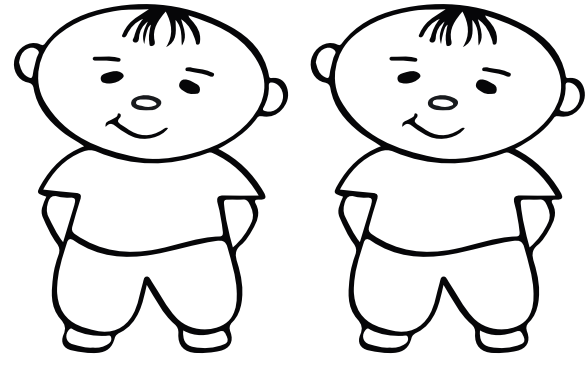


Рис. 3



Леша, 3 года **Дима, 4 года**

Пусть дети попробуют назвать дополнительные параметры, которые можно отнести к персональным данным. (номер телефона, место учебы, национальность...).

Педагог: «Теперь посмотрите на рис. 3. Будет ли вам теперь проще отличить мальчиков? Почему?»

Педагог: «Что еще может отличать двух мальчиков, помимо имени и возраста?»

На этом шаге дети должны попробовать сами назвать другие факторы, которые помогут отличить детей. Если необходимо, можно привести пример: «Леша может учиться в школе № 1, а Дима — в школе № 2»; «Леша может жить в Ростове-на-Дону, а Дима — в Москве».

Педагог: «Чем больше вы знаете о человеке, тем больше вы владеете его персональными данными».

Педагог: «Как Вы считаете, всегда ли безопасно сообщать другому человеку свои персональные данные, может ли быть какая-то опасность?».

Возможные угрозы:

1. «Что может произойти, если злоумышленник знает ваш адрес?» (ограбление).

2. «Что может произойти, если злоумышленник знает адрес вашей электронной почты или номер телефона?» (навязчивые звонки в целях баловства, спам).

3. «Что может произойти, если вы расскажете кому-нибудь персональные данные своих родителей?» (номер телефона, номер банковской карты – кража денег).

Педагог: Можно ли не бояться сообщать о своих персональных данных в Интернете?

Вывод: важно донести до учащихся, что пользователи интернета – те же люди, с которыми мы общаемся в реальной жизни, поэтому угрозы не просто не исчезают, а наоборот, усиливаются, за счет того, что в интернете можно действовать анонимно, не под своим настоящим именем.

5–6 классы

Подростки 12–14 лет уже активно общаются в социальных сетях, которые выступают одной из главных коммуникативных площадок в их среде, наравне с живым общением в рамках школьных занятий. Возрастную группу можно отнести к наиболее подверженной рискам, поскольку тематика профилактической работы в начальной и средней школе значительно отличается: в первом случае в качестве приоритетного развивается ознакомление с правилами дорожного движения, с переходом в среднюю школу на первый план выходят проблемы медиаграмотности и медиабезопасности. Для определения круга проблем, требующих особого внимания и проработки, школьникам предлагается пройти небольшое тестирование.

Тест «Защита персональных данных от доступа злоумышленников в сети Интернет»

1. Как Вы считаете, что такое «персональные данные»?
a) фамилия, имя и отчество человека;
b) секретная информация о человеке;
c) любая информация, по которой можно определить конкретного человека.

2. Что из перечисленного можно отнести к персональным данным? (обведите все варианты, которые посчитаете правильными)
a) имя;
b) фамилия;
c) отчество;
d) возраст;
e) национальность;
f) номер телефона.

3. Как Вы считаете, безопасно ли открыто писать о своих персональных данных в интернете?
a) безопасно, злоумышленник никак не сможет воспользоваться тем, что знает мои персональные данные;
b) безопасно, с помощью интернета мне нельзя навредить;
c) опасно, злоумышленники могут воспользоваться интернетом, чтобы навредить мне в реальной жизни;
d) опасно, вред можно нанести и через интернет.

4. Какие опасности могут подстерегать вас в интернете?

Практическая сторона вопроса показывает, что особое внимание необходимо уделять правилам безопасного поведения в социальных сетях.

На примере одной из самых популярных среди молодежи социальной сети «ВКонтакте» можно выделить ряд наиболее актуальных информационных угроз:

1. Использование социальных сетей в качестве хранилищ информации, перебрасывая документы в виде сообщений.

2. Использование социальных сетей в качестве быстрого заработка денег.

3. Открытая публикация персональных данных в постах-объявлениях.

4. Публикация сведений, которые в совокупности с другими данными могут выступать в качестве персональных данных.

На их основе разработаны карточки, демонстрирующие ту или иную проблему. Работу с карточками предлагается проводить в формате интеллектуальной игры, разделив аудиторию на несколько микрогрупп.

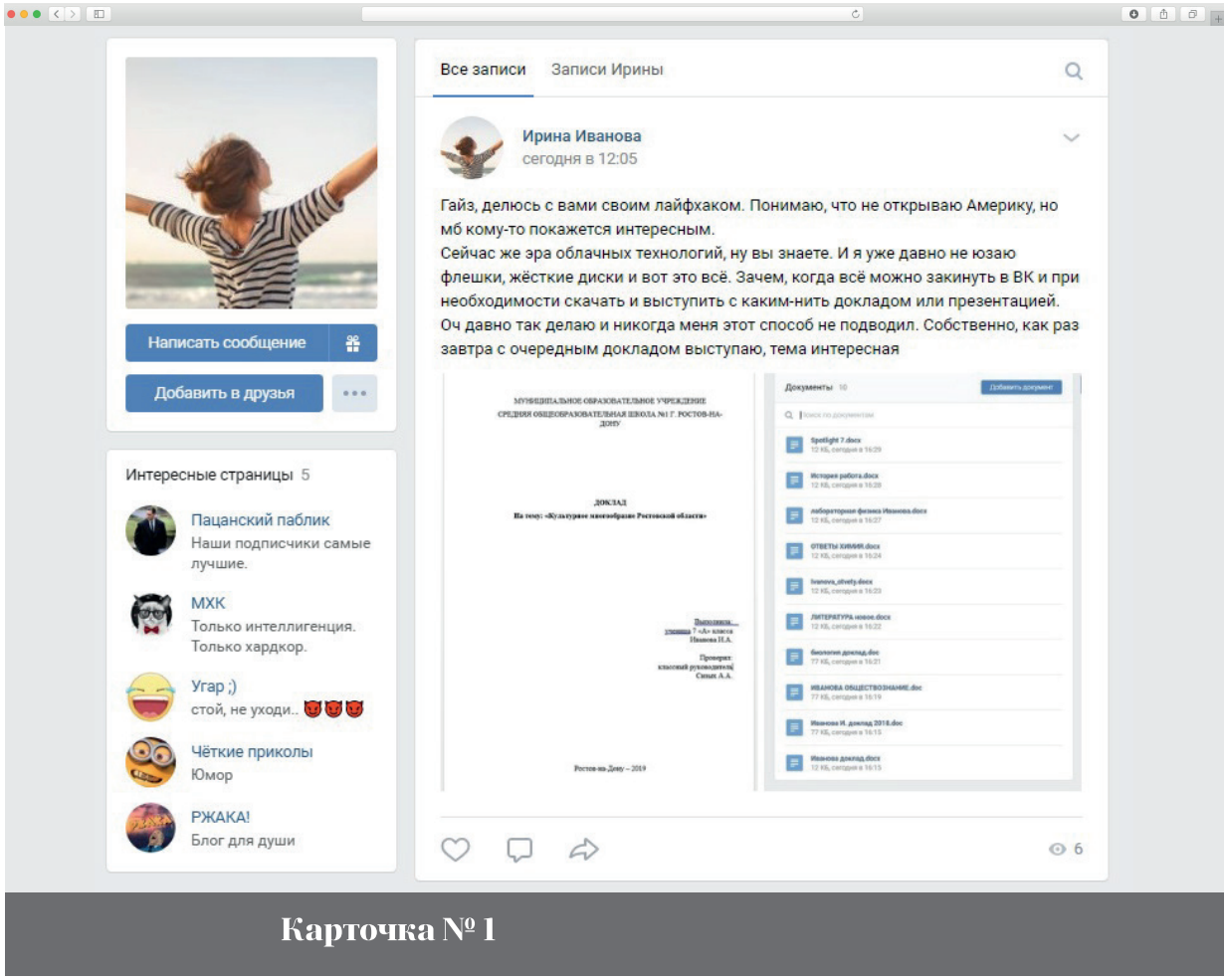
Интеллектуальная игра «Безопасность в социальных сетях»

Цель: продемонстрировать подросткам средней школы наличие реальных угроз в социальных сетях.
Задачи:
1. Выявить наиболее актуальные угрозы для подростков 12–14 лет.
2. Выработать основные правила безопасного использования социальных сетей.
Формат: интеллектуальная игра.
Время проведения: 40–50 минут.

Ход работы:

Педагог делит учащихся на микрогруппы (не более 5 человек в каждой): их может быть 6 — по количеству карточек, или же 2–3 микрогруппы с выдачей команде сразу 2–3 карточек.

Задача каждой команды — проанализировать карточку и определить наиболее явную угрозу, после чего предложить меры для избежания утечки персональных данных. В помощь педагогу предлагаются пояснения к каждой карточке.



Карточка № 1

Рис. 4

Угроза:

1. Размещение в социальных сетях документов и важных файлов.

Интернет-пользователи все чаще стали использовать социальные сети в качестве хранилищ информации, забывая, что все переправляемые файлы находятся в открытом доступе в разделе «Документы». Другие интернет-пользователи могут наравне с владельцем воспользоваться ими, в том числе для получения информации в мошеннических целях.

