Занятие: **«Киберугрозы современности: главные правила их распознавания и предотвращения»**

Форма занятия: семинар
Цель: расширение знаний о киберугрозах, формирование навыков их распознавания и оценки рисков.
Возраст обучающихся: 15-16 лет
План занятия:
1. Обсуждение правил предотвращения киберугроз, которые встречаются при работе в Интернете. Составление листовок «Правила защиты от киберугроз» (20 мин.)

2. Практикум «Опасность 419» (20 мин.)

3. Подведение итогов занятия. (5 мин.)

Ход занятия.
Занятие начинается показом социального видеоролика «Безопасный интернет - детям!»[2] После просмотра ролика учитель объявляет тему занятия и предлагает обучающимся самим сформулировать цель занятия.
Доклад «Киберугрозы и информационная безопасность», сайт http://www.kaspersky.ru/downloads/pdf/kaspersky_global_it_security_risks_survey.pdf)[3]
Обсуждение правил предотвращения киберугроз, которые встречаются при работе в Интернете. Продолжительность 20 минут.

У каждого обучающегося на столе лежит чистый лист бумаги – заготовка листовки по безопасности в Интернете. Перед тем, как начать работать учитель объясняет, что по ходу обсуждения каждый обучающийся должен заполнять листовку правилами, которые ему кажутся необходимыми и важными. После того, завершения обсуждения, отдельные обучающиеся зачитывают свои листовки, остальные могут добавлять правила. Листовки собираются после урока для того, чтобы их раздать обучающимся других групп.
Учитель начинает обсуждение с вопроса к аудитории: «Что вы знаете об угрозах, которые исходят из Интернета?» Просит обучающихся перечислить опасности, которые могут угрожать человеку, его персональному компьютеру, мобильным устройствам. На доске фиксируются ответы
После короткого обсуждения учитель приводит данные «Лаборатории Касперского» За последний год 91% компаний, представители которых приняли участие в опросе, сталкивались с угрозами информационной безопасности. В России этот показатель еще выше – 96%. Более того, ситуация становится только хуже: почти половина участников исследования

2 http://www.youtube.com/watch?v=9uvNVZMdeIk&feature=player_embedded 3 Доклад «Киберугрозы и информационная безопасность», сайт http://www.kaspersky.ru/downloads/pdf/kaspersky_global_it_security_risks_survey.pdf) 4 Дрозд А. Основные методы сетевых мошенников (ликбез). Материал с сайта http://www.securitylab.ru/blog/company/securityinform/90304.php

утверждает, что количество кибератак за этот период увеличилось. Перечисляя киберугрозы, которые представляются им самыми значительными, большинство участников исследования во всем мире ставят на первое место вирусы, шпионское ПО и другие вредоносные программы (61%). Спам назвали источником угрозы 56% респондентов. Третье место (36%) заняли фишинговые атаки, за ними идут сбои, вызванные проникновением в корпоративную сеть (24%), и DDoS-атаки (19%)[3].
Таким образом, можно выделить 3 группы серьезных киберугроз:
1. Шпионское ПО и др. вредоносные программы,

2. Спамы,

3. Фишинговые атаки.

Обсуждение основных правил защиты от главных киберугроз. Все ответы детей записываются на доске.
При обсуждении внимание учеников обращается на то, откуда могут исходить опасность. На первом месте в этом списке стоят социальные сети. Хотя в последнее время стал распространенными атаки на компьютер через мобильные устройства памяти (флешки).
«Сегодня большинство вредоносных программ создаются либо для того, чтобы рассылать спам, либо для того, чтобы красть у пользователя важные данные.
Если данные действительно важные и дорогостоящие, то для их похищения злоумышленники специально разрабатывают троян, который гарантированно будет работать на компьютерах в той организации, откуда нужно украсть данные. Осуществить внедрение такого вредоносного ПО обычно гораздо проще не через интернет, а с помощью записанных на флэшках «троянов». Флэшки могут подбрасываться как в здание, где располагается организация, так и размещаться, скажем, на парковке рядом с ним, где их с большой долей вероятности наверняка найдёт именно сотрудник нужной организации. Поэтому если вы нашли на улице или в здании флэшку, не торопитесь радостно вставлять её в свой компьютер – лучше сначала отдайте системному администратору, который просканирует её и при необходимости обезвредит.
Бывают и более банальные, но не менее эффективные способы заразить компьютер недостаточно осторожного пользователя. Например, от знакомого по Skype Вам может прийти сообщение в духе «Посмотри, на этой фотографии он так похож на нашего друга (одноклассника)!», ну и, конечно, ссылка на саму эту фотографию. При переходе по ссылке фотография почему-то не открывается в браузере, а сохраняется на жесткий диск, но мало кто на это обращает внимание. Хотя они-то как раз и должны насторожить! В общем, когда «фото» не открывается,

