ПЕДЧАС

для педагогов

Тема: «*Основы безопасности в сети Интернет*»

Тема: «Основы безопасности в сети Интернет».
Цель: формирование устойчивых жизненных навыков при работе в сети Интернет.
Форма проведения: круглый стол.

Повестка:

1. Что такое интернет? Для чего нужен Интернет?
2. Какие существуют риски при пользовании интернетом, виды мошенничества и как их можно снизить?
3. Что такое безопасный чат?
4. Как вы можете обезопасить себя при пользовании службами мгновенных сообщений?

1. Что такое интернет? Для чего нужен Интернет?

- Всемирная паутина ежегодно завлекает в свои сети миллионы новых пользователей.
- Среднестатистический современный человек уже с трудом представляет свое существование без Интернета.
- Однако далеко не все могут точно ответить на вопрос, что такое интернет – ведь для каждого из нас он играет свою роль.

Интернет нужен для передачи и приема информации. Его можно представить как одно большое виртуальное поле информации, которое замечательно структурировано и оснащено системой поиска. Без системы поиска интернет не был бы настолько популярен.

Ответ на такой вопрос скоро перейдет в стадию максимально обобщенной парадигмы. "Для чего нужна жизнь?" и "Для чего нужен Интернет?" - это вопросы, которые в скором будут находится на одном уровне значимости. Как ответить на этот вопрос подробно?

Сколько людей, столько и мнений. Каждому нужен интернет по своему. Статья длиною в три тысячи символов недостаточна, чтобы даже сокращенно пробежаться по всем целям использования интернета в наше время.

Давайте обратимся к основным пунктам, которые как нам мыслится имеют первостепенное значение.

Для чего нужен интернет:

1. Чтобы передавать и принимать тексты, сообщения, офисные документы (в электронном виде, в любом из существующих форматов), графические материалы, аудиозаписи, видеоматериалы и т.д. То есть, другими словами - осуществлять оперативное (и долгосрочное, перспективное) общение со своими партнерами, коллегами по работе, клиентами, родственниками или друзьями.

2. Получать доступ к огромному числу справочников (адресных, географических, отраслевых, специальных и т.п.) и иной схожей, но более подробной информации.

3. Постоянно быть в курсе последних мировых и региональных новостей (причем, информацию можно как "просматривать" (в текстовом, графическом виде, в видео формате), так и "прослушивать".

4. Создавать, исполнять или пользоваться процессами и технологиями. Мы можем: проводить любые операции со своими банковскими счетами (от проплат по международным контрактам до оплаты коммунальных услуг); участвовать в биржевых торгах, не выходя из дома или офиса (а с помощью "ноутбука" и сотовой или спутниковой связи, вообще из любой

точки земного шара); покупать (и продавать) все, что необходимо для бизнеса или для личного потребления, через Internet-магазины. Сегодня в мире через Сеть продается практически все, часто - с доставкой на дом. Можно выбрать по каталогу одежду или обувь, заказать обед, запросить понравившуюся книгу или видеокассету и все будет доставлено по указанному адресу.

5. Общаться по интересам, чувствовать себя гражданином мира. То, что помогает всем, кто нуждается в групповой и индивидуальной психотерапии, а также обычном каждодневном развитии: ведь где и когда еще можно одновременно обсуждать одно и то же с несколькими сотнями, а то и тысячами людей?

6. Удаленно учиться*, иными словами* - ***получать образование в другой стране,*** не выезжая из своей. На самом деле никакая другая учеба не может быть так удобна. Ехать потом, за подтверждением и окончательным получением всех документов, конечно, придется, но ведь вначале - какая экономия сил, средств, времени! А если учесть, что термин "учеба" подразумевает не только преподавателей в аудиториях, академические часы и дисциплины, но и любой познавательный процесс, участвуя в котором, человек приобретает и закрепляет разнообразные навыки.

7. Осуществлять Internet-консалтинг, как поиск и обработку информации из самой сети (поиск поставщиков и потребителей, мониторинг и анализ рынков и т.д). Проводить маркетинговые и социологические исследования рынка. Где как не в Сети это можно делать быстро и довольно в больших объемах?

