Государственное бюджетное профессиональное образовательное учреждение Московской области
«Раменский дорожно-строительный техникум»

Методическая разработка внеаудиторного мероприятия для проведения конференции по теме:

«Безопасность в сети интернет»

Учебная дисциплина «Информатика»
1, 2 курс

Составили: преподаватель Чупракова С. Н.

Преподаватель Кумов Я.С.

2022

Пояснительная записка

Данная методическая разработка предназначена для проведения конференции на тему: «Безопасность в сети интернет»

Цель данной методической разработки: обеспечение проведения конференции по вопросам формирования информационно-коммуникационной культуры.

Задачи конференции:

1) информирование обучающихся о видах информации, способной причинить вред здоровью и развитию, запрещенной или ограниченной для распространения на территории Российской Федерации, а также о негативных последствиях распространения такой информации;

2) информирование обучающихся о способах незаконного распространения такой информации в информационно–телекоммуникационных сетях, в частности в сетях Интернет и мобильной сотовой связи, в том числе путем рассылки SMS-сообщений незаконного содержания;

3) ознакомление обучающихся с международными принципами и нормами, с нормативными правовыми актами Российской Федерации, регулирующими вопросы информационной безопасности несовершеннолетних;

4) обучение студентов правилам ответственного и безопасного пользования услугами Интернет и мобильной сотовой связи, другими электронными средствами связи и коммуникации, в том числе способам защиты от противоправных и иных общественно опасных посягательств в информационно–телекоммуникационных сетях, в частности от таких способов разрушительного воздействия на психику детей, как кибербуллинг (жестокое обращение с детьми в виртуальной среде) и буллицид (доведение до самоубийства путем психологического насилия);

5) предупреждение совершения обучающимися правонарушений с использованием информационно–телекоммуникационных технологий.

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

В рамках конференции 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» (в том числе распространяемой в сети Интернет); № 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 ребенке порочные наклонности, сформировать у ребенка искаженную картину мира и неправильные жизненные установки).

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.

Тема конференции «Безопасность в сети интернет»

Цель конференции: формирование информационно-коммуникационной культуры и грамотности у обучающихся как фактора безопасности в информационном обществе.

Задачи:

Образовательные:

- расширить знания обучающихся об информационной безопасности.
- сформировать у обучающихся адекватное отношение к понятиям реального и виртуального мира.
- сформировать правила работы, которые способствуют положительному влиянию использования компьютера и интернета в жизни человека и снижают негативное влияние.

Развивающие:

- развивать познавательную активность студентов;
- развивать способность приспосабливаться к различным условиям деятельности и к разным деловым партнерам;
- развивать навыки поиска, сбора и обработки информации в сети Интернет.

Воспитательные:

- **в**оспитывать у обучающихся умения: выслушивать точку зрения другого, участвовать в диалоге;
- воспитывать взаимоуважение;
- формировать интерес к работе товарища.

Целевая аудитория: студенты 1, 2 курса.

Материально - техническое обеспечение: компьютер, мультимедийный проектор, презентации студентов.

Время проведения: 90 минут.

Место проведения: кабинет информатики.

Методы и формы обучения: словесный (дискуссия, рассказ); видеометод; наглядный (демонстрация); проблемный метод мотивации интереса; интерактивная форма обучения (обмен мнениями, информацией).

План конференции:

1. Организационный момент (вводное слово преподавателя) -5 минут.
2. Выступления студентов с презентациями - 45 минут.
3. Викторина «Кибербезопасность» (рефлексия)– 35 минут
4. Подведение итогов конференции - 5 мин.

Ход конференции

1. Организационный момент

Вводное слово преподавателя

Сегодня количество пользователей сети Интернет постоянно увеличивается, причем доля молодежи и совсем юной аудитории пользователей очень велика. К большому удивлению многих пользователей сети существуют Законы Интернета, так как Интернет является публичным местом.

