# Методический сборник
# для подготовки и проведения классного часа для школьников
# по вопросам информационной безопасности

Составитель:

Балагурова А.К.,

помощник проректора, директора

Центра цифровой трансформации образования

ГУ ДПО «ИРО Забайкальского края»

г. Чита
2022 год

# Содержание

# Введение

Методический сборник разработан для оказания информационной и методической поддержки педагогического работника в подготовке и проведении классного часа для школьников разных возрастных категорий по вопросам информационной безопасности.

Приведенные формы работы с учащимися при проведении классного часа по вопросам информационной безопасности не являются обязательными и единственно верными, основная идея – сделать классный час интересным, эффективным и полезным, поспособствовать формированию навыков информационной безопасности, соответствующих определенному школьному возрасту.

Сборник содержит рекомендации по проведению классного часа (или другого занятия, в рамках которого уместно будет осветить тему информационной безопасности) для школьников по вопросам информационной безопасности. Рекомендации разделены соответственно возрастным категориям учащихся.

Сборник также содержит электронные ресурсы, которые будут полезны педагогическому работнику при подготовке к занятию, посвященному информационной безопасности.

## Начальная школа 1 - 4 классы

**Цель:** создание условий для повышения уровня грамотности учащихся в вопросах информационной безопасности

**Задачи:**

- ознакомить учащихся с правилами ответственного и безопасного поведения в современной информационной среде;

- объяснить основы сетевого этикета;

- обсудить правила безопасной работы в сети Интернет;

- выявление угроз и пути их решения при работе в сети Интернет.

**Ожидаемые результаты:** повышение уровня осведомленности учащихся о проблемах информационной безопасности при использовании сети Интернет, потенциальных рисках и путях защиты от сетевых угроз

Учащихся начальных классов рекомендуется ознакомить со следующими аспектами:

- с правилами ответственного и безопасного поведения в современной информационной среде, способах защиты от противоправных посягательств в сети Интернет и мобильной (сотовой) связи;

- как критически относиться к сообщениям в СМИ (в т.ч. электронных), мобильной (сотовой) связи, как отличить достоверные сведения от недостоверных, как избежать вредной и опасной для них информации, как распознать признаки злоупотребления их доверчивостью и сделать более безопасным свое общение в сети Интернет;

- как общаться в социальных сетях (сетевой этикет), не обижая своих виртуальных друзей, и избегать выкладывания в сеть компрометирующую информацию или оскорбительные комментарии ит.д.

Большое значение для эффективности урока информационной безопасности имеет не только содержание, но и форма его проведения.

Целесообразно использовать для 1-4 классов – урок-путешествие, урок-викторину, урок-соревнование, урок-игру, беседу.

**Ход занятия**

В качестве примера приводится урок-сказка.

Рекомендуется подкрепить сказку презентационным материалом.

«Сказка о золотых правилах безопасности в Интернет»

В некотором царстве, Интернет - государстве жил-был Смайл-царевич- Тьютор-Королевич, который правил славным городом ИнфоБезом.

И была у него невеста – прекрасная Смайл-царевна-Он-лайн-Королевна,день и ночь проводившая в виртуальных забавах.

Сколько раз предупреждал еѐ царевич об опасностях, подстерегающихв сети, но не слушалась его невеста.

Не покладая рук трудился Смайл-царевич, возводя город ИнфоБез, заботился об охране своих границ и обучая жителей города основам безопасности в Интернет-государстве.

И не заметил он, как Интернет- паутина всѐ-таки затянула Смайл-царевну в свои коварные сети.

Погоревал – да делать нечего: надо спасать невесту.

Собрал он рать королевскую - ИнфоБезову – дружину дистанционную.

Стали думать головы мудрые, как вызволить царевну из плена виртуального.

И придумали они «Семь золотых правил безопасного поведения в Интернет», сложили их в котомку Смайл-царевичу, и отправился он невесту искать.

Вышел на поисковую строку, кликнул по ссылкам поганым, а они тут как тут: сообщества Змея-искусителя-Горыныча, стрелялки Соловья-разбойника, товары заморские купцов шоповских, сети знакомств-зазывалок.

Как же найти-отыскать Смайл-царевну?

Крепко задумался Тьютор-королевич, надел щит антивирусный, взял в руки меч-кладенец кодовый, сел на коня богатырского и ступил в трясину непролазную.

Долго бродил он, отбиваясь от реклам зазывающих и спамов завлекающих.

И остановился на распутье игрища молодецкого трѐхуровневого, стал читать надпись на камне, мохом заросшим: на первый уровень попадѐшь – времени счѐт потеряешь, до второго уровня доберѐшься – от родных-близкихотвернѐшься, а на третий пойдѐшь - имя своѐ забудешь.

И понял Смайл-царевич, что здесь надо искать невесту.

Взмахнул он своим мечом праведным и взломал код игрища страшного!

Выскользнула из сетей, разомкнувшихся Смайл - царевна, осенила себяпаролем честным и бросилась в объятия своего суженого.

Обнял он свою невесту горемычную и протянул котомочку волшебную со словами поучительными: «Вот тебе оберег от козней виртуальных, свято соблюдай наказы безопасные!»

1. Всегда помни своѐ Интернет-королевское имя (E-mail, логин, пароли) ине кланяйся всем подряд (не регистрируйся везде без надобности)!
2. Не поддавайся ярким рекламам-указателям и не ходи тропками, путанными на подозрительные сайты: утопнуть в трясине можно!
3. Если пришло письмо о крупном выигрыше – это «обманная грамота»: просто так выиграть невозможно, а если хочешь зарабатывать пиастры, нужно участвовать в полезных обучающих проектах !
4. Чтобы не забыть тропинку назад и вернуться вовремя, бери с собой Клубок волшебный (заводи себе будильник, садясь за компьютер)!
5. Если хочешь дружить с другими царствами-государствами, изучай полезные сервисы: они помогут тебе построить «Мой королевский мир», свой царский блог, форум для глашатаев важных – друзей званных
6. Не забывай обновлять антивирусную программу – иначе вирус

Серый Волк съест весь твой компьютер!

7. Не скачивай нелицензионные программные продукты – иначе пиратыпотопят твой корабль в бурных волнах Интернета!

Залилась совестливыми слезами дева красная, дала своему наречѐнному слово честное, что не будет пропадать в забавах виртуальных, а станет трудиться на благо народа города своего ИнфоБеза, сама начнѐт обучаться и помогать будет люду заблудшему и погрязшему в трясине сетевой.

И зажили они дружно и счастливо с мечтою расширить границы образовательные.

После прослушивания сказки необходимо обсудить и выявить основные аспекты информационной безопасности, выявить угрозы и пути защиты от них.

Учитель начинает обсуждение с вопроса к аудитории: «Какие угрозы подстерегали королевича и царевну?». Просит учеников перечислить опасности, которые могут угрожать человеку, его персональному компьютеру, мобильным устройствам. На доске фиксируются ответы учеников.

Обсуждение основных правил защиты от главных киберугроз. Все ответы детей записываются на доске.

При обсуждении внимание учеников обращается на то, откуда может исходить опасность.

После обсуждения на доске записаны основные правила защиты от киберугроз:

1. Нельзя оставлять в публичном доступе или отправлять незнакомцам по почте, при общении в социальной сети или в чате контактную информацию (адрес, телефон) - любой злоумышленник может выследить человека по его адресу или номеру телефона.

2. Нельзя соглашаться на уговоры незнакомых людей о личной

встрече. Подобные предложения лучше игнорировать, а общение со слишком настойчивым человеком прекратить.