Например, другой пользователь может использовать материалы вашей курсовой работой или научной статьи для своих нужд. В таком случае ваше авторство будет сложно доказать, и публикация может не пройти систему «Антиплагиат». Злоумышленники могут использовать сохраненные вами копии паспорта, реквизиты карты, ИНН, СНИЛС и других документов в мошеннических целях.

Рекомендации:

1. Если возникла острая необходимость использовать данный канал для переброски файла, важно сразу же удалить его из раздела «Документы» после использования. Однако в этом случае важно осознавать, что файл будет удален только со страницы. Все, что попадает в Интернет – там и остается!

2. Привести к минимуму распространение персональных данных в любом их виде в Интернете.

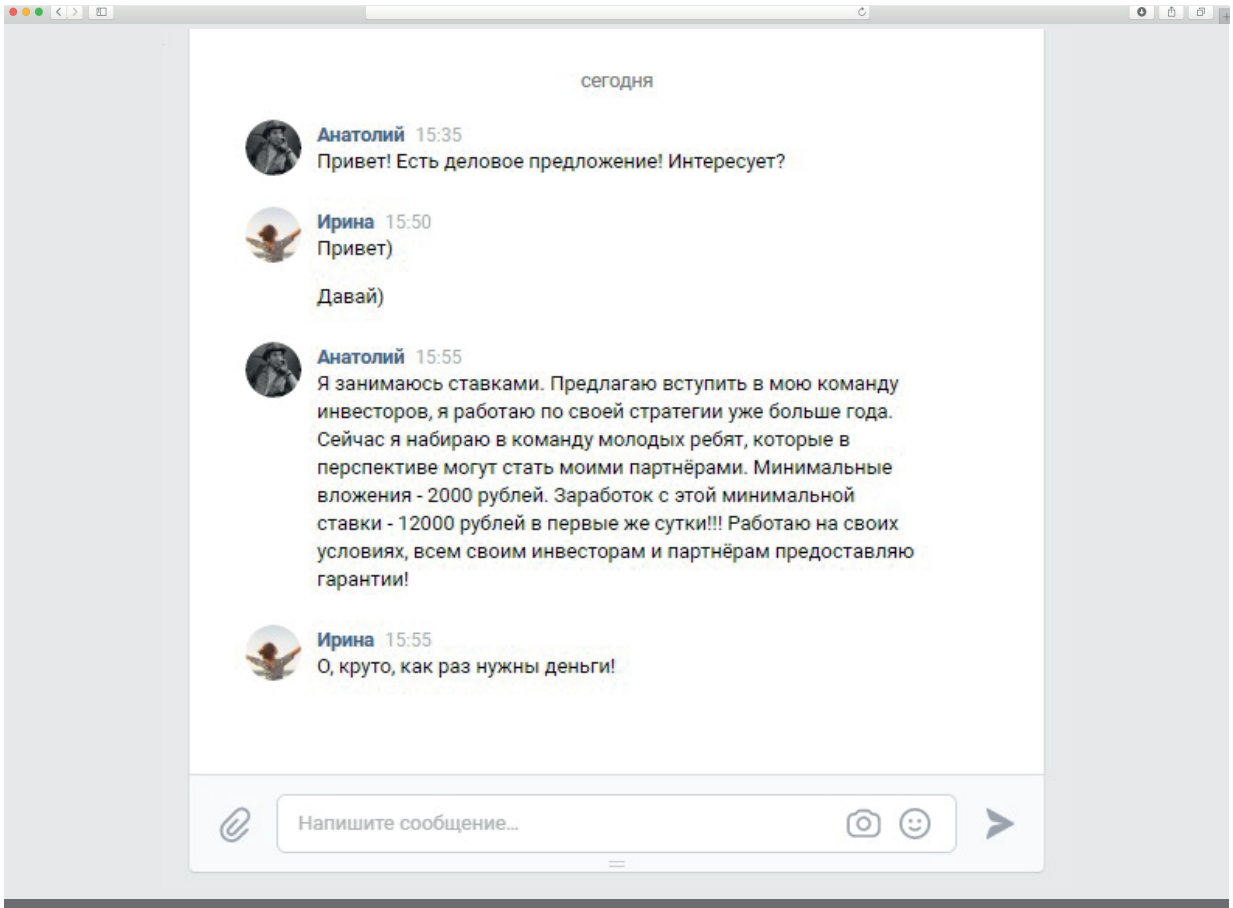


Рис. 5

Карточка № 2

Угроза:

1. Утечка персональных данных и потеря денежных средств.

«Быстро заработать» в социальных сетях очень часто предлагают мошенники, которые выманивают у пользователей персональных данные, дающие доступ к денежным средствам.

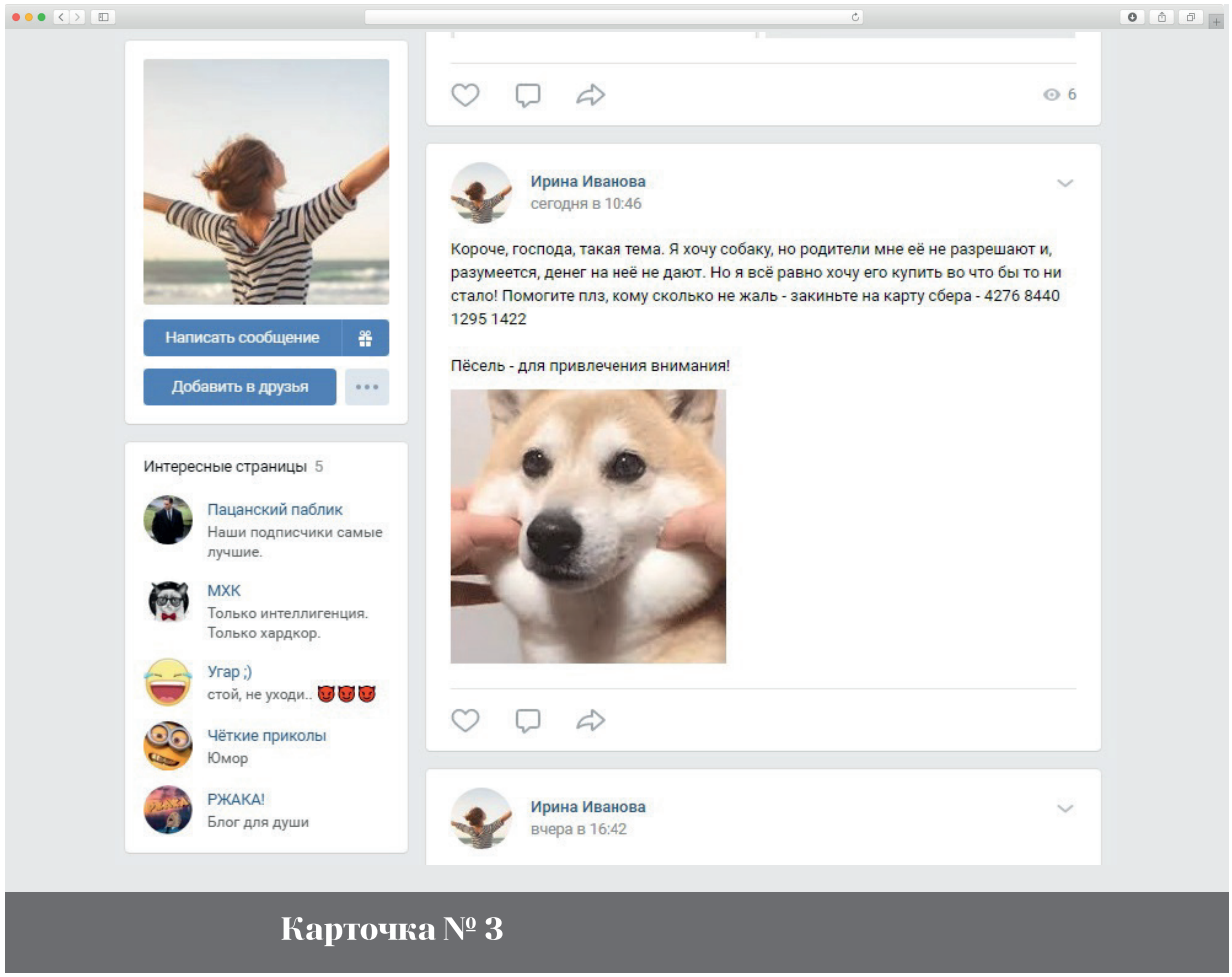
Рекомендации:

1. Никогда не отправляйте незнакомым людям, которые нашли вас через социальные сети, свои персональные данные (паспортные данные, реквизиты банковских карт, номер телефона и др.).

2. Ни один официальный работодатель не будет предлагать потенциальным работникам вносить аванс или делать первое вложение. Если это произошло, скорее всего, вы имеете дело с мошенником.

3. Необходимо проверять каждое сделанное вам предложение: официально работающие компании будут иметь официальные сообщества в социальных сетях, сайты, лендинги. Сверьте контакты человека, написавшего вам, с данными на сайте.

4. Обратитесь за советом к знакомому взрослому человеку (родители/классный руководитель): стоит ли доверять полученному предложению?



Карточка № 3

Рис. 6

Угроза:

1. Получение доступа к банковской карте или системе «банк-онлайн».