В сети много полезного, а также и много угроз, ложной информации и мошенничества.

Давайте посмотрим, какие угрозы могут быть в сети интернет и как обезопасить себя от них.

2. Выступления студентов с презентациями (фрагменты презентации в Приложении №3).

3. Викторина «Кибербезопасность» (фрагмент викторины представлен в Приложении №2).

Группа делится на 4 команды, каждая команда поочередно отвечает на вопросы. У каждой команды по 5 вопросов различной сложности, вопрос на 200 баллов, на 400, 600, 800 и 1000. Максимально каждая команда может набрать 3000 баллов.

4. Подведение итогов конференции

Подсчет баллов и объявление победителей (Приложение № 4 – Оценочный лист).

Заключительное слово преподавателя

Интернет – это первая в истории цивилизации среда общения, порядок в которой поддерживается самими пользователями. Для этого ими выработаны определенные правила поведения в сети – виртуальный этикет, которые в значительной мере определяются практикой (правила интернет-безопасности и интернет-этикета представлены в Приложении №1).

Вывод

В ходе проведения конференции студенты должны научиться делать более безопасным и полезным свое время пребывания в сети Интернет, а именно:

- критически относиться к сообщениям и иной информации распространяемой в сетях Интернет, мобильной (сотовой) связи, посредством иных электронных средств массовой коммуникации;

- отличать достоверные сведения от недостоверных, вредную для них информацию от безопасной;

- избегать навязывания им информации способной причинить вред их здоровью, нравственному и психическому развитию, чести, достоинству и репутации;

- распознавать признаки злоупотребления их неопытностью и доверчивостью попытки вовлечения их в противоправную и иную антиобщественную деятельность;

- распознавать манипулятивные техники используемые при подаче рекламной и иной информации;

- критически относиться к информационной продукции, распространяемой в информационно–телекоммуникационных сетях;

- анализировать степень достоверности информации и подлинность ее источников;

- применять эффективные меры самозащиты от нежелательных для них информации и контактов в сетях.

Список литературы и интернет-ресурсы:

1. П. Н. Дерянин, О. О. Михальский, Д. И. Правиков, А. Ю. Щербаков. Теоретические основы компьютерной безопасности. – М.: Радио и связь, 2000.
2. А. Г. Асмолов, А. Л. Семенов, А .Ю. Уваров. Российская школа и новые информационные технологии: взгляд в будущее десятилетие.- М.:, 2010.
3. Г. У. Солдатов, М. И. Лебешева. Опасное любопытство. Кто и как попадает на сайты, несущие угрозу для здоровья школьников?//Журнал «Дети в информационном обществе» - М., 2011, №8 – СС.46-55.
4. Сайт Компьютерная безопасность. Безопасность жизни (http://blog.chljahsoft.net/3167);
5. Сайт Безопасный Интернет для детей: законодательство, советы, мнения, международный опыт (http://i-deti.org/);
6. Буклет Безопасный интернет детям Министерства внутренних дел РФ (http://www.mvd.ru/userfiles/liflets_k_deti_06.pdf);
7. Материалы III ежегодного Форума Безопасного Интернета (http://safor.ru/prezentacii11.php);