3. Не надо публиковать адрес своей электронной почты ни на каких форумах, сайтах сообществ и социальных сетей. Он может стать добычей спамеров, и почта после этого наполнится мусорными письмами.

4. Не следует переходить по ссылкам в сообщениях от неизвестных адресатов. Это может быть небезопасно, поскольку сообщение может быть отправлено злоумышленниками.

5. Нельзя переходить по ссылкам в сообщениях с чрезмерно заманчивыми предложениями, например, поднять «рейтинг» учетной записи или получить «супервозможности» в социальной сети. Чаще всего такие сообщения рассылают мошенники для того, чтобы заманить пользователя на вредоносную веб-страницу и заразить его компьютер вирусом.

6. Не следует обращать внимания на предложение бесплатных подарков, легкого заработка, сообщения о получении наследства и т.п. Такие сообщения рассылают только мошенники.

Примеры других сказок о безопасности в сети Интернет для детей

- Сказка о Колобке Смайлике и Интернете https://teremok-1.tvoysadik.ru/upload/tsteremok_1_new/files/9d/1e/9d1e55ba0f69a3e304135b4d7e8ad80f.pdf

- Как Мышонок учился безопасному поведению в сети Интернет https://teremok-1.tvoysadik.ru/upload/tsteremok_1_new/files/06/f8/06f8962a74f12c2a72031accd303e116.pdf

Рекомендуется продемонстрировать учащимся мультфильмы о безопасности в сети Интернет. Примеры роликов приведены ниже.

- https://yandex.ru/video/preview/8254694210029947537

- https://yandex.ru/video/preview/15241746767284006816

## Основная школа (5 - 7 и 8 - 9 классы)

**Цель:** создание условий для повышения уровня грамотности учащихся в вопросах информационной безопасности, расширение знаний учащихся о кибербезопасности и киберугрозах, формирование навыков их распознавания и оценки рисков, их минимизация

**Задачи:**

- ознакомить учащихся с нормативно-правовой базой;

- ознакомить обучающихся с адресами помощи в случае интернет-угрозы и интернет-насилия, номером всероссийского детского телефона доверия;

- выявить и обсудить основные правила обеспечения информационной безопасности в сети Интернет, научиться выявлять риски и минимизировать их;

- закрепить полученные знания путем выполнения творческого задания.

**Ожидаемые результаты:** повышение уровня осведомленности учащихся о проблемах информационной безопасности при использовании сети Интернет, умение оценивать потенциальные риски и минимизировать их.

В ходе урока «Информационная безопасность» в среднем звене целесообразно познакомить обучающихся с международными стандартами в области информационной безопасности детей, которые отражены в российском законодательстве:

- Федеральный закон Российской Федерации № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (Закон определяет информационную безопасность детей как состояние защищенности, при котором отсутствует риск, связанный с причинением информацией (в том числе распространяемой в сети Интернет) вреда их

здоровью, физическому, психическому, духовному и нравственному развитию.);

- № 252-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию», (направленный на защиту детей от разрушительного, травмирующего их психику информационного воздействия, переизбытка жестокости и насилия в общедоступных источниках массовой информации, от информации, способной развить в ребѐнке порочные наклонности, сформировать у ребѐнкаискаженную картину мира и неправильные жизненные установки.)

Важно ознакомить обучающихся с адресами помощи в случае интернет- угрозы и интернет-насилия, номером всероссийского детского телефона доверия(https://politech47.mskobr.ru/files/informaciya_o_liniyah_pomowi_v_sluchae_internet-ugroz.pdf).

Линия помощи в случаях Интернет-угроз «Горячая линия». На «Горячую линию» можно попасть круглосуточно, набрав адрес www.saferunet.ru и нажав на красную кнопку «Горячая линия».

Линия помощи «Дети онлайн». Линия помощи «Дети онлайн» – служба телефонного и онлайн консультирования для детей и взрослых по проблемам безопасного использования детьми и подростками Интернета и мобильной связи. Обратиться на «Линию помощи» можно:

- по телефону 8 800 250 00 15 (с 9 до 18 по рабочим дням, время московское)

- по электронной почте helpline@detionline.com •

- на сайте www.detionline.com

Возможны следующие формы проведения урока: урок - пресс-конференция, урок-викторина, урок-соревнование, урок-презентация проектов, урок-практикум, урок-встреча с системными администраторами и т.д.

В качестве примера для учащихся 5-7 классов предлагается урок - беседа «10 правил безопасности в Интернете».

Каждый современный человек, ежедневно проводит время в интернете.Но интернет - это не только источник информации и возможность общаться на расстояние, но и угроза информационной безопасности. Вы можете скачать из сети компьютерный вирус, Вашу учетную запись или адрес электронной почты, могут взломать злоумышленники.

Правила безопасности в интернете.

1) Используйте надежный пароль. Первое и главное правило сохранности Ваших данных, учетных записей, почтовой пересылки это надежный пароль. Много раз хакеры взламывали страницы в социальных сетях или почтовые адреса из-за того, что пользователь ставил простой пароль. Вы ведь не хотите, чтобы Ваши личную переписку узнал кто-то чужой? Используйте генератор паролей, чтобы получить надежный пароль.

Генератор паролей создается, чтобы помочь вам с придумыванием устойчивых к взлому и легко запоминающихся паролей.

Часто бывает: вы зарегистрировались где-нибудь, а там просят: «введите пароль». В спешке приходится вводить что-нибудь типа qwerty или 12345. Последствия могут быть фатальными для вашего аккаунта: при попытке взлома такие пароли проверяются в первую очередь. Чтобы этого не происходило, надо создавать сложный пароль, желательно состоящий из букв разного регистра и содержащий цифры и другие символы. Для создания таких паролей существуют специальные программы. Но, на наш взгляд, гораздо легче набрать наш адрес и просто выбрать понравившийся пароль.

- Советы:
- Выбирайте пароль посложнее, состоящий из символов разного регистра, с цифрами и для абсолютной надёжности - знаками препинания.
- Не используйте пароль, связанный с теми данными, которые могут

быть о вас известны, например, ваше имя или дату рождения.

- Пароли, которые вы видите на экране создаются в реальном времени на вашем компьютере, поэтому исключена возможность перехвата пароля по сети. Разные посетители сайта видят разные пароли. Если вы зайдете на сайт второй раз, пароли будут другими.

- Вы можете выбрать пункт меню браузера "Файл|Сохранить как...", чтобы пользоваться генератором паролей в оффлайне.

- Генератор паролей полностью прозрачен: скачайте файл passwd.js, чтобы увидеть, как создается пароль, и убедиться в абсолютной надежности.

2) Заходите в интернет с компьютера, на котором установлен фаервол или антивирус с фаерволом. Это в разы уменьшит вероятность поймать вирусили зайти на вредоносный сайт.

3) Заведите один основной почтовый адрес и придумайте к нему сложный пароль. При регистрации на форумах, в соц. сетях и прочих сервисах Вы будете указывать его. Это необходимо если Вы забудете пароль или имя пользователя. Ни в коем случае не говорите, никому свой пароль к почте, иначе злоумышленник сможет через вашу почту получить доступ ко всем сервисам и сайтам, на которых указан Ваш почтовый адрес.

4) Если Вы хотите скачать какой-то материал из интернета, на сайте где не нужна регистрация, но от Вас требуют ввести адрес своей электронной почты, то, скорее всего, на Ваш адрес будут высылать рекламу или спам. В таких случаях пользуйтесь одноразовыми почтовыми ящиками.

5) Скачивайте программы либо с официальных сайтов разработчиков. Не скачивайте программы с подозрительных сайтов или с файлообменников. Так Вы уменьшите риск скачать вирус вместо программы.