8. Заниматься рекламой. Пока что самым популярным и распространенным видом является и самая примитивная - баннерная. Она лидирует по всем параметрам, но не далек тот день, когда и все остальное сюда придет.

9. Создавать собственный сайт. То есть - тоже заниматься рекламой, но уже вроде как никого на это не "заряжая", собственными силами. Удобно: деньги тратятся на это один раз - при создании, а не каждый раз, как понадобится напомнить о себе. Плюс неограниченное количество информации, размещенное на своем сайте, подробно представленное и "обставленное" всем чем угодно - текстами, фото, графиками, видео-роликами.

10. Работа в интернете! И тут уж, сами понимаете, как он может быть нам НЕ НУЖЕН? Универсальнейший инструмент и предмет обработки этим самым инструментом - одновременно.

К сожалению, в интернете плохая сторона представлена более ярко, ну а светлая созидающая сторона блекнет. Все зависит от самих пользователей интернета. Мы сами наполняем нашу жизнь и определяем ее качество. Мы сами наполняем интернет и определяем его ведущую сторону.

2. Какие существуют риски при пользовании интернетом, и как их можно снизить?

Все опасности интернет-среды мы объединяем в четыре крупные группы рисков:

Контентные риски

Контентные риски — это материалы (тексты, картинки, аудио, видеофайлы, ссылки на сторонние ресурсы), содержащие насилие, агрессию, эротику и порнографию, нецензурную лексику, информацию, разжигающую расовую ненависть, пропаганду анорексии и булимии, суицида, азартных игр, наркотических веществ и т.д. Столкнуться с ними можно практически везде. Это и сайты, и социальные сети, и блоги, и торренты, и видеохостинги, фактически все,

что сейчас существует в Интернете. Зачастую подобный материал может прийти от незнакомца по почте в виде спама или сообщения.

Негативные контентые материалы можно условно разделить на:

- незаконные, к которым могут относиться: детская порнография; наркотические средства; материалы, имеющие отношение к расовой или религиозной ненависти; а также ненависти или агрессивного поведения по отношению к группе людей, отдельной личности или животным; азартные игры и т.д.

- неэтичные, противоречащие принятым в обществе нормам морали и социальным нормам.

Контентные риски связаны с другими типами рисков Сети. Например, просмотр тех или иных видео-материалов может привести к заражению компьютера вирусами и потере важных данных. Очень многие распространители подобного негативного контента преследуют цель заразить компьютер, чтобы в дальнейшем иметь возможность манипулировать данными и действиями зараженного компьютера. Пропаганда негативных материалов также может идти через социальные сети, блоги, различные форумы. В данном случае контентные риски пересекаются с коммуникационными.

Коммуникационные риски

Коммуникационные риски связаны с межличностными отношениями интернет-пользователей и включают в себя риск подвергнуться оскорблениям и нападкам со стороны других. Примерами таких рисков могут быть: незаконные контакты (например, груминг), киберпреследования, кибербуллинг и др. Для подобных целей используются различные чаты, онлайн-мессенджеры (ICQ, Google talk, Skype и др.), социальные сети, сайты знакомств, форумы, блоги и т.д.

Даже если большинство пользователей существующих чат-систем (веб- чатов или IRC) обладают добрыми намерениями, существует, к сожалению, растущее число людей, использующих эти беседы со злым умыслом. В некоторых случаях они хотят обманом заставить детей выдать личные данные, такие как домашний адрес, телефон, пароли к персональным страницам в интернете и др. В других случаях они могут оказаться педофилами в поисках жертвы. Выдавая себя за сверстника и устанавливая дружеские отношения с ребенком, они выведывают о нем много информации и понуждают к личной встрече.

Оказаться жертвой намного проще, чем кажется. Каждый участник той или иной социальной сети может признаться, что хотя бы один раз ему приходило непристойное предложение от неизвестного человека. Это беда не только социальных сетей. На любом популярном форуме, в блоговом сообществе и чате появляются такие участники, которые хамят и оскорбляют других участников.