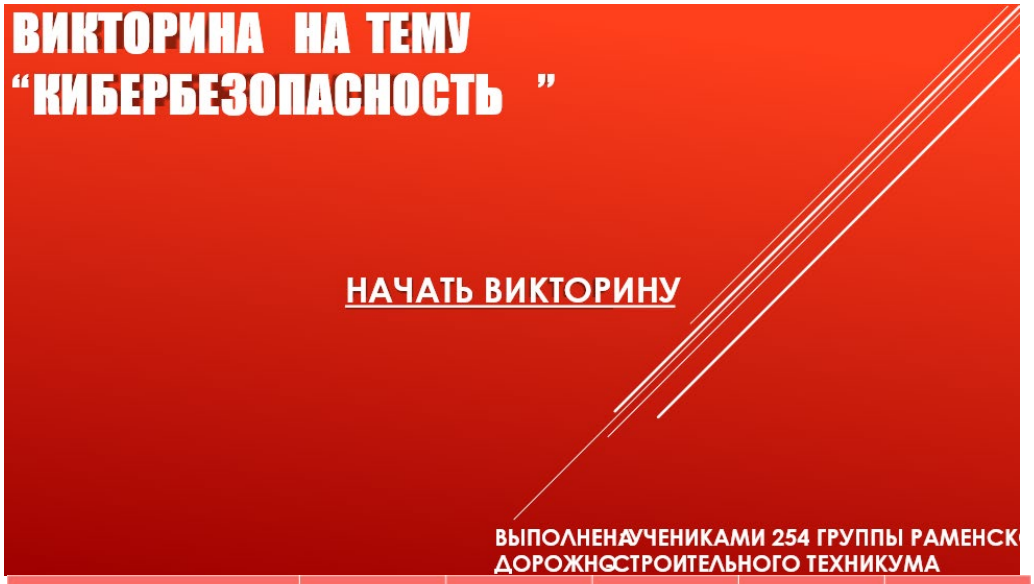
Приложение №1

Правила интернет-безопасности и интернет-этикета

1. Чаще обновляй операционную систему.
2. Используй лицензионные антивирусные программы.
3. Делай резервные копии важных документов.
4. Никогда не давайте личной информации о себе и членах семьи (номер телефона, адрес, данные паспорта идентификационный код) без разрешения родителей.
5. Если вы получаете или отсылаете информацию, которая беспокоит Вас (угрозы, оскорбления), не пытайтесь сами разобраться в этом, обратитесь к родителям. А вообще не делайте этого никогда.
6. Разрешайте родителям быть в курсе Ваших событий в социальных сетях. Общение должно быть корректным.
7. Не соглашайтесь на предложения встретиться с виртуальными знакомыми, если все же решились, то идите на встречу с друзьями, а не один.
8. Не принимайте предложения, не читайте писем от людей, которые Вам не знакомы или которым Вы не доверяете.
9. Не посещайте сомнительные сайты, содержащие всплывающие окна-рекламы. Пользуйтесь только образовательными сайтами.
10. Никому не давайте свой пароль электронной почты или страницы в социальной сети.
11. Никогда не делайте того, что может стоить больших денег Вашей семье, за исключением того, когда родители об этом знают.
12. Всегда будьте вежливыми с теми, с кем общаетесь, не употребляйте нецензурные слова в сообщениях. Это не украсит Вас перед окружающими.
13. Не набирайте текст сообщений В ВЕРХНЕМ РЕГИСТРЕ, это принимается в сети как крик и может вызвать гнев собеседника.
14. Не рассылайте любую информацию незнакомым Вам людям без их просьбы. Это воспринимается как «спам» и огорчает пользователей.
15. Никогда не пересылай «цепочковые» сообщения, удаляй их сразу после получения. Они могут тебе навредить.
16. Всегда веди себя в сети так, как хочешь, чтобы с тобой вели себя окружающие!

Приложение №2

Викторина «Кибербезопасность»



КОМАНДА №1	200	400	600	800	1000
КОМАНДА №2	200	400	600	800	1000
КОМАНДА №3	200	400	600	800	1000
КОМАНДА №4	200	400	600	800	1000

КОМАНДА №1

ВОПРОС НА **400** БАЛЛОВ

Как отличить фишинг сайт от обычныго?