6) Не нажимайте на красивые баннеры или рекламные блоки на сайтах, какими бы привлекательными и заманчивыми они не были. В лучшем случае, Вы поможете автору сайта получить деньги, а в худшем - получите вирус. Используйте плагины для браузеров, которые отключают

рекламу на сайтах.

7) Если Вы работаете за компьютером, к которому имеют доступ другие люди (на роботе или в интернет кафе), не сохраняйте пароли в браузере. В противном случае, любой, кто имеет доступ к этому компьютеру,сможет зайти на сайт, используя Ваш пароль.

8) Не открывайте письма от неизвестных Вам пользователей (адресов). Или письма с оповещением о выигрыше в лотереи, в которой Вы просто не участвовали.

9) Не нажимайте на вплывающие окна, в которых написано, что Ваша учетная запись в социальной сети заблокирована. Это проделки злоумышленников! Если Вас вдруг заблокируют, Вы узнаете об этом, зайдя в эту социальную сеть, или администрация отправит Вам электронное письмо.

10) Периодическим меняйте пароли на самых важных сайтах. Так Вы уменьшите риск взлома вашего пароля. Пользуясь этими правилами безопасности в интернете, Вы существенно уменьшите риск получить вирус на свой компьютер или потерять учетную запись на любимом сайте.

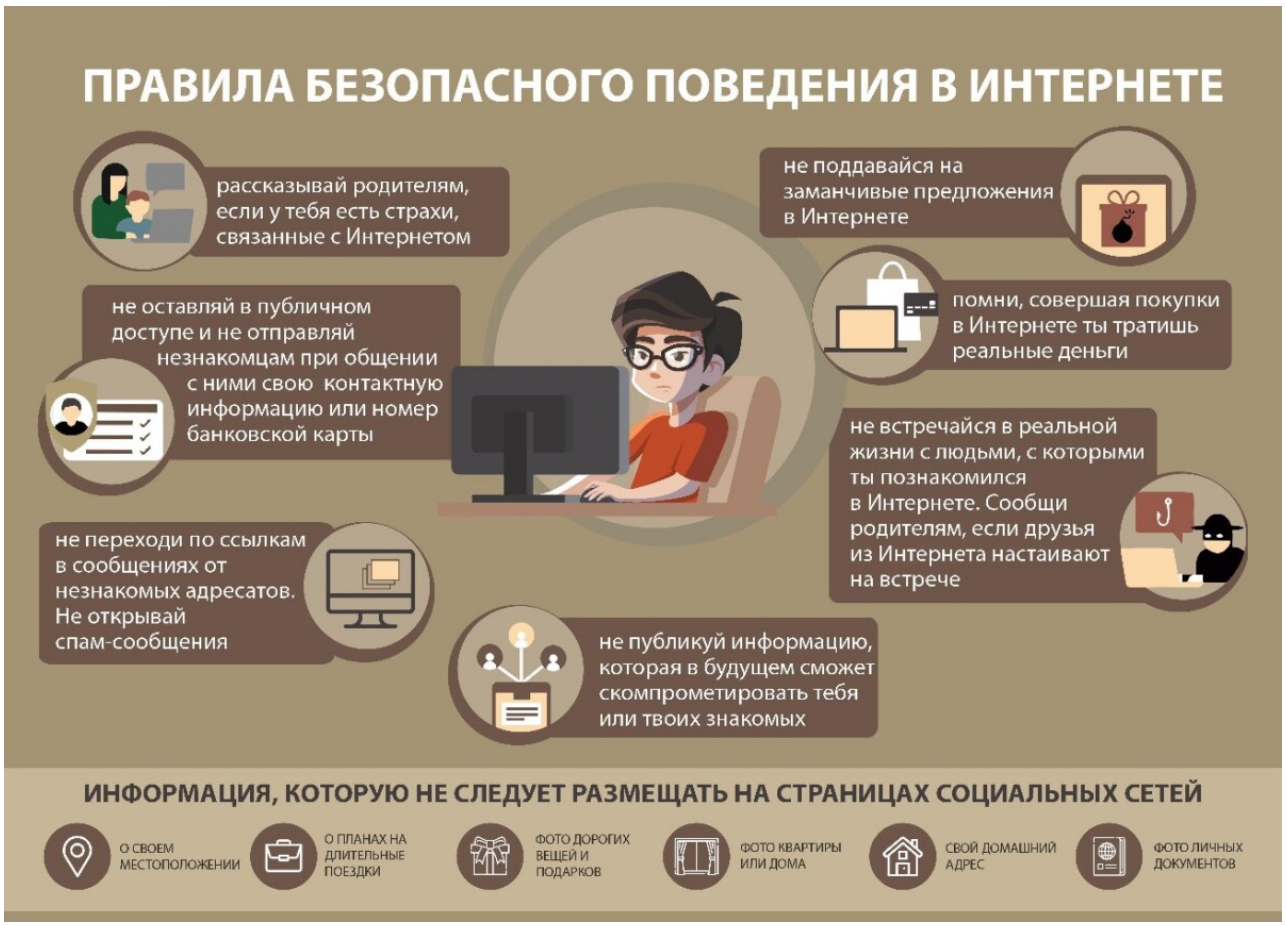
Варианты работы с этой информацией

**1. Обсуждение и дополнение основных 10 правил.**

Учащимся предлагается обсудить и дополнить эти основные правила с учетом уже имеющегося у них опыта работы в интернете.

**2. Рисуем инфографику**

Учащимся предлагается нарисовать плакат в стиле современной инфографики, где размещаются основные правила безопасной работы в сети Интернет.




В качестве примера для учащихся 8-9 классов предлагается занятие в формате семинара «Киберугрозы современности: главные правила их распознавания ипредотвращения»

**1. Обсуждение правил предотвращения киберугроз, которые встречаются при работе в Интернете**

У каждого ученика на столе лежит чистый лист бумаги – заготовка листовки по безопасности в Интернете. Перед тем, как начать работать учитель объясняет, что по ходу обсуждения каждый ученик должен заполнять листовку правилами, которые ему кажутся необходимыми и важными. После того, завершения обсуждения, отдельные ученики зачитывают свои листовки, остальные могут добавлять правила. Учитель начинает обсуждение с вопроса к аудитории: «Что вы знаете об угрозах, которые исходят из Интернета?» Просит учеников перечислить опасности,

которые могут угрожать человеку, его персональному компьютеру, мобильным устройствам. На доске фиксируются ответы учеников. Проводится обсуждение ответов.

Анализируя исследования, проводимые «Лаборатории Касперского» можно выделить 3 группы серьезных киберугроз:

1. Шпионское программное обеспечение и другие вредоносныепрограммы.
2. Спамы;
3. Фишинговые атаки.

Обсуждение основных правил защиты от главных киберугроз. Все ответы детей записываются на доске.

После обсуждения листовок на доске должен быть записаны основные правила защиты от киберугроз.

**2. Практикум «Угроза 419»**

Цель: формирование навыков распознавание спама в «нигерийских письмах».

Одной из разновидностей спама являются «Нигерийские письма» или другое название «Угроза 419». «Нигерийские письма» - вид мошенничества, получивший наибольшее развитие с появлением спама. Называется так потому, что письма особое распространение получили в Нигерии, причем еще до распространения Интернета они распространялись по обычной почте, начиная с середины 1980 годов. С появлением интернета «Нигерийские письма» стали нарицательным понятием.

