Приложение к докладу

«РАЗРАБОТКА ТЕХНОЛОГИЧЕСКОЙ КАРТЫ И ПРОВЕДЕНИЕ МЕРОПРИЯТИЯ НА ТЕМУ «БЕЗОПАСНЫЙ ИНТЕРНЕТ»

**1. Что такое «интернет»**

Интернет – это замечательное изобретение человечества. Здесь можно найти друзей и единомышленников. Можно стать членом какого-то сообщества. Можно получить информацию по любому интересующему тебя вопросу.

Интернет (от лат inter – между и net[work] – сеть) – глобальная компьютерная сеть, связывающая между собой как пользователей сетей, так и пользователей индивидуальных (в том числе домашних) компьютеров.

**2. Какие опасности нас подстерегают в сети интернет.**

1) Спам

В наши дни у каждого заведена своя электронная почта. На неё приходят различные рассылки с подписанных нами сайтов, рабочие документы, отчёты и многое другое. Помимо прочего на вашemail могут приходить и спамные рассылки с незнакомых адресов. На самом деле они не так безобидны, как могут показаться на первый взгляд.

Ни за что не отвечайте на письма со спамом,спамеры могут узнать о том, что твой email действующий и могут дальше отсылать тебе спам. Если письмо содержит прикреплённый файл, то ни в коем случае не открывайте его, - там наверняка содержится вирус. В любом случае, стоит обязательно проверить файл на вирусы перед его просмотром.

2) Кибербуллинг–виртуальное издевательство.

Первый случай кибербуллинга был зафиксирован в 2002 году. Американский подросток Жислен Раза ради развлечения снял видеоролик, в котором он, подобно герою фильма «Звездные войны», фехтовал бейсбольной битой вместо лазерного меча. Эту запись посмотрели миллионы людей, через несколько дней был создан специальный сайт с исходным видео и пародиями на него. Насмешки сломали психику Жислена. Против одноклассников, разместивших исходное видео в интернете, был подан судебный иск.

Спектр целей киберпреследователей широк, но всех объединяет стремление нанести жертве психологический ущерб. Это могут быть шутки, которые просто уязвят жертву, а может быть психологический террор, который приведет к суициду.

Различают 8 основных видов кибербуллинга:

•Флейм (виртуальная перепалка) – обмен эмоциональными репликами в открытом доступе (чат, форум, блог);

• Буллинг – отправка жертве повторяющихся оскорбительных сообщений или звонков по сотовой связи;

• Понижение авторитета жертвы на форумах и чатах, совместное обсуждение реальных и мнимых недостатков жертвы;

• Клевета – распространение оскорбительной и неправдивой информации в виде фото, сообщений, песен;

• Самозванство – преследователь представляется жертвой, используя доступ к её аккаунту или создавая фейк, и распространяет в интернете негативную информацию, провоцируя окружающих на конфликт с жертвой;

• Изоляция. Формы изоляции в киберпространстве могут быть разными, начиная от создания закрытого сообщества до игнорирования сообщений жертвы.

•Киберпреследование – скрытое выслеживание жертвы с целью организации нападения, избиения, изнасилования и т.д.

•Хеппислепинг («HappySlapping» с английского «счастливое похлопывание») - избиение жертвы и запись этого на видео, с последующим выкладыванием ролика в сети.

Первое, что необходимо предпринять – это собрать доказательства издевательств над тобой. Потом отправить жалобу администраторам данного ресурса с просьбой принять меры. Второе, заблокировать отправку сообщений от обидчика. И третье, проявить выдержку и не ввязываться в конфликт.Если вас расстроило сообщение, картинка, видео и т.д. обратитесь за помощью и советом к родителям.Лучшая защита от нападения – игнор.

Помните, что анонимность в сети мнимая. Так что в случае нанесения реального вреда, найти злоумышленника можно. Следует скопировать сообщения, содержащие угрозы, и обратиться в правоохранительные органы.

Если вы явились свидетелем кибербуллинга, то можете помочь следующими действиями: выступить против преследователя, показать ему, что его действия оцениваются негативно, поддержать жертву, которой нужна психологическая помощь, сообщить взрослым о факте агрессивного поведения в сети.