УЗНАТЬ ОТВЕТ

ОТВЕТ:

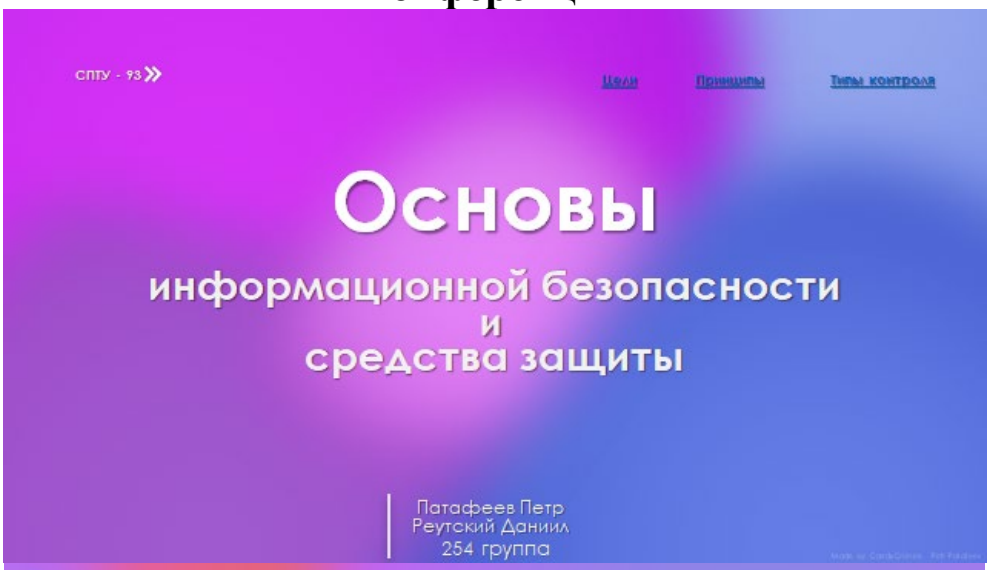
Как правило, мошенники регистрируют похожие домены. Например, вместо «online.sberbank.ru» можно увидеть «onllinesberbank.ru» или «online.sbrbank.ru». Также сайт может располагаться на поддомене, например, «sberbank.site.ru».