Как правило, у получателя письма просят помощь в многомиллионных операциях, обещая солидные проценты с сумм. Если получатель согласится,у него выманиваются всё большие суммы денег на сборы, взятки и т. д. В худших вариантах жертве предлагается полулегально прибыть в Нигерию, где его либо арестовывали за незаконное прибытие в страну и у

него вымогаются деньги за освобождение, либо похищали с целью полученияявыкупа.

Мошенничество профессионально организовано: у мошенников есть офисы, работающий факс, часто мошенники связаны с правительственными организациями, и попытка получателя письма провести самостоятельное расследование не обнаруживает противоречий в легенде. Сделка подаётся как «безвредное» беловоротничковое преступление, что мешает жертве обратиться к властям. Разумеется, обещанных денег жертва в любом случае не получает: их просто не существует.

Спамеры оперативно реагируют на ситуацию в мире, отслеживая очаги нестабильности. Поэтому постоянно появляются новые разновидности

«Нигерийских» писем — например, «кенийские» или «филиппинские». Во время войны в Ираке активно шли спамерские рассылки «иракского» спама.

Подавляющее большинство «нигерийского» спама идет на английском языке, но в 2004-2005 гг. спамеры взялись активно осваивать Рунет. Появился «нигерийский» спам на русском языке, эксплуатирующий горячие события российской политической жизни.

«Нигерийские письма» являются дидактическим инструментом для формирования навыков распознавания спама и фишинговых атак.

Учитель делит аудиторию на 4 группы. Каждой группе выдает конверт,в котором содержится образец «нигерийского письма» и задание:

1. Внимательно прочитайте текст письма.
2. Выделите в нем моменты, указывающие на то, что это спам.
3. Перечислите факты, указанные в письме, которые кажутся вам недостоверными, подозрительными.

После того, как группы выполнят задание, начинается коллективное обсуждение. Вопросы для обсуждения:

1. Как можно распознать «нигерийское письмо»?

2. Как вы думаете кто авторы «нигерийских писем»?
3. Какую цель преследуют авторы «нигерийских писем»?
4. Можно ли считать безвредными «нигерийские письма»?

Результаты работы группы представляет один ученик. Все остальные ученики могут задавать вопросы и высказывать свое мнение. Учитель на доске записывает главные особенности «Нигерийских писем», которые нашли ученики, дополняет, систематизирует.

Подведение итогов занятия.

**Карточка 1**

*«Меня зовут Бакаре Тунде, я брат первого нигерийского астронавта, майора ВВС Нигерии Абака Тунде. Мой брат стал первым африканским астронавтом, который отправился с секретной миссией на советскую станцию «Салют-6» в далеком 1979 году. Позднее он принял участие в полете советского «Союза Т-163» к секретной советской космической станции «Салют-8Т». В 1990 году, когда СССР пал, он как раз находился на станции. Все русские члены команды сумели вернуться на землю, однако моему брату не хватило в корабле места. С тех пор и до сегодняшнего дняон вынужден находиться на орбите, и лишь редкие грузовые корабли*

*«Прогресс» снабжают его необходимым. Несмотря ни на что мой брат не теряет присутствия духа, однако жаждет вернуться домой, в родную Нигерию. За те долгие годы, что он провел в космосе, его постепенно накапливающаяся заработная плата составила 15 000 000 американских долларов. В настоящий момент данная сумма хранится в банке в Лагосе. Если нам удастся получить доступ к деньгам, мы сможем оплатить Роскосмосу требуемую сумму и организовать для моего брата рейс на Землю. Запрашиваемая Роскосмосом сумма равняется 3 000 000 американских долларов. Однако для получения суммы нам необходима ваша помощь, поскольку нам, нигерийским госслужащим, запрещены все операции с иностранными счетами. Вечно ваш, доктор Бакаре Тунде, ведущий*

*специалист по астронавтике».*

**Карточка 2**

*«Дорогой друг,*

*Я послан к вам по поводу моего покойного клиента, фамилия которого совпадает с вашим. Хотя мы еще не встречались друг с другом и раньше, но я верю, что судьба свела нас на ссылка на purpose.It будет лучше, мы утверждаем, и использовать деньги, чем позволить Ecobank топ-чиновников делиться и отвлекать его в своих соответствующих частных счетов, как заброшенный месторождения. Если закон не мог по конституции банка предоставить их должностными лицами право на наследование месторождения умершего клиента, вы и у меня больше прав, потому что умерший может быть ваш дальний родственник, так как он является гражданином вашей страны.*

*Прежде всего, я работал на него в течение многих лет, поэтому я верю, что он будет счастлив с нашим расположением, чтобы претендовать на фонд особенно когда противоположное состояние деньги незнакомым выступает в подобных старший staffs.You Ecobank, должны понимать, что в финансовых возможностей учреждения, подобные этой, общей, но не слышал. Люди вкладывают свои деньги в финансовые институты и некоторые из этих счетов являются либо закодированы или конфиденциально ссылка на operated.Normally, когда нечто подобное*

*происходит в финансовом учреждении, сообщается в управлении. Он не опубликованы и соответствующие финансовые учреждения только информирует адвокат своего клиента в зависимости от обстоятельств может быть и ждет реальный наследник, чтобы показать. По истечении указанного периода определяется банком получателя, чтобы придумать, руководство отправляет деньги своим «долгом Re-преобразования Департамента и закрытия счета.*

*Теперь вопрос в том, кто управляет «Долг Re-преобразования*

*Департамента", а кто управления? Ответ прост: они председателей, управляющих директоров и членов Правления. Эти люди разделили деньги, и никто не задает вопросы. На самом деле, такой вопрос даже не обсуждается вне заседаний совета директоров. Если мое расположение обращаюсь к вам, и я получить ваше согласие работать в качестве партнеров в передаче фонда, я буду начинать с необходимой правовой процесс, как покойный адвокат. В сущности, мне нужно будет быть предоставлена информация ниже, так что я могу начать с правовой процесс создания ближайших родственников с умершим;*

1. *Ваше полное имя*
2. *Возраст*
3. *Адрес*
4. *Частная Телефон*
5. *Профессия*
6. *Национальность*
7. *Другой адрес электронной почты ссылка на yahoo.com, ссылка hahotmail.com.*

*После этого, я должен подготовить и отправить Вам образцы письмо- заявку, которая будет представлена в банке, положив претендовать на его балансе US $ 10,500,000.00. Фонд может быть оплачен на банковский счет, вы будете назначать в установленном порядке или по видам чек кассира обращается в ваше имя и пользу.*

*Хотя трудно точно оценить время, которое потребуется, чтобы заключить этот вопрос, но я уверен, что весь процесс не займет до 10 рабочих дней с момента вы официально обратиться с банком transfer.I фонда " м предлагается 40% от общего фонда как вознаграждение за вашу помощь, моя будет составлять 50%, и мы будем дарить 9% (US $ 945 000) для благотворительной организации нашего выбора в то время как 1% (US $ 105,000 ) будет установлена в сторону, с учетом всех прочих расходов, которые могут возникнуть в процессе transfer.I фонда надеемся, что вы*

*оцените это предложение, как я взял многие вещи во внимание, прежде чем предлагать такое соотношение обмена.*

*Наконец, я хочу, чтобы вы знали, что я столкнулся с трудностями, пытаясь отправить это письмо к вам, как простой сообщении. Именно поэтому я прикрепил его. Поэтому мой скромный совет, который вы открываете новый адрес электронной почты либо в ссылка на hotmail.com, ссылка на yahoo.com и ссылка на Gmail.com содействовать нашей электронной*