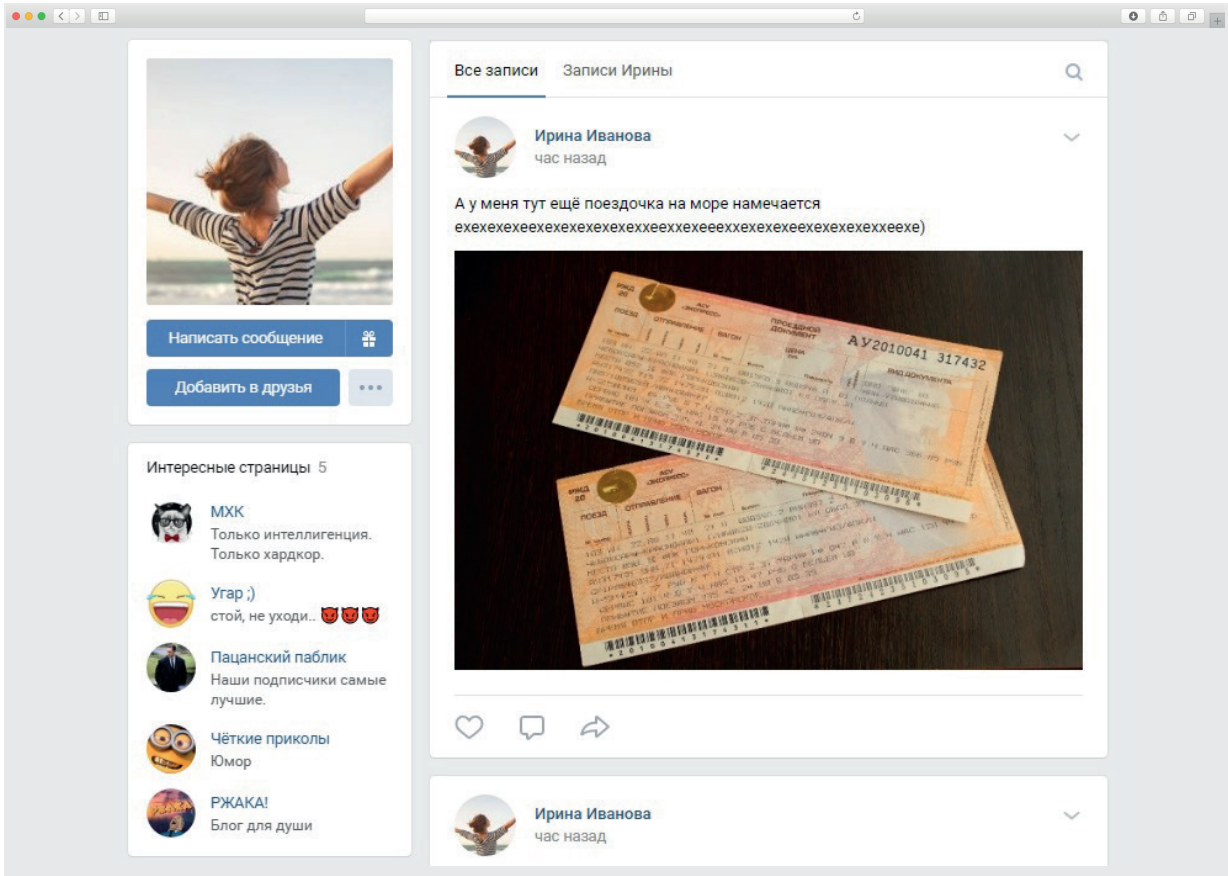
Зная реквизиты вашей банковской карты, злоумышленник может расплатиться средствами на ней за покупки в интернет-магазине, совершить перевод с карты на карту и т. д.

Рекомендации:

1. Не оставляйте в открытом доступе номер банковской карты и другие ее реквизиты.

2. Размещая объявления в социальных сетях, перенаправляйте пользователей на другие ресурсы сбора денег (краудфандинговые платформы), которые заботятся о сохранности персональных данных и используют первичные средства для защиты денежных переводов.

3. Никогда не сообщайте номер банковской карты родителей или или других родственников без их согласия.



Карточка № 4

Рис. 7

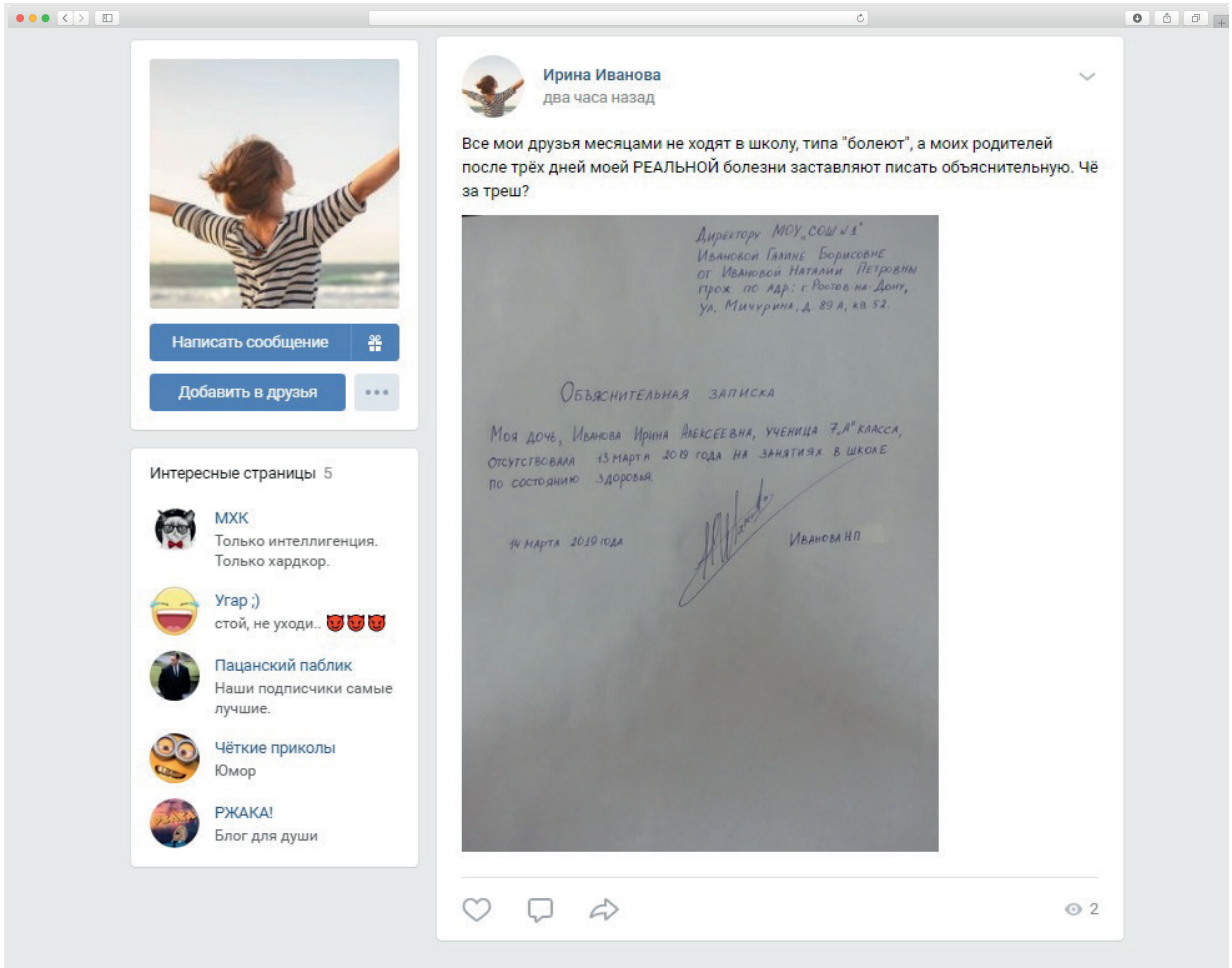
Угроза:

1. Публикация билета с открытым PNR-кодом (код бронирования – первые шесть буквенно-цифровых символов) может привести к его использованию любым другим пользователем. Мошенник может воспользоваться вашим билетом, просто показав его на входе или при регистрации раньше вас.

Рекомендации:

1. Не публикуйте в социальных сетях фотографии билета, на которых видно имя пассажира, дата рождения, PNR-код и штрих-код. В крайнем случае, эти данные можно «заштриховать» с помощью графических редакторов.

2. Не оставляйте в открытом доступе и уже реализованные билеты, так как они все еще содержать ваши персональные данные (например, номер банковской карты, с которой проводилась оплата).



Карточка № 5

Рис. 8

Угроза:

1. Публикация в открытом доступе персональных данных третьего лица (в данном случае, ФИО родителя, адрес проживания, личная подпись).

Данные сведения позволят мошеннику подделать документы, связанные с подписью указанного лица.

Рекомендации:

1. Никогда не выкладывать в открытый доступ персональные данные других людей без их согласия. При возникновении необходимости опубликовать документ – «заштриховать» с помощью графических редакторов все персональные данные.