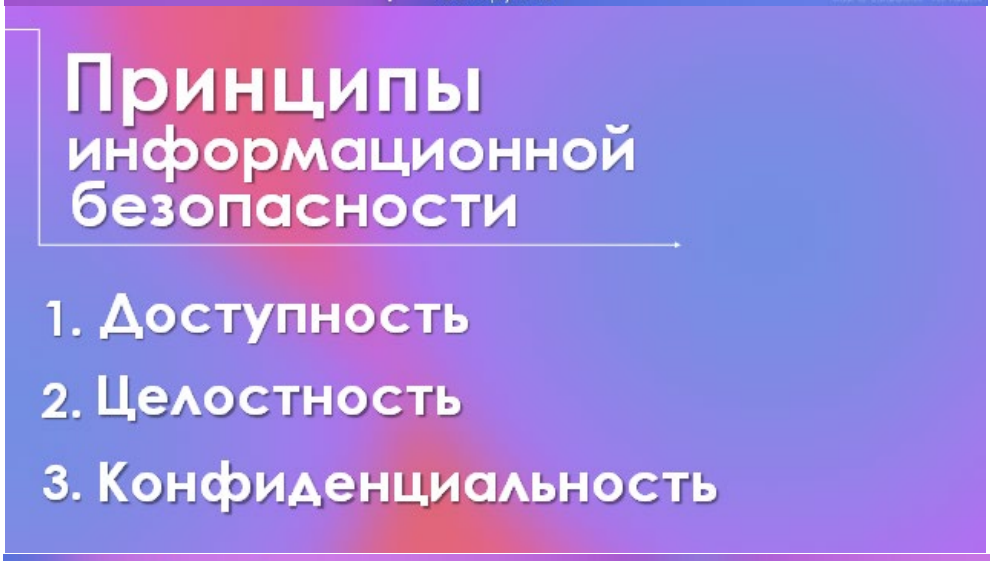
Отсутствие SSL сертификата

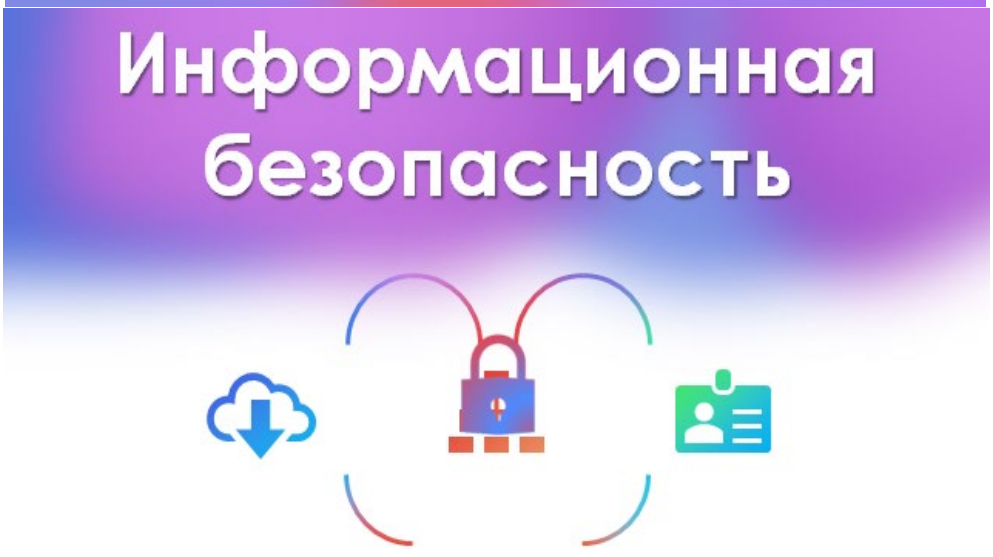
ВЕРНУТЬСЯ К ВЫБОРУ ЗАДАНИЙ

Приложение №3

Фрагмент одной из презентаций, представленных на конференции

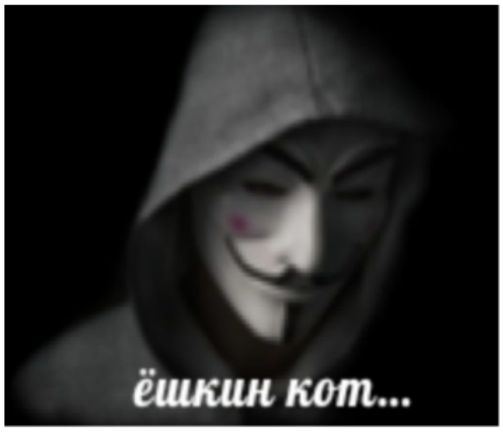






СПОСОБЫ КРАЖИ ДАННЫХ:

- Отправка электронных писем
- Создание фишинговых сайтов
- СМС – фишинг
- Вишинг (это не про вишню)



«ЛЕГКИЕ ДЕНЬГИ»

Не смотря на разнообразие способов обмана, мошенники преследует одну цель – украсть данные о банковских картах

Статистика за II квартал 2022 года

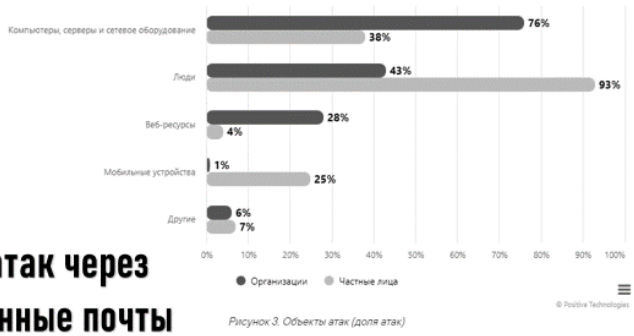


Рисунок 3. Объекты атак (доля атак)

Доля атак через электронные почты

Примеры скамерских/фишинг объявлений

Слили промокоды Ozon на покупки за 1 рубль!