*корреспонденции. Вы также можете связаться со мной через номер*

*+22890945333.*

*С наилучшими пожеланиями, Г-н Джонсон Slami Esq.»*

**Карточка 3**

*«Уважаемый Добрый день!*

*Я юрист, г-н Карл Алекс Хендерсон*

*Юрист в семье покойного президента Мусу Yaradua, мне было поручено семья в поисках хорошей инвестицией в вашей стране, предпочтительно недвижимость, я должен был обеспечивать конфиденциальность и доверие в этой сделке, так что вы находитесь в лучшем положении, знать больше, чем меня на этом инвестиции.*

*Деньги наличными $ 25,2 млн., Муса Yaradua семей хотят инвестировать эти деньги в вашу страну с вашей поддержкой, и мы обнаружили, что этот план, чтобы переместить его с помощью дипломатических средств. Пожалуйста, это очень конфиденциальная и совершенно секретной, я буду лететь вниз, чтобы посмотреть вам в лицо подписывать документы, необходимые для инвестиций, как только вы получите фонд.*

*Мы предлагаем 10% от общей суммы за вашу помощь в этом проекте, в то время как 5% будет использоваться для любых непредвиденных расходов, которые могут возникнуть при переводе средств.*

*Я с нетерпением ждем вашего ответа на это письмо.*

*Если вы примете мое предложение, я хотел бы иметь следующую информацию ниже, чтобы начать процесс.*

1. *Ваше полное имя:*
2. *Ваш номер телефона:*
3. *Ваш возраст:*
4. *Ваш пол:*
5. *Род занятий:*
6. *Вашей страны:*

*С уважением,*

*Адвокат г-н Карл Алекс Хендерсон Сотовые +2348020574082*

*факс +23417641464»*

**Карточка 4**

*«From: Prince Joe Eboh*

*Date: Wednesday, April 21, 2004 12:53 PMSubject: TRANSFER*

*Принц Джо Эбох*

*Уважаемый господин,/госпожа,*

*Надеюсь, что это послание найдет Вас в хорошем здравии. Я - Принц Джо Эбох, Председатель "Комитета заключения контрактов", "НигерийскойКомиссии Развития Дельты (NDDC)", являющейся филиалом нигерийской Национальной Нефтяной Корпорации (NNPC).*

*Нигерийская Комиссия Развития Дельты (NDDC) была создана*

*покойным Главой государства, генералом Сани Абача, который умер 18-ого июня 1998 года, для управления прибылью, образующейся от продаж нефти и ее субпродуктов.*

*Предполагаемый ежегодный доход на 1999 год составил свыше 45 миллиардов долларов США, сведения об этом содержаться в отчете Генерального аудитора Федеративной республики Нигерия ( FMF A26 ONE 3B Параграф "D") за ноябрь 1999 года.*

*Я - Председатель Комитета заключения контрактов, и мой комитет исключительно ответственен за то, как и куда должны распределяться денежные средства. Во всех случаях мы действуем от имени Федерального правительства Нигерии. Мой Комитет заключает контракты с иностранными подрядчиками для разработки нефтяных месторождений в районе дельты Нигера.*

*Так случилось, что в одном из контрактов нам удалось сэкономить US$25,000,000. Но, из-за существования некоторых внутренних законов, запрещающих государственным служащим в Нигерии открытие иностранных счетов, мы не имеем возможности перевести эти деньги за границу.*

*Однако, эти деньги US$25,000, 000 могут быть оформлены в форме оплаты иностранному подрядчику, поэтому мы хотели бы использовать ваш счет в банке как держателя бенефициария фонда. Мы также достигли соглашения, о том, что Вам будет предоставлена награда за содействие в этой операции в размере 20 % полной суммы, переданной как нашему иностранному партнеру, в то время как 5 % будут сохранены на непредвиденные расходы, которые обе стороны понесут в ходе реализации этой сделки, а остаток в 75 % будет сохранен для членов комитета.*

*Если Вы решите принять наши условия, Вы должны послать мне немедленнодетали вашего счета или открыть новый счет в банке, куда мы сможем осуществить перевод денег в сумме US$25,000, 000 , держателем которой вы будете, до тех пор, пока мы не прибудем в вашу страну за*

*нашей долей. Для нас не важно, каким бизнесом вы занимаетесь.*

*Все, что нам необходимо, это название вашей компании, ваш личный номер телефона / факса, полное имя, адрес и детали вашего счета в банке, на который будет осуществлен перевод через Apex Bank .*

*Отметьте, что эта сделка, как ожидается, должна будет реализована в пределах 21 рабочего дня со дня, когда мы предоставим все необходимые сведения Федеральному Министерству финансов, которое одобрит необходимое валютное распределение для перемещения этих средств на ваш счет. Пожалуйста, рассматривайте вышесказанное как конфиденциальные сведения.*

*Прошу Вас ответить мне как можно скорее.*

*Спасибо за ваше сотрудничество. Искренне ваш, Принц Джо Эбох»*

Занятие завершается ответом на вопрос «Как и для чего нужно знать основные правила безопасной работы в Интернете?».

## Старшая школа (10 - 11 классы)

**Цель:** создание условий для повышения уровня грамотности учащихся в вопросах информационной безопасности, расширение знаний учащихся о кибербезопасности и киберугрозах, формирование навыков их распознавания и оценки рисков, их минимизация

**Задачи:**

- ознакомить учащихся с нормативно-правовой базой;

- ознакомить обучающихся с адресами помощи в случае интернет-угрозы и интернет-насилия, номером всероссийского детского телефона доверия;

- выявить и обсудить основные правила обеспечения информационной безопасности в сети Интернет, научиться выявлять риски и минимизировать их;

- закрепить полученные знания путем выполнения творческого задания.

**Ожидаемые результаты:** повышение уровня осведомленности учащихся о проблемах информационной безопасности при использовании сети Интернет, умение оценивать потенциальные риски и минимизировать их.

В рамках урока «Информационная безопасность» в старших классах целесообразно познакомить обучающихся с международными стандартами в области информационной безопасности детей, которые отражены в российском законодательстве:

- Федеральный закон Российской Федерации № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (Закон определяет информационную безопасность детей как состояние защищѐнности, при котором отсутствует риск, связанный с причинением информацией (в том числе распространяемой в сети Интернет) вреда их

здоровью, физическому, психическому, духовному и нравственному развитию.);

- № 252-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию», (направленный на защиту детей от разрушительного, травмирующего их психику информационного воздействия, переизбытка жестокости и насилия в общедоступных источниках массовой информации, от информации, способной развить в ребѐнке порочные наклонности, сформировать у ребѐнкаискаженную картину мира и неправильные жизненные установки.)

Необходимо обратить внимание обучающихся на классификацию вредоносных информационных ресурсов:

- информация, причиняющая вред здоровью и (или) развитию детей;
- информация, запрещенная для распространения среди детей;
- информация, ограниченная для распространения среди детей определенных возрастных категорий.

На уроке необходимо затронуть следующие аспекты:

- перечень рисков, подстерегающих ребенка в сети Интернет;
- рекомендации по грамотному использованию электронной почты;
- технологии безопасного общения в средах мгновенного обмена сообщениями.

Необходимо обеспечить обучающихся:

- инструкциями по безопасному общению в чатах;
- советами по профилактике и преодолению Интернет-зависимости;
- общими правилами по безопасности детей в сети Интернет.

Также рекомендуется рассмотреть следующие объекты, являющиеся опасными в Интернете:

- нежелательные программы;
- защита личных данных;
- мошенничество;

- виртуальные «друзья»;
- пиратство;
- on-line-игры;
- этика;
- критический подход к информации.