2 http://www.youtube.com/watch?v=9uvNVZMdeIk&feature=player_embedded 3 Доклад «Киберугрозы и информационная безопасность», сайт http://www.kaspersky.ru/downloads/pdf/kaspersky_global_it_security_risks_survey.pdf) 4 Дрозд А. Основные методы сетевых мошенников (ликбез). Материал с сайта http://www.securitylab.ru/blog/company/securityinform/90304.php

пользователь «входит» в папку с ним, и видит, что это не просто abcd.jpg, а abcd.jpg.scr, то есть, исполняемый файл, а его компьютер уже заражен вирусом».[4]

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

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 получения выкупа.

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» (Приложение) и задание:

1. Внимательно прочитайте текст письма.

2 http://www.youtube.com/watch?v=9uvNVZMdeIk&feature=player_embedded 3 Доклад «Киберугрозы и информационная безопасность», сайт http://www.kaspersky.ru/downloads/pdf/kaspersky_global_it_security_risks_survey.pdf) 4 Дрозд А. Основные методы сетевых мошенников (ликбез). Материал с сайта http://www.securitylab.ru/blog/company/securityinform/90304.php

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.

Приложение.

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 дня он 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

2 http://www.youtube.com/watch?v=9uvNVZMdeIk&feature=player_embedded 3 Доклад «Киберугрозы и информационная безопасность», сайт http://www.kaspersky.ru/downloads/pdf/kaspersky_global_it_security_risks_survey.pdf) 4 Дрозд А. Основные методы сетевых мошенников (ликбез). Материал с сайта http://www.securitylab.ru/blog/company/securityinform/90304.php

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 на hotmail.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

2 http://www.youtube.com/watch?v=9uvNVZMdeIk&feature=player_embedded 3 Доклад «Киберугрозы и информационная безопасность», сайт http://www.kaspersky.ru/downloads/pdf/kaspersky_global_it_security_risks_survey.pdf) 4 Дрозд А. Основные методы сетевых мошенников (ликбез). Материал с сайта http://www.securitylab.ru/blog/company/securityinform/90304.php

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 PM
Subject: TRANSFER
Принц Джо Эбох
Уважаемый господин,/госпожа,
Надеюсь, что это послание найдет Вас в хорошем здравии. Я - Принц Джо Эбох, Председатель "Комитета заключения контрактов", "Нигерийской Комиссии 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.

2 http://www.youtube.com/watch?v=9uvNVZMdeIk&feature=player_embedded 3 Доклад «Киберугрозы и информационная безопасность», сайт http://www.kaspersky.ru/downloads/pdf/kaspersky_global_it_security_risks_survey.pdf) 4 Дрозд А. Основные методы сетевых мошенников (ликбез). Материал с сайта http://www.securitylab.ru/blog/company/securityinform/90304.php

Если Вы решите принять наши условия, Вы должны послать мне немедленно детали 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»

Подведение итогов занятия.

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

Для подготовки и проведения занятий по безопасной работе детей в Интернете рекомендуется использовать материалы журнала для педагогов, психологов и родителей «Дети в информационном обществе», который издается Фондом Развития Интернет (http://detionline.com).

2 http://www.youtube.com/watch?v=9uvNVZMdeIk&feature=player_embedded 3 Доклад «Киберугрозы и информационная безопасность», сайт http://www.kaspersky.ru/downloads/pdf/kaspersky_global_it_security_risks_survey.pdf) 4 Дрозд А. Основные методы сетевых мошенников (ликбез). Материал с сайта http://www.securitylab.ru/blog/company/securityinform/90304.php