Такое происходит не первый раз, подписчики канала [redacted] пользуются подобным постоянно! и забирают БЕСПЛАТНО не только одежду и обувь, но и iphone 12 за 1 450₽, apple watch 7 за 990₽, playstation 5 за 2 990₽

SCAM

[redacted] закрыты через 24 часа - [redacted]

Также в одно время набирали популярность идентичные по постановки текста промо с содержанием типа: «Угарный препод из МГУ», «Бывший сотрудник Тинькофф создал свой телеграмм канал», «Санкции открыли лазейку в законах, позволяющим россиянам зарабатывать деньги из воздуха», "Депутат призвала заблокировать аккаунт..." и тому подобный бред, который к правде относится также, как то, что Хогвартс существует.

Живешь от ЗП до ЗП?
Работай удаленно, проектируй дома и зарабатывай 80к - 150к в месяц, как тебе такое предложение?

Меня зовут Александр Касумов, я более 10 лет занимаюсь строительством и проектированием. У меня 2 фирмы: "Строй и живи" и "СВ-Фундамент". В кейсах у нас более 2500 спроектированных и 1300 построенных домов. А еще у меня есть школа для проектировщиков, в которой обучилось более 5000 студентов.

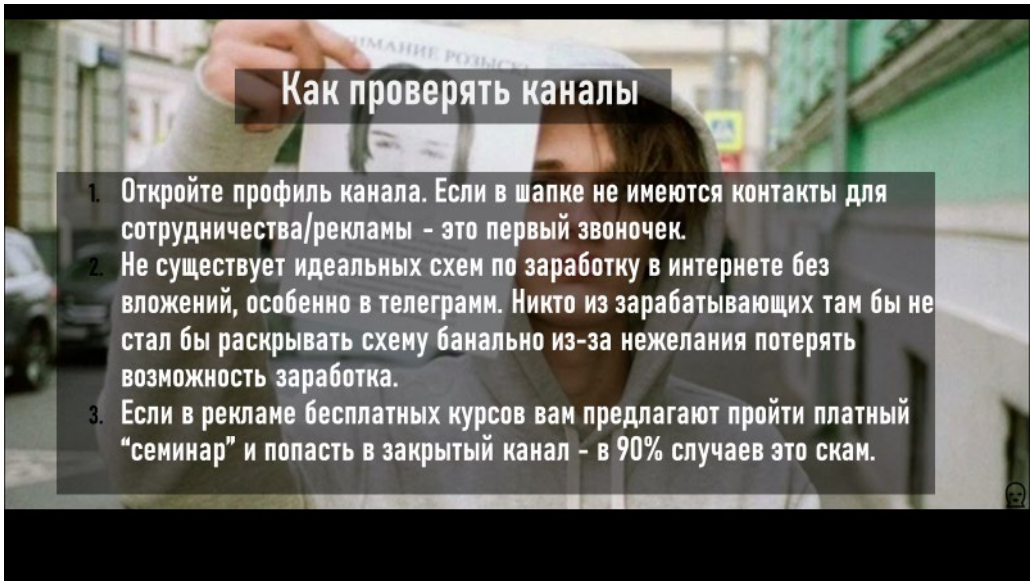
А теперь немного о тебе:
- У тебя нет технического образования и ты думаешь, что проектирование - это сложно?
- Ты устал работать в офисе за копейки и хочешь повысить свой доход?
- Или ты уже строитель и дополнительно хочешь научиться проектировать [redacted]

SCAM

Узнаешь себя? Тогда ре[redacted], где ты узнаешь:

- Почему нужно выбрать именно проектирование домов?
- Как стать востребованным проектировщиком и выйти на стабильный доход?
- Где искать своих первых клиентов?

Регистрируйся на вебинар по ссылке: [redacted]



Оценочный лист

КОМАНДА №1					
КОМАНДА №2					
КОМАНДА №3					
КОМАНДА №4					