Важно обеспечить обучающихся информацией о программном обеспечении, позволяющим осуществлять безопасную работу в сети Интернет, контентной фильтрации.

Важно ознакомить обучающихся с адресами помощи в случае интернет- угрозы и интернет-насилия, номером всероссийского детского телефона доверия(https://politech47.mskobr.ru/files/informaciya_o_liniyah_pomowi_v_sluchae_internet-ugroz.pdf).

Линия помощи в случаях Интернет-угроз «Горячая линия». На «Горячую линию» можно попасть круглосуточно, набрав адрес www.saferunet.ru и нажав на красную кнопку «Горячая линия».

Линия помощи «Дети онлайн». Линия помощи «Дети онлайн» – служба телефонного и онлайн консультирования для детей и взрослых по проблемам безопасного использования детьми и подростками Интернета и мобильной связи. Обратиться на «Линию помощи» можно:

- по телефону 8 800 250 00 15 (с 9 до 18 по рабочим дням, время московское)
- по электронной почте helpline@detionline.com •
- на сайте www.detionline.com

Возможные формы проведения урока в 9-11 классах – лекция, деловая игра, урок-презентация проектов, мозговой штурм «Интернет-безопасность», дискуссия, дебаты, встреча со специалистами медиа-сферы, системными администраторами и т.д.

Для учащихся старших классов средней школы будет актуальным

урок с использованием кейс-технологии.

**Кейс «Новый смартфон для отца»**

Илья Комаров, студент 4-го курса экономического факультета, вернулся домой после сдачи последнего экзамена зимней сессии. Экзамен был сдан на «отлично», и настроение у Ильи было соответствующим. Тем более что на телефон пришло сообщение от банка о начисление первой заработной платы от крупной энергетической компании, где он проходил стажировку.

Особенно его обрадовало начисление обещанной премии в размере 15000 рублей. Теперь у Ильи наконец-то появились деньги для покупки подарка ко дню рождения отца.

Выбирать подарок Илье не пришлось, недавно у его отца, Петра Петровича Комарова, сломался телефон. Вирусное приложение не только

«съело» все деньги со счета отца, но и безвозвратно повредило операционную систему старенького смартфона. Илья однозначно решил подарить отцу новый смартфон.

Он привычным движением открыл ноутбук и начал изучать предложения различных магазинов, сравнивая цены и параметры предлагаемых моделей.

Полчаса поисков в интернете привели Илью на сайт интернет-магазина, предлагающего современные устройства по низкой цене.

**Информация с сайта интернет-магазина:**

1. ***Интернет адрес:*** http://i-crop.ru/
2. ***Указанный адрес:*** г. Калининград.
3. ***Происхождение товара:*** таможенный конфискат.
4. ***Цены на товары:*** на 50% меньше рыночных.
5. ***Способ оплаты:*** кошелек QIWI.

6. ***Сроки доставки:*** от 1 -го до 20-ти дней.

7. ***Гарантии:*** Опись вложения содержимого бандероли.

***Характеристика роли в ситуации.*** Представьте себя на месте советника по личной информационной безопасности, к которому обратился Илья Комаров.

***Постановка задачи.*** Помогите Илье оценить безопасность покупки в данном интернет-магазине. Ответьте на поставленные вопросы:

1. Какая представленная информация вызывает доверие употенциального клиента?

2. Выделите незнакомые понятия, которые присутствуют в тексте, идайте им определение.

3. Какая информация на сайте не вызывает вашего доверия?

4. Каким образом можно проверить добросовестность интернет-магазина? Перечислите как можно больше способов.

5. Какой совет вы бы дали Илье Комарову?

За дополнительной информацией вы можете обратиться на сайт или в приложение к кейсу (см. ниже).

Приложение

**О магазине.** *Мы находимся в г. Калининград и успешно работаем с 2005 года! Аппараты были изъяты у различных фирм и предпринимателей при попытке контрабандного ввоза в Россию, без уплаты таможенной пошлины и соответствующих налогов. Как правило, предприниматели, желающие сэкономить на уплате налогов, пытаются провезти контейнеры со смартфонами и планшетами под видом радиодеталей или радиоэлектронного лома, на которые таможенная пошлина на ввоз существенно ниже, чем на мобильные телефоны и планшетные компьютеры. Наша цель - максимально быстро реализовать товар, поэтому мы устанавливаем столь доступные цены.*

*Вся продукция - оригинальная, от официальных производителей. Техника поставляется из США и Европы. Мы не продаем китайские подделки. На весь товар предоставляется гарантия 1 год. Гарантийное обслуживание обеспечивают официальные сервисные центры на территории РФ. Все телефоны русифицированы. Комплектация полная (заводская).*

*Мы всегда отправляем заказы своим клиентам посылкой с описью вложения содержимого. В этом случае сотрудники почты обязаны в Вашем присутствии вскрыть посылку до оплаты наложенного платежа, чтобы сверить содержимое посылки с описью. Таким образом, Вы сможете убедиться, что в посылке действительно находится мобильный телефон или планшетный компьютер надлежащего качества. Перед отправкой посылки заказчику, товар проверяется на отсутствие дефектов или брака. Данные условия гарантируют отсутствие в изделии дефектов и удовлетворяют законным требованиям Потребителя в течении гарантийного срока с момента передачи товара потребителю».*

**Доставка и оплата.** *Доставка осуществляется Почтой России или курьером службы экспресс-доставки DHL по всей территории РФ и СНГ. Самовывоза нет. Оплата только через QIWI кошелек (VISA QIWI Wallet).*

*СПОСОБЫ ДОСТАВКИ:*

*1. Доставка курьером экспресс-почты DHL: 1-3 дня (только при условии полной предоплаты заказа).*

*2. Доставка бандеролью наложенным платежом: 7-20 дней (требуется оплата гарантийного взноса 500 рублей*).*

**Гарантийный взнос - это обязательное и неоспоримое условие, которое гарантирует серьезность Вашего намерения приобрести товар. Сумма гарантийного взноса не зависит от модели телефона или планшетного компьютера и составляет 500 рублей за каждую единицу товара. Доставка по России и СНГ - бесплатно. Экспресс-доставка*

*курьером DHL также осуществляется бесплатно, но только после полной предоплаты заказа.*

*ОПЛАТА ЧЕРЕЗ QIWI КОШЕЛЕК:*

*1. Зарегистрируйтесь на сайте QIWI кошелька "VISA QIWI Wallet" (используйте тот же номер телефона, который укажете в заказе).*

*2. Пополните счет QIWI кошелька на сумму равную стоимости заказаили гарантийный взнос 500 рублей (см. способы пополнения).*

*3. На сайте WWW.QIWI.COM войдите в свой кошелек и выберите ПЕРЕВЕСТИ -> ПО E-MAIL.*

*4. В форме перевода укажите сумму, равную стоимости заказа илигарантийный взнос 500 рублей и e-mail platezh@i-crop.ru. Оплатите.*

*5. Сообщите на наш e-mail (info@i-crop.ru) номер заказа, номер Вашего телефона, сумму платежа, дату и время перевода.*

*6. Заказ будет отправлен на следующий день. Мы сообщим Вам трек-номер для отслеживания посылки.*

*Пополнить QIWI кошелек можно через QIWI терминалы, банковской картой, со счета мобильного телефона и многими другими способами.*

*Если Вы выбрали способ "доставка наложенным платежом", то при получении посылки Вас попросят оплатить наложенный платеж в кассе почтового отделения.*

*Для чего требуется гарантийный взнос: это вынужденная мера с нашей стороны, поскольку у нас часто бывают случаи, когда заказчик, по независящим от нас причинам, не является на почту и не выкупает посылкус заказом, в результате чего нам приходится платить за пересылку посылкив оба конца + почтовый сбор за хранение посылки на почте сверх установленного срока. В связи с этим, чтобы избежать лишних финансовых потерь, мы просим Вас оплатить гарантийный взнос. Схема здесь действует следующая: если Вы не являетесь на почту и не выкупаете посылку, то сумма гарантийного взноса покрывает наши расходы, затраченные на пересылку товара в оба конца. Никакого перерасхода с*

*Вашей стороны не будет, так как при отправке заказа сумма гарантийного взноса вычитается из его стоимости. Просим Вас с пониманием отнестись к данным условиям.*

**Материалы для педагога по обсуждению кейса**

**Какая информация призвана вызвать доверие у клиента:Срок существования магазина**

Указанная информация призвана вызывать доверие к магазину у покупателей. Однако написать на сайте все что угодно. Поэтому подобной информации не следует доверять.