3)Секстинг

Секстинг - пересылка личных фотографий, сообщений интимного содержания посредством современных средств связи: сотовых телефонов, электронной почты, социальных сетей.

Проблема секстинга заключается в том, что конфиденциальные фотографии могут быстро стать достоянием общественности.Когда фотография становится доступной в Интернете, то практически невозможно удалить все ее копии.В некоторых странах секстинг является уголовным преступлением, а если на интимных фотографиях изображен несовершеннолетний, то это считается детской порнографией.Причём виновными могут быть признаны оба: как человек, отправивший фотографии, так и получивший их — это классифицируется как производство и хранение детской порнографии соответственно.Кроме того, лицу, пославшему свои фотографии в обнажённом виде, могут быть предъявлены обвинения в сексуальном домогательстве.

Обратись к человеку, который непосредственно размеcтил у себя твою фотографию. Попроси его удалить эту фотографию. Если же человек отказывается, то обратись к администраторам ресурса, на котором была размещена твоя фотография. Если же и администраторы откажут, то необходимо обратиться в суд, но это ты уже должен сделать вместе с родителями.

Если тебе целенаправленно присылают подобную информацию, удаляй и не отвечай.Сообщи в полицию, если ты получил подобное содержимое. Ты не знаешь, является ли отправитель педофилом или нет. Таким образом, ты можешь помочь обществу.

Около 85% сотрудников отделов кадров говорят, что учитывают цифровую репутацию, решая, принять ли человека на работу. Поэтому твоя цифровая репутация очень важна, а думать над этим лучше уже сейчас.

4) Фальшивые письма и фишинговые сайты

Обычно злоумышленники используют доменные адреса с опечатками или субдомены.Другая распространённая уловка заключается в использовании внешне правильных ссылок, в реальности ведущих на фишинговый сайт. Т.е. написан один адрес, а гиперссылка ведет на другой.

В данном направлении выделяют следующие виды мошенничества:

• Вишинг. Мошенники высылают своей жертве сообщение о возникновении какой-то критической ситуации (исчезли деньги со счёта, срочная перерегистрация и прочее). В таких письмах используются реальные логотипы и названия банков, платёжных систем, социальных сетей; призыв к срочным действиям и ссылка, по которой нужно пройти для «подтверждения» информации.Перейдя по ссылке, ты попадаешь на сайт мошенников. Он внешне очень похож на официальный сайт, от имени которого тебе пришло письмо. Там тебя просят ввести всю необходимую информацию

• Фарминг. Это внедрение на компьютер вредоносной программы.Как только пользователь пытается посетить сайт, он перенаправляется специальной программой на его копию, созданную мошенником. Там человек, не замечая смены сайта, вводит свой логин и пароль.

• Смишинг.Мошенники рассылают сообщения на мобильный телефон, содержащие ссылку на фишинговый сайт.Переходя по ссылке, пользователь вводит свои личные данные, и таким образом информация передаётся злоумышленникам. На подставном сайте для получениякакой-либо услуги просят отправить SMS на предложенный номер или ввести свой номер сотового телефона, чаще всего это копии файлообменных сервисов.В первом случае с телефонного счёта абонента списывается крупная сумма, во втором - номер добавляется в базу адресов рассылки SMS-спама и может использоваться для дальнейших фишинговых действий.

5) Взлом аккаунта в социальной сети и почты.

Потеря контроля над аккаунтом может привести к различным последствиям, таким как рассылка спама и зараженных файлов от твоего имени или опубликование твоей переписки с друзьями.

Ты можешь заинтересовать не только кибер, но и других преступников. Например, размещая информацию о своей квартире, благосостоянии твоей семьи, сообщая куда ты с семьей поедешь на каникулы, ты можешь заинтересовать воров.

К тому же можно спровоцировать травлю себя со стороны пользователей сети, а также заражение вашего компьютера.

6) Фиктивные интернет-магазины.

Такие магазины являются незаконными. Они не имеют юридического адреса, не зарегистрированы в государственной предпринимательской базе.

Зачастую оплату товаров или часть оплаты требуется произвести сразу, до их доставки. Мошенники после произведённой оплаты пропадают, перестают отвечать на сообщения и телефонные звонки или присылают некачественный товар, за который невозможно вернуть деньги.

7) Заражение компьютерными вирусами.