Коммуникационные риски включают в себя «незаконный контакт» и «киберпреследование» (или кибер-буллинг).

Незаконный контакт — это общение между взрослым и ребенком, при котором взрослый пытается установить более близкие отношения для сексуальной эксплуатации ребенка. Это понятие включает в себя такие интернет-преступления как домогательство и груминг.

Домогательство — причиняющее неудобство или вред поведение, нарушающее неприкосновенность частной жизни лица. Такое поведение может заключаться в прямых или косвенных словесных оскорблениях или угрозах, недоброжелательных замечаниях, грубых

шутках или инсинуациях, нежелательных письмах или звонках, показе оскорбительных или унизительных фотографий, запугивании, похотливых жестах, ненужных прикосновениях, похлопываниях, щипках, ударах, физическом нападении или в других подобных действиях.

Груминг — установление дружеских отношений с ребенком с целью изнасилования. Злоумышленник нередко общается в интернете с ребенком, выдавая себя за ровесника либо ребенка немного старше. Он знакомится в чате, на форуме или в социальной сети с жертвой, пытается установить с ним дружеские отношения и перейти на личную переписку. Общаясь лично («в привате»), он входит в доверие к ребенку, пытается узнать номер мобильного и договориться о встрече.

Киберпреследование (или кибер-буллинг) — это преследование пользователя сообщениями, содержащими оскорбления, агрессию, сексуальные домогательства с помощью различных интернет-сервисов. Также, киберпреследование может принимать такие формы, как обмен информацией, контактами; запугивание; подражание; хулиганство (интернет-троллинг); социальное бойкотирование. По форме буллинг может быть не только словесным оскорблением. Это могут быть фотографии, изображения или видео жертвы, отредактированные так, чтобы быть более унизительными.

Подобный унизительный контент может исходить от одного человека или группы людей по одному или нескольким электронным контактам жертвы, на электронный ящик или в сообщениях онлайн-мессенджеров. Распространены также случаи преследования в социальных сетях или на подобных им ресурсах. При этом помимо рассылки оскорбительных сообщений и вывешивания унизительных материалов, изображений или видеозаписей, буллер может также взломать профиль или страницу жертвы и организовать спам-рассылку по всем контактам жертвы.

К сожалению, кибербуллинг — очень распространенное явление среди российских подростков. Каждый пятый ребенок может признать, что подвергался буллингу онлайн или в реальной жизни. И это беда не только России, она распространена во всем мире. Но в России дети становятся жертвами буллинга в интернете так же часто, как и в реальной жизни.

Нередко кибербуллинг берет начало в отношениях с реальными людьми, и в этом случае, жертва знает своих оскорбителей. Когда же буллинг берет свое в интернете, всегда важно удостовериться, чтобы он не перерос в реальное насилие над ребенком.

Электронные риски.

Электронные (кибер-) риски — это возможность столкнуться с хищением персональной информации, риск подвергнуться вирусной атаке, онлайн-мошенничеству, спам-атаке, шпионским программам и т.д. Вредоносное ПО (Программное Обеспечение) использует широкий спектр методов для распространения и проникновения в компьютеры, не только через компакт-диски или другие носители, но и через электронную почту посредством спама или скачанных из Интернета файлов.

К вредоносным программам относятся вирусы, черви и «троянские кони» – это компьютерные программы, которые могут нанести вред вашему семейному компьютеру и хранящимся на нем данным. Они также могут снижать скорость обмена данными с Интернетом и даже использовать ваш компьютер для распространения своих копий на компьютеры ваших друзей, родственников, коллег и по всей остальной глобальной Сети. Защита в социальных сетях — это задача, которая не так давно стала актуальна для их

пользователей. Буквально несколько месяцев назад, взлом страниц в социальных сетях превратился в один из основных способов распространения спама в Интернете.