**Что такое Русификация?**

Русификация в информатике - приспособление аппаратного и программного обеспечения к работе с русским языком; переход на использование русского языка в интерфейсе компьютеров и компьютеризованной бытовой техники.

Самое интересное что одним из признаков контрабандного товара (которым якобы торгуют владельцы магазина) является отсутствие русификации. А если заводская(лицензионная) русификация на оборудовании все таки произведена значит оборудование уже на заводе планировалось поставлять в Россию. Тогда как он мог стать контрабандным?

**Не знакомые понятия:**

**Что такое QIWI КОШЕЛЕК?**

Электронная платежная система QIWI кошелек создана в 2006 году. С помощью QIWI кошелька можно не только оплачивать услуги связи, но и покупки в интернет магазинах. Сам по себе QIWI кошелек безопасен. Вызывает подозрение то, что интернет магазин работает ТОЛЬКО С QIWI КОШЕЛЬКОМ!!!

**Что такое ТАМОЖЕННЫЙ КОНФИСКАТ?**

Понятно, что это импортный товар, который прошел через таможню. Но вот словом "конфискат" обычно в русском языке означают что-то

конфискованное. По закону, всё конфискованное на таможне храниться до решения суда. А после вынесения решения суда конфискованный (без слова таможенный) товар либо продают (безопасный товар) либо сжигают (небезопасный товар).

**Что такое Наложеный платеж?**

Наложенный платёж — денежная сумма, которую почта взыскивает по поручению отправителя с адресата при вручении последнему почтового отправления, и которая пересылается отправителю (или указанному им лицу)почтовым или телеграфным переводом.

Т.е. вы оплачиваете свою покупку на почте, когда забираете товар. А почтовые работники отправляют полученные средства продавцу. Наложный платеж является одним из самых безопасных способов оплаты интернет-покупки. Особенно если производится Опись содержимого посылки.

**Трек-номер (Почтовый идентификатор)**

При помощи почтового идентификатора, возможно, узнать о местонахождении и состоянии почтового отправления. Добросовестные продавцы действительно отправляют своим клиентам Трек-номера, которые позволяют следить за доставкой. Мошенники всегда стараются вызвать доверие мнимой прозрачностью своей деятельности.

**Что такое ОПИСЬ ВЛОЖЕНИЯ БАНДЕРОЛИ?**

**Опись вложения** – это бланк утвержденной формы, который заполняет отправитель. В бланке перечисляются все вложения, каждому вложению присваивается оценочная стоимость. Опись вложения защищает от воровства на ПОЧТЕ. А значит гарантией честности магазина быть не может.

**Информация, не вызывающая доверия:**

**Отсутствие полного юридического адреса**

Мошенники всегда стараются скрыть свою личность. Если на сайте нет указания юридического адреса продавца. То скорее всего владельцы сайта мошенники. И в том случае если ваша покупка не будет вам

доставлена вы даже не сможете написать заявление в правоохранительные органы.

**Гарантийный платеж**

Тревожный признак. Согласитесь, странно получается, с одной стороны продавец уверяет что товар вам понравиться, и он надлежащего качества, с другой он боится, что вы откажетесь от доставленного товара. Эти 500 рублей мошенники оставят себе, и конечно же никакого товара вы неполучите.

**Полная предоплата как обязательное условие**

Тревожный признак. Полная предоплата, тем более проведенная переводом с QIWI кошелька, фактически означает что вы просто подарили мошенникам деньги. Достойные доверия интернет-магазины не работают по такой схеме.

**Отсутствие самовывоза**

Тревожный признак. Скорее всего, у мошенников нет даже офиса. Работают и отвечают клиентам из интернет-кафе или с домашнего компьютера.

**Перевод через QIWI кошелек по электронному адресу**

Тревожный признак. E-mail нельзя отследить, и соответственно очень сложно установить личность продавца.

**Для проверки добросовестности магазина можно предпринять следующие действия:**

1. Проверить отзывы о магазине на форумах. Если отзывы отрицательные воздержитесь от покупки.

2. Проверить входит ли магазин в черный список, воспользовавшись соответствующим сайтом. Если магазин входит в черный список -воздержитесь от покупки.

3. Проверить срок регистрации сайта. Если срок регистрации домена очень мал и не соответствует заявленному сроку существования интернет-магазина. Воздержитесь от покупки.

4. Проанализируйте всю открытую информацию. Найдите все незнакомые понятия и узнайте, что они значат.

**Совет Илье Комарову:**

Воздержаться от покупки. Приобрести телефон в надежном интернет -магазине.

# Альтернативные практикумы

Приведенные выше практические занятия вы можете заменить на альтернативные. Подходящая для практического занятия возрастная категория учащихся определяется педагогом самостоятельно

## 1. Виды атак с использованием социальной инженерии

Тему рекомендуется рассмотреть с учащимися разных возрастных групп. Для учащихся начальной школы - в подходящем формате, например, в формате беседы. Учащиеся среднего и старшего звена могут не только ознакомиться с теорией, но и выполнить практическую работу.

Перед выполнением практической части стоит ознакомить учащихся с понятием «социальная инженерия».

В контексте информационной безопасности социальная инженерия – это психологическое манипулирование людьми с целью совершения определенных действий или разглашения конфиденциальной информации. Следует отличать от понятия социальной инженерии в социальных науках - которое не касается разглашения конфиденциальной информации. Совокупность уловок с целью сбора информации, подделки или несанкционированного доступа от традиционного «мошенничества» отличается тем, что часто является одним из многих шагов в более сложной схеме мошенничества.

Существует несколько видов атак с использованием социальной инженерии (https://www.kaspersky.ru/resource-center/threats/how-to-avoid-social-engineering-attacks):

- Ловля «на живца»
- Претекстинг
- Фишинг
- Вишинг и смишинг

- «Ты – мне, я – тебе»

- Взлом электронной почты и рассылка по контактам

- «Охота» и фарминг

Учащиеся делятся на 7 команд. Каждая команда закрепляет за собой один вид атаки.

Задание. Каждой команде необходимо сделать видеоролик (около минуты или менее) с помощью сервиса Visper (https://visper.tech/). Visper – это платформа визуальных персонажей для создания видеоконтента, в основе ее работы содержится искусственный интеллект. Каждый ролик должен содержать: краткое описание вида атаки, несколько примеров. Каждая команда презентует свой ролик.

Занятие заканчивается демонстрацией роликов командами и ответами на вопросы учащихся других команд.

## 2. Компьютерные вирусы и вредоносное программное обеспечение (ПО)

Практическая работа выполняется с использованием инструментов совместной деятельности (например, с использованием Яндекс.Документы). Перед проведением занятия педагогу необходимо подготовить шаблон презентации для дальнейшего совместного редактирования и настроить права доступа.