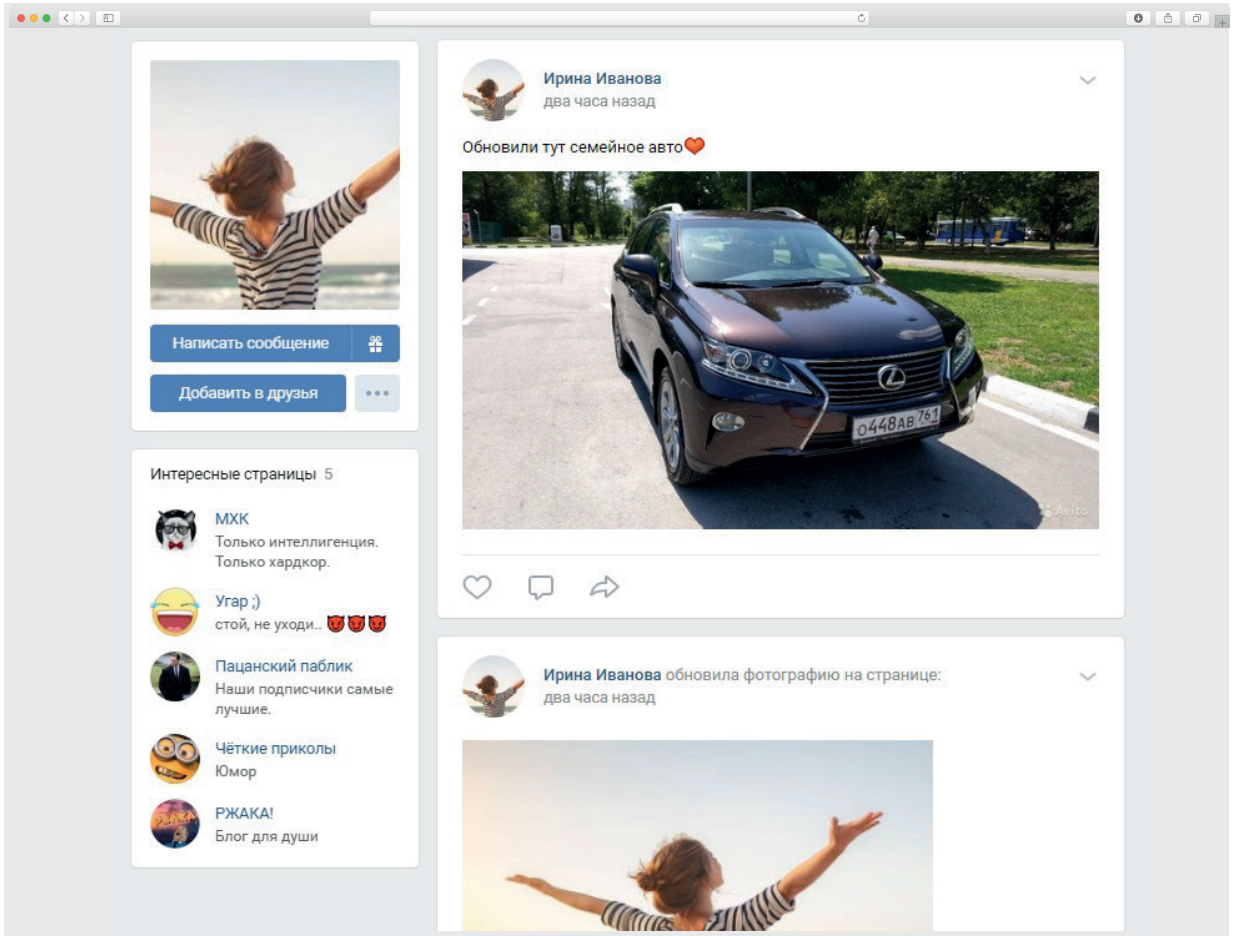


Рис.9

Карточка № 6

Угроза:

1. Публикация фотографии автомобиля с открытыми номерами.

По государственному номеру из открытых баз данных можно определить владельца машины, узнать номер телефона, адрес проживания.

Мошенник способен изготовить такие же номера и установить их на другой автомобиль, при нарушении штрафы будут приходить настоящему владельцу номеров. Кроме этого, фотография может демонстрировать «ценность» автомобиля: аксессуары внутри салона, шины.

Рекомендации:

1. При публикации фотографии автомобиля необходимо «заштриховывать» государственные номера с помощью графических редакторов.

2. При публикации подобной фотографии не стоит забывать, что данные об автомобиле, включая его государственный номер, не являются персональными данными и не подлежат защите со стороны закона, поэтому, предоставляя эти сведения в открытый доступ в интернет, вы не сможете контролировать распространение фотографии и использование сведений о ней.

7–9 классы

Учащиеся 7–9 классов являются не просто активными, но и уверенными пользователями интернет-пространства. В связи с этим возрастает и актуальность риска подверженности информационным угрозам.
Для определения наиболее важных тем в вашей группе школьникам предлагается пройти следующее тестирование:

Тест «Защита персональных данных от доступа злоумышленников в сети Интернет»

1. Как Вы считаете, что такое «персональные данные»?

a) паспортные данные человека;
b) любая информация, по которой можно определить конкретного человека;
c) все что угодно, что сам человек посчитает своими персональными данными: от паспортных данных до личных вещей.

2. Что из перечисленного указано на Вашей личной странице в социальной сети? (обведите все правильные варианты)
a) фамилия;
b) имя;
c) дата рождения;
d) информация о родственниках;
e) город проживания;
f) место учебы;
g) номер телефона;
h) фотографии с геолокацией.

3. Как часто в личной переписке Вы сообщаете собеседнику такие данные как: номер телефона, номер банковской карты, пароли.
a) никогда;
b) очень редко;
c) периодически;
d) очень часто.

4. На Ваш взгляд, с какими угрозами можно столкнуться в интернете?

Учитывая уровень навыков работы в интернете учеников 7–9 классов, авторы разработали викторину с соревновательным элементом.

Викторина «Цифровая защита»

Цель: сформировать основные принципы в культуре обращения с собственными персональными данными.

Задачи:

1. Научить школьников быстро распознавать информационные угрозы.
2. Сформировать четкое представление о различных категориях персональных данных.
3. Научить подростков защищать свои персональные данные в информационном пространстве.

Формат: игровая викторина.

Перед началом работы педагог делит группу на 2 команды. За каждый этап команды получают баллы. Та из них, которая набрала большинство, выигрывает.

Этапы:

1. Определение сообщений, содержащих угрозу.
2. Работа с карточками.
3. Анализ анкет.

Время проведения: 60–90 минут.

I этап

Максимальное количество баллов: 6.

Правильный ответ – 1 балл, неполный – 0,5 балла, правильное дополнение к ответам соперника – 0,5 балла.

Педагог: Часто нам приходят сообщения с просьбой занять денег, перейти по ссылке или осведомляющие о победе в розыгрышах призов. Больше половины из них созданы мошенниками. В этом задании вам надо будет не попасться на уловки мошенников и отличить сообщения, созданные мошенниками, от правдивого сообщения.

Каждая команда получает по 4 вопроса. Внимательно прочитайте их и определите: какое сообщение представляет угрозу, какое – нет.

Вопросы 1 команды:

1. Я занимаюсь ставками. Предлагаю вступить в мою команду инвесторов, я работаю по своей стратегии уже больше года. Сейчас я набираю в команду молодых ребят, которые в перспективе могут стать моими партнерами. Минимальные вложения – 2000 рублей. Заработок с этой минимальной ставки – 12000 рублей в первые же сутки!!! Работаю на своих условиях, всем своим инвесторам и партнерам предоставляю гарантии!

2. Здравствуй, поменял номер телефона. Теперь звони сюда восемь 99 шесть сто 53 шестнадцать восемьдесят 3.

3. Привет! Скинула наши фотографии с вечеринки сюда vk.cc8579419474.

4. Добрый день! Увидел на Вашей стене сбор денег на корм для бездомных собак. Готов помочь. Напишите номер карты, ФИО владельца и три цифры на обороте карты. Это необходимо для обмена валюты. Перевод делаю из Италии.

Вопросы 2 команды:

5. Здравствуй. Пишу курсовую работу, в рамках которой провожу социальный опрос. Пройди, пожалуйста, по ссылке https://www.survio.com/ru/ankety-udovletvorennosti-zakazcchikov и ответь на вопросы. Буду благодарен.

6. Доброго времени суток. Сегодня мы определили победителя конкурса vk.com/gamees?w=wall-170363487_73 Вы выиграли iPhone Xs Max. Прошу Вас заполнить следующие поля: ФИО, адрес получателя, номер телефона для связи. Доставка будет осуществляться в районе 4–10 дней. Стоимость почтового сбора составляет 800 рублей, которую Вы оплачиваете сейчас.

7. Еще раз привет. Сегодня виделись уже. Хотел у тебя занять 1000 рублей до среды. Помнишь Светку Соколову, сестру мою, так ей 16 лет завтра? Пригласила на день рождение и мне не удобно с пустыми руками идти. Выручишь?

8. Здаров! Тут слили базу данных, поищи свой bazadannyh2019.xlsx.

Ответы:

1 – угроза: неосознанная добровольная передача денежных средств мошенникам.

2 – безопасно: Лаборатория Касперского предлагает подобным образом шифровать номер телефона при передаче в интернете.

3 – угроза: переход по незнакомым ссылкам грозит заражению компьютера вирусами.

4 – угроза: для перевода средств другому лицу отправителю необязательно знать CVC2 Вашей карты (трёхзначный код). Скорее всего, мошенник хочет получить доступ к карте.

5 – безопасно: значок «s» в комбинации «https:» говорит о надежности сайта. Сам сайт «www.survio.com» можно проверить в интернете.

6 – угроза: выманивание денег на «почтовый сбор» за победу в конкурсе, в котором вы не принимали участия.

7 – угроза: лучше снова позвонить другу и убедиться, что это его просьба. Фраза «Сегодня виделись уже» не является достаточным основанием для доверия, так как о встрече могли знать третьи лица.

8 – угроза: переход по незнакомым ссылкам грозит заражению компьютера вирусами.

II этап

Максимальное количество баллов: 12 баллов.

Каждая правильно решенная карточка – 2 балла.

Педагог раскладывает на столе все 12 карточек и приглашает по одному представителю от каждой команды вытащить по 6 карточек.

На карточках написаны различные категории персональных данных (фамилия, имя, фотография, национальность, номер банковской карты, номер телефона, кличка домашнего питомца, государственный номер автомобиля, отпечаток пальца, кольцо, подаренное бабушкой, рост, паспортные данные).

Задача каждой группы заключается в том, чтобы в течение 10 минут ознакомиться с выбранными карточками и описать ситуации, когда предложенная категория в карточке выступает персональными данными и когда ее недостаточно для признания таковыми.

Возможные варианты ответов:

1. Фамилия. На конференции работу ученика отмечают как лучшую, называя только фамилию. В данном случае фамилия

Фамилия	**Имя**	**Фото**
Национальность	**Паспортные данные**	**Банковская карта**
Рост, вес, группа крови	**Кольцо, подаренное бабушкой**	**Номер телефона**
Кличка домашнего питомца	**Гос. номер автомобиля**	**Отпечаток пальца**

не является раскрытием персональных данных, поскольку учеников с подобной фамилией может быть большое количество, к тому же, не были указаны остальные данные, такие как город, школа, класс. Если же учитель делает замечание ученику в школе, называя его фамилию и класс – это разглашение персональных данных.