В частности, теперь вирусное ПО (программное обеспечение), которое рассылает спам в социальной сети может быть установлено на ваш компьютер с любого сайта. И от вашего лица могут регулярно рассылаться абсолютно любые сообщения, избавиться от которых не поможет ни одна защита самого сайта. Хотя бы просто по той причине, что в этом случае потребуется не защита вашей страницы, а современное антивирусное программное обеспечение. Поэтому не забывайте обновлять свою антивирусную программу и следить за защитой своего компьютера.

К сожалению, вероятность наткнуться на подобные вредоносные программы очень велика. Помимо негативного воздействия на компьютер и мобильное устройство, можно стать жертвой еще одного вида кибер- преступления — кибер-мошенничества. В самом широком смысле мошенничество — это умышленный обман или злоупотребление доверием с целью получения какой-либо выгоды.

Мошенничество в сети Интернет (кибермошенничество) — один из видов киберпреступления, целью которого является обман пользователей. Хищение конфиденциальных данных может привести к тому, что хакер незаконно получает доступ и каким-либо образом использует личную информацию пользователя (номера банковских счетов, паспортные данные, коды, пароли и др.), с целью причинить материальный и финансовый ущерб.

Потребительские риски

Потребительские риски – злоупотребление в интернете правами потребителя. Включают в себя: риск приобретения товара низкого качества, различные поделки, контрафактная и фальсифицированная продукция, потеря денежных средств без приобретения товара или услуги, хищение персональной информации с целью кибер-мошенничества, и др.

Также дети, зачастую совершая онлайн покупки, могут растратить значительные суммы своих родителей, если каким-либо способом имели или получили к ним доступ.

Одним из самых распространенных видов данного типа рисков является мошенничество — это умышленный обман или злоупотребление доверием с целью получения какой-либо выгоды. Мошенничество, как правило, является преступлением.

Поскольку мошенничество в сети интернет совершается с помощью различных технических средств и разнообразного количества программ, то некоторые его виды могут быть отнесены и к группе электронных рисков, а часть к группе коммуникационных, поскольку включает в свою схему установления более близкого контакта с жертвой в течение какого-либо времени (например, с помощью электронных писем и смс, которые могут привести и к реальным встречам с мошенниками).

Десять правил безопасного пользования интернетом

Интернет прочно вошел в нашу жизнь. Он помогает нам общаться с друзьями, знакомиться с новыми людьми, учиться, слушать любимую музыку и смотреть фильмы. Возможности Глобальной сети с каждым годом возрастают. Но, как оказывается, интернет может приносить не только пользу, но и вред.

Как же предотвратить его вредоносное воздействие? Предлагаем вашему вниманию ряд практических рекомендаций, используя которые вы сможете избежать многих интернет —

угроз. Они помогут обезопасить не только общение с людьми во всемирной паутине, а также снизят нежелательные риски при использовании онлайн — игр и мобильного телефона.

1. Для защиты своего компьютера необходимо регулярное обновление программного обеспечения, использование надежных антивирусных и антишпионских программ.

2. В интернете не стоит переходить по ссылкам и нажимай кнопки во всплывающих сообщениях, которые кажутся подозрительными. Даже если вас будут уверять, что там находится нечто очень важное лично для вас.

3. Для защиты личной информации придумайте надежный пароль и никому его не сообщайте. Для каждого ресурса стоит использовать уникальные логины и пароли.

4. Никогда не предоставляйте секретные сведения, например, номер счета или пароль в ответе на сообщение электронной почты или в социальных сетях.

5. Прежде чем вводить секретные сведения в веб-форме или на веб-странице, обратите внимание на наличие таких признаков, как адрес веб-страницы, начинающийся с префикса https и значка в виде закрытого замка рядом с адресной строкой, который обозначает безопасное соединение.

6. Для безопасности общения в социальных сетях оставляйте как можно меньше данных о себе и избирательно подходите к предложениям о дружбе.

7. Откройте пункт «Настройки» или «Параметры» в таких службах, как Facebook и Twitter, чтобы настроить список пользователей, которые могут просматривать ваш профиль или фотографии, помеченные вашим именем, контролировать способы поиска информации и добавления комментариев о вас, а также узнать, как можно заблокировать некоторых пользователей.