Вирусы могут повредить или полностью уничтожить все файлы и данные, подконтрольные пользователю, от имени которого была запущена заражённая программа, а также повредить или даже уничтожить операционную систему со всеми файлами в целом.Меняются программные настройки, таинственным образом добавляются новые функции, необычные процессы появляются в диспетчере задач, или программы ведут себя так, будто их использует кто-то другой, а ты потерял над ними контроль.По статистике каждое тридцатое письмо заражено почтовым червем, а около 70% всей корреспонденции являются нежелательными.

С помощью вирусов хакеры могут использовать ресурсы компьютера для какой-либо незаконной деятельности. Файлывирусныхпрограммы называют служебным именем, маскируют под другую программу, файл другого типа или просто дают привлекательное для запуска название, иконку и т.п.

Если на твоем мониторе появилось сообщение, в котором требуют срочно активировать систему Windows, а для этого заплатить какую-то сумму, то знайте это вирус! Даже если это сообщение закрывает все окна и не дает тебе пользоваться компьютером, ничего платить не надо — это в любом случае не поможет. Обратитесь к сервисам по борьбе с баннерами на компьютере, которые есть у большинства антивирусных программ.

8) Ложь в сети и информационный мусор

«Если информация из Интернета, значит, она достоверна», - ошибочное мнение, поскольку интернет представляет собой безграничное количество мнений как профессионалов и дилетантов, так и откровенных обманщиков.

Интернет содержит огромное количество информации и, к сожалению, часть этой информации является информационным мусором. К тому же информация имеет свойство устаревать, а зачастую из общего контекста вырывается фрагмент и подается под определенным углом зрения.

Поисковый спам (мусорные страницы, тексты со ссылками на основной сайт с целью повышения его рейтинга в поисковых системах), репостинг (информация копируется и разносится по разным сайтам и соцсетям, иной раз меняя даже смысл сказанного), управляемая информация (заведомо ложная информация разносится с умыслом повлиять на общественное мнение) – всё это источники информационного мусора.

Так как отличить правду от ложной информации?

- Быть критичным к любой информации;

- Сортировать источники и экспертов по авторитетности;

- Проверять информацию: делать личные запросы, искать источники и официальные документы;

- Повышать собственную грамотность.

**3. Меры предосторожности в сети Интернет**

• Пользователю нужно уметь различать сайты по авторитетности, надежности, а информацию по достоверности;

• Ограничьте списки друзей в социальных сетях: не должно быть случайных и незнакомых людей;

• Используйте настройки конфиденциальности аккаунта: настройте просмотр содержимого вашей учетной записи "только для друзей”;

• Защищайте свою частную жизнь: не указывайте пароли, телефоны, адреса, дату рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как вы и ваши родители планируете провести каникулы;

• При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8.

• Для социальной сети, почты и других сайтов необходимо использовать разные пароли;

• Защищайте свою репутацию - держи ее в чистоте и задавай себе вопрос: хотел бы ты, чтобы другие пользователи видели, что ты загружаешь?

• Не размещайте фотографии и видео со своими друзьями без их разрешения. Обращайтесь к друзьям, чтобы они также соблюдали конфиденциальность и не размещали ваши фотографии и видео в общем доступе;

• Не создавайте и не распространяйте любую сексуальную информацию;

• Не используйте веб-камеру для общения с людьми, которых вы не знаете, также не раскрывайте им вашу личную информацию (имя, место жительства, учёбы и прочее);

• Если вы действительно желаете встретиться с человеком, с которым познакомились в интернете, то договоритесь о встрече в общественном месте и желательно взять с собой кого-то еще, например, друга. Если ваш сетевой друг считает, что присутствие кого-то еще - плохая идея, то стоит отказаться от встречи;

• Никогда не открывайте подозрительные ссылки, даже если они пришли от ваших друзей. Убедитесь в том, что друг выслал эту ссылку сам, а его аккаунт не контролирует киберпреступник. Получив файлы, не загружайте неизвестные файлы с расширением .exe, .dll, .bat;

• Не указывайте в личной почте личную информацию;

• Чтобы попасть в свою социальную сеть или на какой-либо другой сайт, лучше используйте закладки или окно быстрого доступа. Таким образом, вы точно попадёте на те порталы, которые безопасны и которыми вы пользуетесь;