2. Имя. Само по себе имя не является персональными данными, но в совокупности с другой информацией, например, номером мобильного телефона, оно уже определяет конкретного человека.

3. Фотография. Изображение человека (фотография или видеозапись) является персональными данными, если оно позволяет установить конкретную личность. Таким образом, фотография «со спины» или без фокусировки на расстоянии не являются персональными данными. Кроме этого, если гражданин позировал за плату или же фотография сделана на общественных мероприятиях (концерт, конференция), то использование данного изображения без согласия является законным.

4. Национальность. Специальная категория персональных данных, которая, однако, выступает таковой только вместе с другими данными: ФИО, биометрические показатели и т. д.

5. Номер банковской карты. Всегда выступает персональными данными, так как даже обезличенные они косвенно указывают на номер банковского счета, который принадлежит конкретному физическому лицу.

6. Номер телефона. Если вам позвонили с рекламного агентства и назвали по имени, были использованы ваши персональные данные, если же в доступе компании только номер телефона, то этот звонок нельзя рассматривать в качестве обработки персональных данных.

7. Кличка домашнего питомца. Не является персональными данными.

8. Государственный номер автомобиля. Государственный регистрационный знак присваивается автомобилю, а не правообладателю, поэтому он, наравне с другими сведениями об автомобиле (марка, модель, пробег и др.) не являются персональными данными. Тем не менее, предоставление этой информации в открытый доступ может нести в себе информационные угрозу.

9. Отпечаток пальца. Биометрическая категория персональных данных, которая всегда выступает таковой, поскольку отпечатки пальцев – индивидуальны.

10. Кольцо. Личные вещи и имущество не являются персональными данными.

11. Рост. Биометрическая категория персональных данных. Однако он может идентифицировать конкретного человека только в совокупности с другими биометрическими, общими или специальными персональными данными. Например, данные о росте, весе, возрасте, ФИО.

12. Паспортные данные. В своей совокупности (серия, номер, код подразделения, ФИО и т. д.) они всегда выступают персональными данными. Только серия или отдел выдачи могут совпадать у разных людей.

III этап

Максимальное количество баллов – 10 баллов.

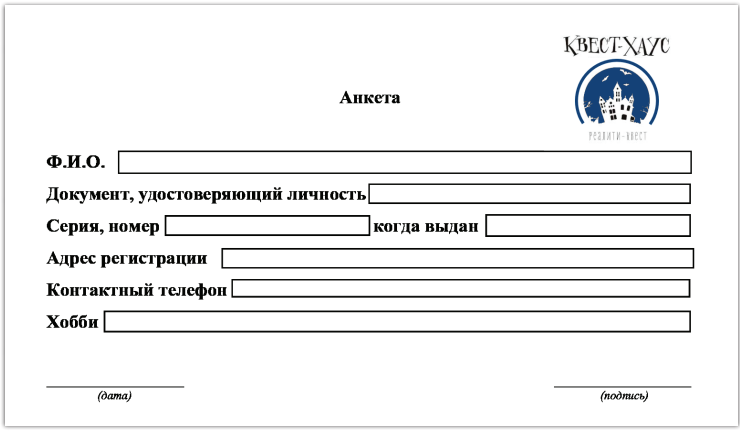
За каждую правильно проанализированную анкету команда получает по 5 баллов.

Педагог раздает каждой группе по 2 анкеты. В течение 10 минут команда обсуждает, какие персональные данные собираются оператором безосновательно или же и вовсе организация не вправе запрашивать. По истечению установленного времени команды меняются карточками. После командного обсуждения по два представителя от каждой команды делятся результатами.

Педагог: большое количество наших действий: будь то это покупка часов или поход в кино – предполагают передачу персональных данных. Иногда организации требуют от клиента/покупателя те персональные данные, которые те не обязаны передавать. Перед вами по 2 анкеты на оказание услуг в различных сферах. За 10 минут вы должны понять, в чем заключается ошибка составления анкеты.

Рис. 10
Комментарий: квест-комната может запросить в анкете хобби, чтобы знать тематику, которая интересна клиентам. Однако заполнение графы с паспортными данными является необязательным.

Рис. 11
Комментарий: как правило, кинотеатр не является оператором, который правомочен осуществлять сбор и хранение персональных данных своих посетителей, поэтому клиент имеет право отказать в предоставлении своих паспортных данных.



КВЕСТ-ХАУС

Анкета

Ф.И.О.

Документ, удостоверяющий личность

Серия, номер **когда выдан**

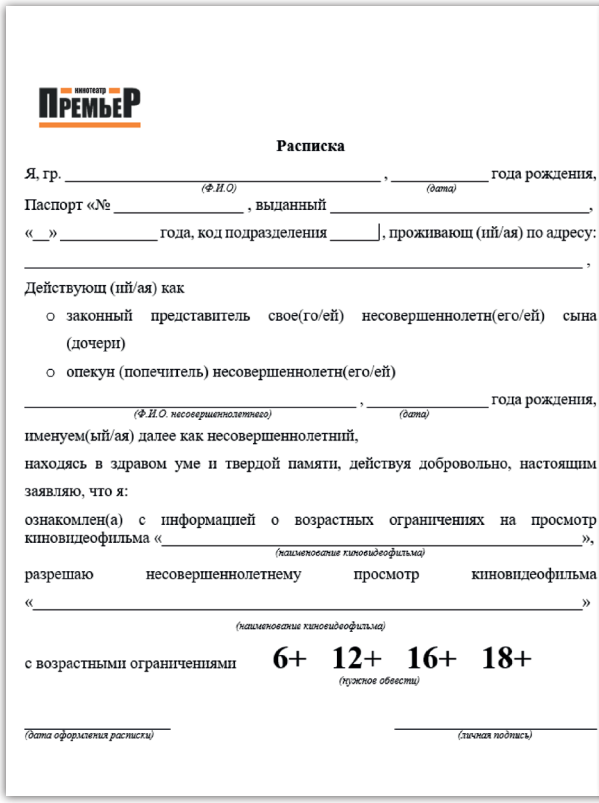
Адрес регистрации

Контактный телефон

Хобби

(дата) *(подпись)*

Рис. 10



кинотеатр ПРЕМЬЕР

Расписка

Я, гр. _____ (Ф.И.О), _____ (дата) года рождения,

Паспорт «№ _____ , выданный _____,

«__» _____ года, код подразделения _____, проживающ(ий/ая) по адресу:

_____,

Действующ(ий/ая) как

- законный представитель свое(го/ей) несовершеннолетн(его/ей) сына (дочери)
- опекун (попечитель) несовершеннолетн(его/ей)

_____ (Ф.И.О. несовершеннолетнего), _____ (дата) года рождения,

именуем(ый/ая) далее как несовершеннолетний,

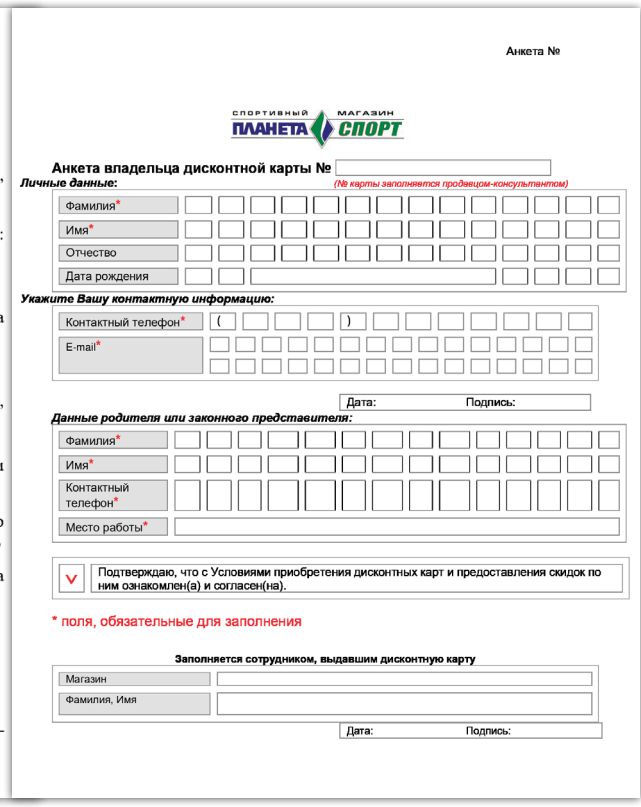
находясь в здравом уме и твердой памяти, действуя добровольно, настоящим заявляю, что я:

ознакомлен(а) с информацией о возрастных ограничениях на просмотр киновидеофильма «_____ (наименование киновидеофильма)»,

разрешаю несовершеннолетнему просмотр киновидеофильма «_____ (наименование киновидеофильма)»

с возрастными ограничениями **6+ 12+ 16+ 18+** (нужное обвести)

(дата оформления расписки) *(личная подпись)*



Анкета №

СПОРТИВНЫЙ МАГАЗИН ПЛАНЕТА СПОРТ

Анкета владельца дисконтной карты №

Личные данные: *(№ карты заполняется продавцом-консультантом)*

Фамилия* | Имя* | Отчество | Дата рождения

Укажите Вашу контактную информацию:

Контактный телефон* ( ) | E-mail*

Дата: Подпись:

Данные родителя или законного представителя:

Фамилия* | Имя* | Контактный телефон* | Место работы*

V Подтверждаю, что с Условиями приобретения дисконтных карт и предоставления скидок по ним ознакомлен(а) и согласен(на).