8. Перед просмотром входящих писем на электронном ящике, проверьте адрес отправителя. Подозрительные письма смело отправляйте в спам, особенно если в таких письмах содержатся прикрепленные файлы.

9. В чатах и системах мгновенного обмена сообщениями вы никогда не можете быть уверенными, кто с вами общается. Постарайтесь избегать общения с незнакомцами и ни в коем случае не соглашайтесь с ним на встречу в реальной жизни.

10. Для скачивания картинки или мелодии вам предлагают отправить смс? Не спешите! Сначала проверьте этот номер в интернете — безопасен ли он и не обманут ли вас.

Будьте бдительны на просторах всемирной паутины и берегите себя!

Что такое безопасный чат?

Человек, с которым происходит общение, в значительной сте-пени определяет, насколько безопасной и приятной для вас являет ся атмосфера в чате. Как правило, степень безопасности чата, в ко-тором общается ребенок, можно определить по трем основным вопросам. Иногда в чатах работают добровольные модераторы, ко-торые предотвращают случаи неуместного общения и могут забло-кировать доступ в чат для хулиганов и других нарушителей порядк. т Если контроль не осуществляется, в чате по крайней мере должна иметься кнопка для связи с администратором. Для детей предпоч тительны контролируемые чаты; уровень безопасности также повы-шается, если беседы сохраняются.

Инструкции по безопасному общению в чатах:

Дети, которые общаются в чатах, должны знать, как делать это безопас-ным образом. Каждый должен помнить о следующих внутренних правилах чата.

1. Не доверяйте никому вашу лич-ную информацию.

2. Сообщайте администратору чата о проявлениях оскорбительного поведе-ния участников.

3. Если вам неприятно находиться в чате, покиньте его.

4. Если вам что-то не понравилось, обязательно расскажите об этом родителям.

5. Будьте тактичны по отношению к другим людям в чате.

Личная беседа

При знакомстве с новым человеком в интерактивной дискус-сионной группе, возможно, захочется перейти от общения в обще-ственном чате к более личной беседе с глазу на глаз. Например, можно начать беседу в общей комнате чата, а затем перейти к об-щению с помощью программы мгновенного обмена сообщениями или переписке по электронной почте. При использовании этих средств можно по-прежнему обеспечить защиту своей личности путем использования псевдонима (например, псевдонимом@до-мен, ru). Кроме того, проще предоставить такой тип адреса на случай, если новым контактом окажется человек, с которым необхо-димо будет прекратить общение. Рекомендуется наставить детей, чтобы они отказывались от участия в личных интерактивных бесе-дах с людьми, которых они не знают в жизни.

Встреча с собеседниками из Интернета

Если ребенок общается в Интернете с новым человеком, воз-можно, ему/ей захочется лично встретиться с этим другом. Даже если дружба через Интернет поддерживалась в течение некоторого времени, эту встречу стоит воспринимать с осторожностью. Не-смотря на то, что большинство встреч друзей по Интернету явля-ются веселыми и безопасными мероприятиями, к сожалению, иногда они могут оставить неприятные впечатления. К счастью, случаи подобного рода крайне редки. Если встреча запланирована, настоятельно рекомендуется сопровождение ребенка родителем или другим взрослым, которому ребенок доверяет, а также прове-дение встречи в общественном месте.

Интернет-этика

Если вы хотите, чтобы дети стали ответственными пользователями, объясните им фундаментальные правила поведения в сети:

- Узнайте правила прежде, чем что-нибудь сказать или сделать. Некоторые чаты и форумы имеют специальные правила, поясняющие, что Вы можете и не имеете права говорить или делать. Так как некоторые люди критически относятся к тем, кто нарушает правила, знание правил может избавить вас и вашего ребенка от ненужного дискомфорта.