Перед непосредственным переходом к практической части работы с учащимися рекомендуется обсудить следующие общие вопросы:

- что такое компьютерные вирусы и вредоносное ПО?

- как компьютер может быть заражен?

- что нужно делать, чтобы минимизировать риски заражения?

Далее учащиеся разбиваются на 8 команд, каждая команда закрепляет за собой отдельный вид вредоносного ПО.

Виды вредоносного программного обеспечения:

1. Вирусы

2. Черви
3. Рекламное ПО
4. Шпионское ПО
5. Программы-вымогатели
6. Боты
7. Руткиты
8. Троянские программы

Каждая команда заполняет шаблон презентации по своему разделу, готовится к демонстрации своего раздела. Каждая команда должна осветить следующие аспекты своего направления: краткое описание, возможные пути заражения компьютера, пути минимизации рисков, личный опыт.

Занятие заканчивается демонстрацией общей презентации и защитой разделов соответствующих команд. После демонстрации каждого раздела остальные участники могут задавать друг другу вопросы, касательно темы, высказывать свой личный опыт.

### 3. Фишинговые письма

Фишинг - вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей - логинам и паролям. Это достигается путём проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени банков или внутри социальных сетей. В письме часто содержится прямая ссылка на сайт, внешне неотличимый от настоящего, либо на сайт с редиректом (перенаправлением).

Учитель делит аудиторию на 8 групп. Каждой группе достается карточка, содержащая текст фишингового письма (подчеркивание означает гиперссылку). Задание для всех команд одинаковое:

1. Внимательно прочитайте текст письма.
2. Выделите в нем моменты, указывающие на то, что это спам.
3. Что необходимо сделать если подобное письмо пришло вам на

почту?

После того, как группы выполнят задание, начинается коллективное обсуждение. Вопросы для обсуждения:

5. Как можно распознать «фишинговое письмо»?
6. Как вы думаете кто авторы «фишинговых писем»?
7. Какую цель преследуют авторы «фишинговых писем»?
8. Можно ли считать безвредными «фишинговые письма»?

Результаты работы группы представляет один ученик. Все остальные ученики могут задавать вопросы и высказывать свое мнение, в том числе делиться личным опытом. Учитель на доске записывает главные особенности «Фишинговых писем», которые нашли ученики, дополняет, систематизирует.

**Карточка 1**

Уважаемый пользователь!

Предупреждение! У Вас 5 новых отложенных писем. Ваша почта версии 2.0.1 в настоящее время отключена от получения входящей почты и больше не будет работать с 23 ноября 2022 года. Для получения сообщений и обновления до версии 3.0.1, пожалуйста, следуйте информации об обновлении ниже.

Обновление до версии 3.0.1 сейчас

**Карточка 2**

Уважаемый пользователь!

Использование квоты вашего почтового ящика превысило 85%. Возможно, вы не сможете получать новые электронные письма. Пожалуйста, мы советуем вам увеличить хранилище почтовой службы или удалить электронную почту, чтобы избежать этого.

Увеличить почтовый ящик

Спасибо,

Почтовый сервис, 2022

**Карточка 3**

Уважаемый пользователь!

В течение 24 часов ваш аккаунт будет удален за рассылку спама. Опровергнуть жалобу вы можете, перейдя по ссылке и заполнив форму авторизации.

Опровергнуть жалобу

С уважением,

Сервис почты

**Карточка 4**

К сожалению, Вам выписан новый штраф.

Посмотреть детали штрафа и номер постановления вы можете, перейдя в раздел Штрафы ГИБДД

Оплатите со скидкой 50% в первые 20 дней!

**Карточка 5**

Сбербанк России

Уважаемый клиент!

Кредитный отдел Сбербанка России уведомляет Вас о том, что на ваше имя был оформлен потребительский кредит через наш онлаин банкинг (https^/online.sberbank.ru) на сумму 680 000 рублей.

На данный момент задолжность не погашена. На 11.11.2022 ваш долг составляет 633 773 рубля с учетом пени (0.7 в сутки).

В связи с этим, на ваше имя Сбербанком России был составлен судебный иск.

Ознакомьтесь с документами:

Договор займа.rar

Судебный иск.rar

С уважение,

Банк России

**Карточка 6**

Добрый день!

Как вы и просили, выложила зарплатную ведомость за ноябрь с коррекциями + премии по ссылке

С уважением,

Ольга Викторовна,

Начальник отдела по работе с персоналом

**Карточка 7**

Коллеги, добрый день!

Мы переработали концепцию проекта «Х». Посмотрите наши предложения и дайте свое заключение.

До конца недели предложения нужно будет скорректировать (при необходимости) и утвердить.

**Карточки 8**

Коллеги, добрый день.

В связи с продлением ограничений было принято решение провести тестирование сотрудников на коронавирус на дому.

Составляется график проведения тестирования по каждому подразделению.

Просьба сегодня выбрать даты для проведения сотрудникам теста на нашем портале

Из приведенной таблицы выберите свободные ячейки.

**Электронные ресурсы по теме «Информационная безопасность»**

1. https://infobez.zabedu.ru/ - портал «Информационная безопасность» - сайт ГУ ДПО «ИРО Забайкальского края». Содержит информацию для образовательных организаций, родителей и детей, в том числе материалы для проведения уроков по информационной безопасности. Содержит много полезной и актуальной информации
2. https://rocit.ru/ - сайт об информационной безопасности, функционирует при поддержке Министерства цифрового развития, связи и массовых коммуникаций РФ. Содержит много полезной и актуальной информации
3. http://www.fid.su/ - Фонд развития Интернет. Информация о проектах, конкурсах, конференциях и др. по компьютерной безопасности и безопасности Интернета
4. http://www.nachalka.com/bezopasnost - Nachalka.com предназначен для учителей, родителей, детей, имеющих отношение к начальной школе. Статья «Безопасность детей в Интернете». Советы учителям и родителям
5. http://habrahabr.ru/company/mailru/blog/252091/ - Советы по безопасности
6. https://politech47.mskobr.ru/files/informaciya_o_liniyah_pomowi_v_sluchae_internet-ugroz.pdf - Информация о линиях помощи в случаях Интернет – угроз
7. https://www.kaspersky.ru/resource-center/threats/computer-viruses-and-malware-facts-and-faqs - Статья от Kaspersky «Компьютерные вирусы и вредоносное ПО: факты и часто задаваемые вопросы»
8. https://www.kaspersky.ru/resource-center/threats/how-to-avoid-social-engineering-attacks - Статья от Kaspersky «Как избежать атаки с использованием социальной инженерии»
9. https://www.kaspersky.ru/blog/email-account-stealing/23433/- Статья от Kaspersky «Как взламывают почту с помощью фишинга»

10. https://digitalsharks.ru/blog/ulovki-hakerov-17-primerov-fishinga/ - Статья «Уловки хакеров. 17 примеров фишинга»

11. https://nsportal.ru/shkola/klassnoe-rukovodstvo/library/2020/10/11/pamyatka-dlya-obuchayushchihsya-ob-informatsionnoy - Образовательная социальная сеть nsportal.ru, содержит в свободном доступе Памятку для обучающихся об информационной безопасности детей

12. https://www.sites.google.com/site/saitkonferencii/sekcia-2/formirovanie-informacionnoj-bezopasnosti-v-skole - Сайт «Аспекты информатизации образования: информационная безопасность (опыт, проблемы, перспективы) содержит множество докладов, в том числе «Формирование информационной безопасности в школе»