* поля, обязательные для заполнения

Заполняется сотрудником, выдавшим дисконтную карту

Магазин | Фамилия, Имя

Дата: Подпись:

Рис. 11 Рис. 12

Рис. 12

Комментарий: в анкете спортивного магазина не обязательно указывать контактный номер телефона и место работы родителя/опекуна. Получение этих данных может быть использовано в рекламных целях или для формирования незаконных баз данных.

Более того, если анкету выдали несовершеннолетнему — это нарушение закона. Согласно требованиям Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», согласие на обработку персональных данных лица, не достигшего 14 лет, дают его законные представители – родители, усыновители, опекуны или попечители. Обработка персональных данных лиц от 14 до 18 лет производится с разрешения самого несовершеннолетнего и письменного согласия его законного представителя.

ДОГОВОР
на оказание риелторских услуг

г. _____ «_____» _____ 2019 г.

Агентство недвижимости «Квадратный метр», именуемый в дальнейшем «Исполнитель», с одной стороны, и _____, именуемый в дальнейшем «Заказчик», с другой стороны, именуемые в дальнейшем «Стороны», заключили настоящий договор, в дальнейшем «Договор», о нижеследующем:

1. ПРЕДМЕТ ДОГОВОРА
1.1. Заказчик поручает, а Исполнитель принимает на себя обязательства по оказанию услуг поиска объекта недвижимости (далее – Объект), с целью использования его Заказчиком на основании договора аренды, субаренды, совместной деятельности, сотрудничества, ответственного хранения и пр.
1.2. Заказчик предъявляет следующие исходные требования к Объекту:
Месторасположение: _____;
Профиль: _____;
Площадь: _____;
Цена: _____ (за кв. метр в год);
Этаж: _____;
Парковка: _____;
Кол-во телефонов: _____;
Вид договора: _____.
1.3. В ходе выполнения Договора Заказчик имеет право изменить исходные требования к Объекту в письменной или устной форме.

2. ИСПОЛНИТЕЛЬ ОБЯЗАН
2.1. Провести поиск Объектов в соответствии с требованиями Заказчика и предложить найденные варианты Заказчику.
2.2. Организовать осмотр Заказчиком тех Объектов, которые он выберет из числа предложенных Исполнителем. Все Объекты, осмотренные Заказчиком, включаются в Лист просмотров (Приложение № 1), являющимся неотъемлемой частью Договора.

3. ЗАКАЗЧИК ОБЯЗАН
3.1. Оплачивать услуги Исполнителя в соответствии с условиями Договора.
3.2. До момента выполнения Исполнителем своих обязательств по Договору вступать в контакт с владельцами Объектов или представителями владельцев Объектов, найденных Исполнителем, только в присутствии Исполнителя, или с согласия Исполнителя.

4. ПОРЯДОК ПРИЕМА-СДАЧИ РАБОТ

4.1. Моментом выполнения Исполнителем обязательств по Договору является момент наступления первого события из числа перечисленных ниже:
4.1.1. Заключение Заказчиком Договора Аренды на указанный в Листе просмотров Объект, его части или другого помещения в том же здании.
4.1.2 Начало фактического использования Объекта Заказчиком. Под фактическим использованием Объекта Стороны понимают физическое пребывание Заказчика (его сотрудников) на территории Объекта более _____ рабочих дней.

5. ОПЛАТА УСЛУГ ИСПОЛНИТЕЛЯ

5.1. Стоимость услуг Исполнителя по Договору согласовывается Сторонами по каждому предложенному Объекту отдельно и указывается в Листе просмотров, оформленном как Приложение № 1 к Договору, перед осмотром Объекта.
5.2. Заказчик оплачивает услуги Исполнителя в течение _____ банковских дней с момента выполнения Исполнителем обязательств по Договору.
5.3. В случае просрочки оплаты Исполнитель вправе взыскать с Заказчика штраф из расчета _____% от стоимости услуг Исполнителя по Договору за каждый день просрочки.

6. ВСТУПЛЕНИЕ В СИЛУ И СРОК ДЕЙСТВИЯ ДОГОВОРА

6.1. Договор вступает в силу с момента подписания его Сторонами.
6.2. Договор действует в течение шести месяцев с момента подписания его Сторонами или до подписания Сторонами Акта приема-сдачи услуг. Данный договор составлен в двух экземплярах, имеющих равную юридическую силу, по одному экземпляру для каждой из Сторон.

7. ЮРИДИЧЕСКИЕ АДРЕСА И БАНКОВСКИЕ РЕКВИЗИТЫ СТОРОН

Исполнитель
Юр. адрес:
Почтовый адрес:
ИНН:
КПП:
Банк:
Рас./счет:
Корр./счет:
БИК:

Заказчик
Фамилия:
Имя:
Отчество:
Паспортные данные:
ИНН:
КПП:
Банк:
Рас./счет:

9. ПОДПИСИ СТОРОН

Исполнитель _____ Заказчик _____

Комментарий: договор, заключаемый с риелтором, на просмотр квартиры можно не заключать, так как нет уверенности, что риелтерское агентство может обеспечить сохранность паспортных и других персональных данных.
Кроме этого, риелтерский договор служит лишь на пользу агентству, и зачастую ограничивает возможности клиента в общении с собственником жилья.

10–11 классы

Согласно отчетам и исследованиям аналитического агентства «Statista» за 2018 год , среднестатистический российский пользователь интернета в возрасте от 16 до 24 лет проводит в социальных сетях почти три часа в день. Молодежь предпочитает даже искать информацию о брендах в соцсетях, а не в поисковиках, а четверть пользователей этой возрастной группы признаются, что большое количество лайков на странице бренда может склонить их к покупке. Все это говорит о чрезмерном доверии современной молодежи к виртуальному пространству.
В связи с этим авторами методических указаний была разработана серия кейсов с наиболее распространенными информационными угрозами.
Перед началом работы с кейсами рекомендуется провести среди учащихся анкетирование, которое выявит уровень их осведомленности в проблематике и поможет педагогу определить наиболее актуальные угрозы для конкретной группы, с которой будет проводиться работа.

Тест «Защита персональных данных от доступа злоумышленников в сети Интернет»

1. Как бы Вы сформулировали определение термина «персональные данные?»
2. Попадали ли Вы когда-нибудь в ситуацию, когда понимали, что произошла утечка Ваших персональных данных (взлом страницы в социальных сетях, потеря доступа к электронной почте и др.)?

a) постоянно;
b) несколько раз;
c) один раз;
d) никогда.

3. По шкале от 1 до 10, где 1 – «никогда», а 10 – «постоянно», ответьте на следующие вопросы (ставьте галочку или плюс):

Вопрос	1	2	3	4	5	6	7	8	9	10
Проводя время в Интернете, я часто оставляю данные о своем имени, фамилии, отчестве, возрасте (при регистрации новых учетных записей, записываясь на прием к врачу, заполняя различные анкеты и др.)										
Проводя время в Интернете, я часто оставляю свой номер телефона (при регистрации новых учетных записей, записываясь на прием к врачу, заполняя различные анкеты и др.)										
Проводя время в Интернете, я часто оставляю номер банковской карточки (совершая онлайн-покупки, оплачивая услуги телефонной связи, оплачивая дополнительные услуги и др.)										
Как Вы считаете, насколько опасной может быть утечка Ваших персональных данных в Интернете? (1 – «не вижу никаких опасностей», 10 – «максимальная угроза»)										

*Социальные сети в 2018 году: глобальное исследование / Сергеева Ю.В. 20.03.2018. URL: https://www.web-canape.ru/business/socialnye-seti-v-2018-godu-globalnoe-issledovanie/ (дата обращения: 12.07.2019).

Классный час по методике case-study

Цель кейсов в контексте данного занятия: привитие обучающимся старшей школы навыков обеспечения медиабезопасности при использовании сети Интернет и развитие медиаграмотности старшеклассников путем интерактивного метода case-study.

Кейсы – это заданные и основанные на реальных фактах ситуации, содержащие в себе некую проблему или противоречие, которые в ходе работы над анализом кейса необходимо решить.

Задачи, реализуемые в ходе проведения классного часа:

1. Привитие обучающимся компетенций по выявлению и оценке информационных угроз, исходящих от потенциально опасных онлайн-коммуникаций.

2. Обучение старшеклассников навыкам ответственного отношения к собственным персональным данным при нахождении в сети Интернет.

3. Обучение старшеклассников основам медиабезопасности, включающим использование технических средств защиты личной информации в интернете, активное применение функционала социальных сетей.

4. Развитие критического мышления старшеклассников относительно информации, распространяемой в сети Интернет и посредством иных электронных средств массовой коммуникации.

5. Обучение школьников контрманипулятивным технологиям касательно попыток вовлечения их в противоправную деятельность.

6. Привитие старшеклассникам навыков выявления мошеннических манипуляций в интернете.

7. Предупреждение совершения учащимися старшей школы правонарушений с использованием сети Интернет.

При проведении классного часа важно учесть возрастную категорию данных кейсов — старшеклассники как группа наиболее активных и осведомлённых о разных возможностях интернет-коммуникации ребят.

Проведение занятия необходимо выстраивать таким образом, чтобы ученики смогли свободно высказать собственную точку зрения по рассматриваемому вопросу, предоставить возможность им быть максимально услышанными.

Этапы работы с кейсом предполагают следующие шаги:

1. В начале педагогу необходимо акцентировать внимание школьников на том, как бы они поступили при возникновении такой ситуации, и после этого предложить прочитать непосредственно сам кейс.

2. Далее обучающиеся ознакамливаются с содержанием кейса (3–5 минут в зависимости от объема), отвечают на поставленные вопросы.

3. Путем ряда наводящих вопросов педагог направляет процесс решения кейса и формулирования важных выводов.

4. Подведение выводов по кейсу и ознакомление учеников с рекомендациями по обеспечению личной безопасности в информационном пространстве, исходя из информационных угроз, которые затронул данный кейс.