• Надо уметь грамотно выбрать почтовый сервис. В интернете есть огромный выбор бесплатных почтовых сервисов, однако лучше доверять тем, кого знаешь и кто первый в рейтинге. Обычно это: Mail.ru, Gmail.com, Mail.yandex.ru, Outlook.com. Некоторые даже используют специальную систему защиты от знаменитых антивирусных программ;

• Используйте авторитетные и устоявшиеся в интернете сайты. Международные сайты могут не регулироваться нашими законами, поэтому риски увеличиваются, так как у вас не будет защиты от государства;

• Проверяйте адреса сайтов в браузерной строке. Когда вводите свои личные данные желательно, чтобы в адресной строке браузера появился значок ключа. Это означает, что соединение безопасно и ваши данные не будут украдены;

• Используйте современные операционные системы, имеющие серьёзный уровень защиты от вредоносных программ, и антивирусные программные продукты известных производителей. Скачивайте их только с официального сайта разработчика ОС. Регулярно обновляйте браузер и антивирусную базу. Помните, браузер - основной путь проникновения вирусов на компьютер. Нередко пиратские версии имеют установленные модули для взлома;

• Не устанавливайте несколько антивирусников, поскольку они распознают друг друга и могут вообще перестать работать;

• Используйте внешние носители информации, такие как флешка, диск или файл из интернета, только из проверенных источников;

• Если вас взломали, то необходимо предупредить всех ваших знакомых, которые добавлены в друзья, о взломе и спамных рассылка от вашего имени;

• При использовании Wi-Fi отключите функцию «Общий доступ к файлам и принтерам». Не допускайте автоматического подключения устройства к сетям Wi-Fi без вашего согласия;

•Ни в коем случае не платите, если вам предлагают работу через интернет и просят заплатить какую-то сумму за регистрацию, открытие счета, в залог или за пересылку данных. Настоящие работодатели не просят денег с соискателей;

• Прежде чем осуществить покупку обязательно изучите информацию о владельце интернет-магазина. На сайте должно быть указано:ИНН, ОГРН, юридический и фактический адрес, телефон, электронный адрес.Отсутствие какой-либо информации из этого списка должно вас насторожить.Отзывы покупателей могут быть созданы самим торговцем, больше доверия вызывают отзывы, где указаны координаты самого человека. Перед заказом необходимо точно знать цену, условия приобретения чего-либо, условия доставки и гарантийные условия. Если это не указано в анкете, то лучше всего будет лично связаться с продавцом и задать ему вопросы.

**4. Практика, создание конфликтных ситуаций**

1) Если вы хотите поделиться со своим другом игрой, нарушаете ли вы закон?

Ответ: Да, нарушается закон об авторском праве. Копирование музыки, фильмов и игр, загрузка и обмен ими — это пиратство. Можно предоставить только во временное пользование диск с игрой.

2) У вас на рабочем столе висит баннер, который предлагает избавиться от него за деньги. Ваши действия?

Ответ: Воспользуюсь сервисами от разработчиков антивирусов, которые помогут мне избавиться от баннеров. Далее необходимо поменять пароли доступа к моим аккаунтам и почте в сети, так как вирус может получить доступ к ним.

3) На телефон пришла смс от администрации социальной сети, где вы зарегистрированы. Они просят вас в рамках проверки достоверности аккаунта выслать свой пароль. Должны ли вы отправлять им свои данные?

Ответ: Нет. Скорее всего, это мошенники, которые хотят получить доступ к вашему аккаунту. Вам необходимо уведомить техподдержку социальной сети о случае фишинга.

4) Вы познакомились с человеком в сети и он предлагает вам встречи интимного характера. Ваши действия?

Ответ: Скорее всего, это педофил. Эта ситуация опасна, поэтому сообщи об этом своим родителям и обратись с ними в полицию.

5) Как выглядит адресная строка безопасного сайта?

Ответ: Более защищенным является сайт, у которого в адресной строке есть индикатор сертификата защиты в виде замка. Это специальная защита от подмены сайта.

6) Придумайте безопасное название почты и пароль.

Например, лучше выбрать «музыкальный\_фанат@» или «рок2013» вместо «тема13».