Рассмотрим все этапы подробно, иллюстрируя разбор каждого кейса.

Кейс № 1

Цель: проверить уровень бдительности учеников старшей школы относительно угроз, исходящих от подозрительных онлайн-коммуникаций.

Описание случая (зачитывается педагогом вслух или школьниками самостоятельно):

Представьте ситуацию. В социальной сети «ВКонтакте» вам приходит личное сообщение от

незнакомого вам человека следующего характера: «Привет, я в ..... году в .... школе учился вместе с твоим отцом. Не виделись с ним тысячу лет. Пришли мне его номер, хочу с ним связаться и вспомнить молодые годы».

Педагог: Как следует поступить в данной ситуации?

Далее педагог направляет ответы аудитории с целью формирования основного вывода о верном поведении в данной ситуации:

Возможный вариант ответа: убедитесь, что вам действительно написал человек, который лично знает вашего отца.

Вопросы, которые помогут установить эту информацию:

1. Перед тем как отвечать, спросите своего отца, действительно ли он знает этого человека?

2. При положительном ответе спросите, почему отправитель не написал напрямую отцу через социальные сети (если родитель имеет собственные учетные записи)?

3. Задайте вопросы, ответ на которые знает только друг детства.

Педагог: Какие угрозы несет описанная ситуация?

Возможные варианты ответа:

1. Угроза доступа к данным банковской карты и последующая утечка финансовых средств или же использование вашей карты для преступных махинаций.

2. Угроза потери доступа к социальным сетям и электронным ресурсам, к которым был привязан номер телефона.

3. Угроза шантажа или же отправки сообщений на этот номер (рекламных, провокационных, вирусных и др.).

Далее педагог подводит итоговые выводы по кейсу и знакомит старшеклассников со следующими рекомендациями:

1. Небезопасно сообщать номер телефона даже знакомым через социальные сети, так как персональные данные могут быть перехвачены на пути к получателю.

2. Если же все-таки нет другого способа, чтобы связаться с человеком, и вы полностью уверены, что вашим собеседником не является злоумышленник, то сообщайте номер телефона (в случае, если имеете несколько), к которому не привязаны ваши банковские карты или же социальные сети. Рекомендуется также сообщать номер телефона в интернете, используя текстовые данные или же закодированные, чередуя цифры или буквы (например, 89пять 2:54 ноль ноль ...).

Таким образом, соблюдая эти несложные правила, вы сможете обезопасить себя и своих близких.

Кейс № 2

Цель: проверить уровень бдительности учеников старшей школы относительно угроз, исходящих от подозрительных рассылок в социальных сетях.

Описание случая (зачитывается педагогом вслух или школьниками самостоятельно):

*Представьте ситуацию. В известной социальной сети Facebook ваш одноклассник пишет вам личное сообщение следующего характера «Привет, А***! Мне прислали твое фото. Посмотри https://foto-j9.net/a».*

Педагог: Как следует поступить в данной ситуации? Какие угрозы могут возникнуть, если человек перейдет на подобный сайт?

Возможные варианты ответа:

1. Угроза заражения устройства вирусными программами.

2. Угроза потери доступа к социальным сетям и электронным ресурсам.

3. Угроза утечки информации из социальной сети (личные фотографии, переписки и др.).

Педагог: Что бы вы порекомендовали делать в сложившейся ситуации?

Рекомендации:

1. Ни в коем случае не переходить по неизвестным и небезопасным ссылкам.

2. Проверять ссылки с помощью специальных серверов или сайтов (http://www.securrity.ru/url_analysis.html?url=++).

3. Прежде чем перейти по ссылке, стоит убедиться, что с вами общается ваш одноклассник, для этого нужно позвонить и спросить у него, что находится по данной ссылке и действительно ли он ее отправил; написать вашему другу и задать вопросы, на которые сможет ответить только он.

4. Не используйте один пароль для всех сервисов, которыми вы пользуетесь. Наиболее безопасным методом защиты своей страницы является использование двухфакторной аутентификации (при попытке входа в аккаунт вам на телефон приходит пароль, который при каждом входе меняется), также можно использовать хранилище паролей или же создавать надёжный пароль (свыше 15 символов), которые будут содержать какую-либо фразу известную только вам.

5. Используйте лицензионные антивирусники – они не дадут возможности перейти на незащищенный сайт.

Кейс № 3

Цель: проверить уровень медиабезопасности учеников старшей школы.

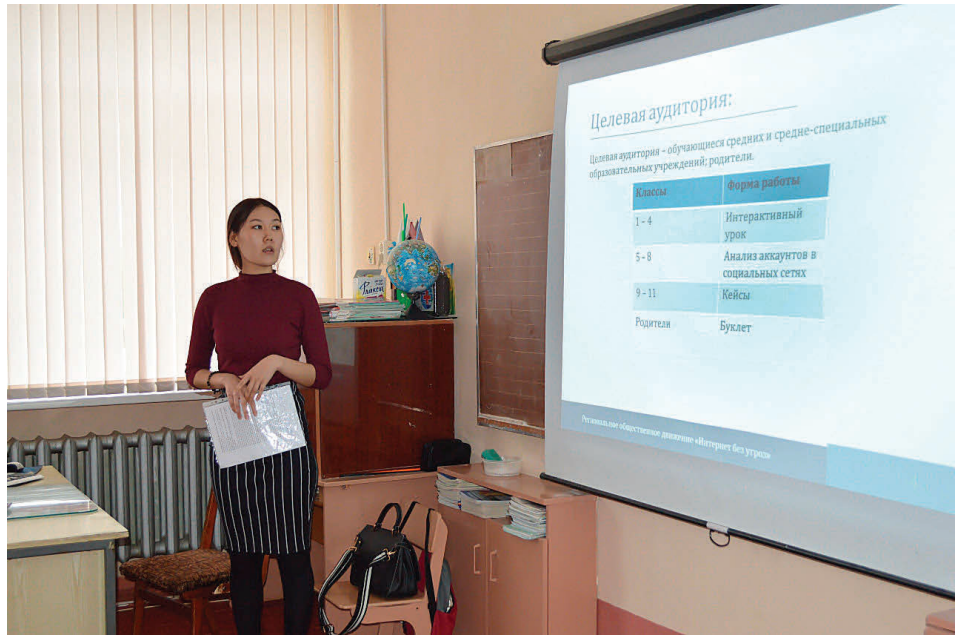
Описание случая: (зачитывается педагогом вслух или школьниками самостоятельно):

Представьте ситуацию. В социальной сети Одноклассники к вам на страничку зашел человек, на аватарке которого изображена ваша фотография, а в профиле указаны все ваши личные данные».

Педагог: Как следует поступить в данной ситуации? Нужно ли как-то отреагировать на эту ситуацию или стоит просто отклонить запрос в друзья? Давайте определим угрозы, которые данная ситуация несет, и сформулируем рекомендации, помогающие минимизировать эти угрозы.

Возможные варианты ответа:

1. Угроза заключается в том, что под вашим именем могут быть совершены разного рода



преступные махинации (помимо того, что украдены ваши персональные данные, также может быть выведана информация о ваших знакомых, от вашего лица может совершаться продажа наркотических средств, происходить другие противоправные манипуляции и др.).

Рекомендации:

1. Сообщайте на вашей станице как можно меньше персональной информации о себе.

2. Помните, что все, что вы выкладываете в сеть, остается там навсегда.

3. Чтобы удалить свои персональные данные со страницы, прежде всего свяжитесь с администрацией ресурса, где она опубликована. Подкрепите требования ссылками на нормы Федерального закона «О персональных данных» от 27.07.2006 г. № 152-ФЗ № 152, который запрещает использовать информацию без разрешения субъекта данных. Предупредите, что в случае отказа вы вправе обратиться в суд согласно статье 24 данного ФЗ (ответственность за нарушение требований ФЗ № 152).

4. Чтобы удалить личные данные из результатов поиска, обратитесь в техническую поддержку поискового сервиса. Например, у «Яндекса» есть специальная форма «Сообщить о нарушении». Однако компания предупреждает: поисковая машина индексирует страницы, которые принадлежат третьим лицам, и не отвечает за их содержание. «Яндекс» может помочь пользователю, но только в том случае, если данные удалили, а они по-прежнему видны в поисковой выдаче.

5. Когда невозможно установить источник распространения персональных данных, обратитесь в надзорные органы: Прокуратуру или в Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

Кейс № 4

Цель: проверить информированность учеников старшей школы об основных способах денежного мошенничества, осуществляемого злоумышленниками через сеть Интернет.

Описание случая (зачитывается педагогом вслух или школьниками самостоятельно):

Представьте ситуацию. В известной социальной сети «ВКонтакте» вам приходит сообщение от друга с текстом: «Привет! У меня проблемы, пришли срочно 1000 на эту карту сбера ..., потом объясню!»

Педагог: какова главная угроза такого сообщения? Сталкивался ли кто-то с такой ситуацией и как на нее лучше отреагировать?

Возможные варианты ответа:

1. Перевод денежных средств мошеннику.

Рекомендации:

1. Необходимо убедиться, действительно ли вам пишет друг, для этого достаточно позвонить ему и объяснить ситуацию. Если друг не отвечает, то можно написать ответное сообщение, но не переводить деньги пока не убедитесь, что отправитель письма – действительно ваш друг. Это можно сделать с помощью дополнительных вопросов, ответы на которые знает только он (как зовут питомца, имя классного руководителя и т. д.). Как правило, этот способ помогает вывести мошенников на чистую воду, даже если они начали с вами переписку.

2. Чаще всего такой схемой обмана пользуются мошенни-

ки в соцсетях, производя массовую рассылку одинаковых сообщений от лица личности взломанной страницы в надежде наткнуться на неразборчивого человека, который отправит деньги, не выясняя.

Педагог: Что можно посоветовать другу, страницу которого взломали?

Рекомендации:

1. Нужно поменять пароль. Надежный пароль должен представлять из себя какую-либо фразу, которую легко ассоциативно запомнить хозяину страницы, зафиксированную латинскими буквами с использованием дополнительных символов. Менять пароль рекомендуется только тогда, когда он себя дискредитировал (как в данном случае – после взлома). Рекомендуется использовать разные пароли для разных платформ и, конечно же, не сообщать никому такие данные!

2. Если вы заметили, что от вашего имени была произведена подобная рассылка, необходимо сообщить всем своим подписчикам о мошеннических действиях (через личные оповещения и на стене). Такую рассылку важно сделать даже в том случае, если вы слишком поздно обнаружили взлом страницы, так как некоторые ваши подписчики могут увидеть сообщение мошенников намного позже и перевести деньги.

Кейс № 5

Цель: проверить уровень медиаграмотности учеников старшей школы.

Описание случая (зачитывается педагогом вслух или школьниками самостоятельно):

Представьте ситуацию. В социальной сети «ВКонтакте» вам приходит сообщение от друга сделать репост публикации, в которой содержится не совсем для вас понятная информация о важности людям славянского происхождения объединяться, подкрепленная историческими сводками, фотографиями с непонятной символикой.

Педагог: Стоит ли выполнять просьбу друга или все-таки отказаться, несмотря на то, что он очень просит вас это сделать? Какие угрозы может нести предлагаемое действие?

Возможный вариант ответа:

1. Угроза заключается в том, что в данной публикации могут содержаться материалы, признанные экстремистскими: текст подобного описания может быть признан разжигающим межнациональную рознь и нарушающим законодательство РФ. За распространение таких вещей в интернете существует серьезное наказание!

Рекомендации:

1. Не публикуйте на своих страницах в социальных сетях материалы, если Вы не понимаете их содержания.

2. Не публикуйте на своих страницах материалы, которые могут оскорблять других людей по национальному, религиозному, политическому и другим признакам.

3. Не публикуйте материалы (новости), если вы не уверены в их достоверности. Распространение фейковых новостей только наносит вред развитию сети Интернет и также регулируется законом.

4. Обратите более пристальное внимание на страницу вашего друга, попросившего сделать репост: увлекается ли он каким-то радикальными течениями, входит ли в состав радикальных органи-

заций? Возможно, вашему другу нужна помощь.

Кейс № 6

Цель: научить старшеклассников выявлять фейковые новости и не поддаваться манипуляции в сети.

Описание случая (зачитывается педагогом вслух или школьниками самостоятельно):

Представьте, что в нескольких чатах в мессенджере WhatsApp вы увидели сообщение, массово распространяемое участники беседы, со следующим содержанием: «У меня дядя работает в полиции. Он сказал, что сейчас под предлогом чем то помочь в тачке детей заталкивают и увозят,а ещё щас раздают бесплатные живачки, а это оказывается спайс, в загородном уже увезли на скорой пару детей, ели откачали. Предупредите детей, пусть будут осторожнее».

Педагог: Стоит ли распространять этот текст? Какую цель могут преследовать авторы такого сообщения?

Возможный вариант ответа:

1. Угроза стать подверженным манипуляции и поспособствовать распространению фейковой новости.

Рекомендации:

1. Стоит критически оценивать всю получаемую информацию. Даже если это сообщение активно тиражируют ваши знакомые – это не повод считать ее истиной. Проверьте, были ли подобные рассылки в сети ранее.

2. Фейковую информацию возможно распознать по определенным признакам. Приведем некоторые из них:

• Чем больше эмоций в сообщении, тем большее подозрение должно вызвать у вас содержание.

• Проверьте наличие данной новости на других сайтах. В новостной журналистике часто применяется правило «трёх источников». Если вы не получите ни одной новости по этому запросу, особенно на порталах официальных СМИ, это с большой вероятностью говорит о том, что информация — фейк.

• Кроме этого, специалисты рекомендуют обращать внимание на наличие свидетелей, визуальных подтверждений (дополнительные фото- и видеоматериалы, прямые трансляции в социальных сетях и др.).

Кейс № 7

Цель: привитие навыков выявления мошеннических манипуляций в интернете.

Описание случая (зачитывается педагогом вслух или школьниками самостоятельно):

В социальной сети «ВКонтакте» в одной из групп, на которую вы подписаны, появился следующий пост, в котором сказано о закрытии приюта для животных. К посту прикреплены несколько фотографий собак. В сообщении сказано, что большинство животных уже успели раздать, однако если не заберут оставшихся щенят, их усыпят. Прикреплен номер телефона, по которому можно позвонить и забрать питомца.

Педагог: Кто-нибудь сталкивался с подобными случаями? Есть ли какие-то возможные угрозы для вас и как лучше поступить в данной ситуации?

Возможные варианты ответа:

1. Списание денежных средств с номера мобильного телефона после совершения звонка на указанный телефон.

Рекомендации:

1. Зачастую мошенники используют самые правдоподобные истории, чтобы вынудить жертву совершить какое-либо действие, при этом акцент делается на повышенную эмоциональную составляющую ситуации. В данном случае наиболее вероятно мошенничество, при котором звонок на указанный номер телефона будет считаться автоматическим принятием платной услуги, за которую у вас спишут деньги.

2. Даже если вы готовы взять питомца, не спешите звонить по указанному номеру. Проверьте по поиску в интернете: было ли такое объявление раньше или размещено ли оно на других ресурсах? Если объявление размещалось неоднократно в течение длительного срока, то, скорее всего, его авторы — мошенники. При закрытии приюта его владельцы не смогут месяцами ждать новых хозяев. Если же объявление размещено впервые и оно распространено на достоверных и авторитетных ресурсах – это хороший признак, что вас не пытаются обмануть. Кроме этого, данное объявление должно появиться и на других зоозащитных страничках в социальных сетях.

3. Найдите в интернете адрес приюта и его контактные данные. Если номер, который вы нашли не совпадает с указанным в сообщении, скорее всего, вас пытаются обмануть.

4. Насторожить должен и тот факт, если вам совершенно бесплатно предлагают забрать породистого животного. Как правило, владельцы приютов или заводчики продают их на специализированных рынках животных.

АНО НЦПТИ

Автономная некоммерческая организация «Национальный центр противодействия терроризму и экстремизму в молодежной среде и сети Интернет» создана в 2018 году на базе регионального общественного движения Ростовской области «Интернет без угроз».

Основные виды деятельности АНО «НЦПТИ»:

- сбор, обобщение и анализ информации о противоправном контенте в сети Интернет, оказывающей негативное воздействие на молодежь;

- передача собранной информации в правоохранительные органы, а также министерства и ведомства, занимающиеся противодействием распространению противоправных материалов в молодежной среде;

- информационно-аналитическое сопровождение федеральных и региональных органов исполнительной власти по вопросам противодействия радикальным идеологиям в молодежной среде, а также формирования культуры медиабезопасности и информационной безопасности;

- информационно-просветительская деятельность в сфере противодействия распространению экстремизма и идеологии терроризма в молодежной среде, а также формирования культуры медиабезопасности и прививания навыков работы с персональными данными;

- разработка образовательных курсов (в том числе и дистанционных) и обучение специалистов из государственных и муниципальных учреждений, правоохранительных органов, образовательных организаций и научных учреждений по вопросам обеспечения информационной безопасности, противодействия идеологии терроризма и экстремизму, медиабезопасности и другим технологиям профилактики негативного влияния на молодежную среду;

- организация и проведение информационно-профилактических мероприятий (конференций, форумов, семинаров, круглых столов, стратегических сессий и других форматов) по обеспечению информационной и комплексной безопасности, противодействию распространению радикальных идеологий и прочих факторов, оказывающих негативного влияние на молодежную среду;

По вопросам сотрудничества:

Директор: Быкадорова Александра Сергеевна

Адрес: 344016, Ростовская обл., Ростов-на-Дону, пр. Театральный, 85, оф. 402

Адрес электронной почты: bykadorova@ncpti.ru

Телефон / факс: 8 (961) 318-57-64

Сайт: http://интернетбезугроз.нцпти.рф/

Страничка в социальной сети «ВКонтакте»: https://vk.com/internetwithouthreats

Реквизиты АНО «НЦПТИ»

Автономная некоммерческая организация «Национальный центр противодействия терроризму и экстремизму в молодежной среде и сети Интернет» (АНО «НЦПТИ»)

ИНН 6163212926

КПП 616301001

ОГРН 1186196059840

Корреспондентский счет 30101810600000000602

БИК 046015602

Расчетный счет 40703810552090002060

Наименование учреждения банка: Юго-западный банк ПАО Сбербанк

Местонахождение банка: 344068 г. Ростов-на-Дону, ул. Евдокимова, 37

ИНН/КПП банка 7707083893/ 616443001

БИК банка 046015602

Юридический адрес: 344010, Ростов-на-Дону, пр. Театральный, 85, оф. 402, тел. (863) 3105383

Организаторы проекта

АНО НЦПТИ

ПРАВИТЕЛЬСТВО
РОСТОВСКОЙ ОБЛАСТИ

Партнеры проекта

МИНИСТЕРСТВО ОБЩЕГО И ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ РОСТОВСКОЙ ОБЛАСТИ

УПРАВЛЕНИЕ РОСКОМНАДЗОРА ПО РОСТОВСКОЙ ОБЛАСТИ

Комитет по молодежной политике Ростовской области
донмолодой.рф

ИНТЕРНЕТ БЕЗ УГРОЗ

АНТИТЕРРОРИСТИЧЕСКАЯ КОМИССИЯ РОСТОВСКОЙ ОБЛАСТИ

ФИРОН
ФОНД ИННОВАЦИОННОГО РАЗВИТИЯ ОБРАЗОВАНИЯ И НАУКИ

Сайт проекта:
культ-просвет.нцпти.рф