- Думайте прежде, чем что-либо напечатать. Удостоверьтесь, что вы говорите приемлемые вещи, которые не приведут к разгоревшемуся конфликту. Единственное, в чем вы можете не сомневаться, — это в том, что все, сказанное вами в Интернете, может вернуться и неотступно преследовать вас.

- Не относитесь критически к другим, особенно к новичкам, даже ес-ли они нарушают правила. Если вы должны помочь кому-то или исправить кого-то, сделайте это по электронной почте, а не на общественном форуме (например, в чате). Помните, что и вы когда-то были новичком.

- Не тратьте время других пользователей впустую. Не посылайте цепочку электронных писем, не передавайте киберслухи, не разыгрывайте других, не рассылайте спам.

- Защищайте личную жизнь и личную информацию других пользователей. Не публикуйте в онлайне чей-либо адрес электронной почты без разрешения владельца. Вместо

этого можно использовать опцию «Отправить по электронной почте». Не используйте без разрешения чужой пароль.

- Не присваивайте вещи, не платя за них (в основном это касается условно-бесплатного программного обеспечения).

Как не следует вести себя в сети

- Печатать ЗАГЛАВНЫМИ БУКВАМИ, что может рассматриваться как крик, провоцирующий спор или конфликт.
- Размещать ложную информацию или грубые высказывания о другом человеке.
- Отправлять большие вложенные файлы, не спросив разрешения у получателя.
- Обращаться к другим в чате по их настоящему имени.
- Рассылать электронную почту рекламного содержания людям, которых Вы не знаете (что является разновидностью спама).
- Отклоняться от темы разговора на форуме.
- Не дожидаться своей очереди или не следовать правилам чата или форума.

4. Как вы можете обезопасить себя при пользовании службами мгновенных сообщений?

Большинство пользователей знакомы со службами мгновенных сообщений (Instant Messaging, IM) - приложениями-мессенджерами, которые позволяют нам общаться с друзьями и знакомыми онлайн в режиме реального времени через интернет и отслеживать их статус в сети.

Мессенджеры приносят реальную пользу, позволяя легко обмениваться информацией и пользоваться другими дополнительными услугами, такими как видеоконференции и голосовой чат.

Однако, эти возможности подразумевают ответственность, и человек, использующий мессенджер, должен осознавать и уделять внимание аспектам безопасности и конфиденциальности служб мгновенных сообщений, чтобы оставаться в безопасности в сети и не раскрывать персональную информацию посторонним. Безопасное использование мессенджера - наша основная тема сегодня.

2. Введение в IM

2.1. Общее представление:

Службы мгновенных сообщений широко используются на протяжении последних 10 лет и их использование с распространением интернета продолжает расти как с точки зрения пользовательской базы, так и сложности приложений.

Популярность мессенджеров в большой степени обусловлена тем фактом, что, в отличие от традиционной электронной почты, ответ на сообщение может быть получен в течение нескольких секунд, что значительно увеличивает скорость коммуникации.

Кроме того, вы всегда знаете, кто из ваших друзей и коллег находится в сети, в то же время и им доступны ваш статус и наличие желания пообщаться.

В дополнение к беседе, вы имеете возможность отправить с помощью мессенджера файл или ссылку, инициировать голосовой или видеочат, доступные в некоторых программах. Вы даже можете играть и удаленно использовать приложения совместно с кем-либо из ваших контактов.

2.2. Предпосылки:

Чтобы начать пользоваться мессенджером, вам всего лишь нужно выбрать сеть и установить программное обеспечение. Наиболее распространенные на сегодняшний день службы мгновенных сообщений - ICQ, AIM (AOL Instant Messenger), Windows Live (MSN) Messenger, Yahoo! Messenger, Jabber и Skype.

Для доступа в сеть используется клиентское программное обеспечение, доступное для бесплатной загрузки.

Существуют также независмые клиенты сторонних производителей, такие как Miranda или Trillian, которые поддерживают несколько протоколов в одной программе, так что если у вас есть аккаунты в нескольких сетях, скажем, ICQ и AIM, вам не нужно устанавливать два различных приложения - вы можете настроить обе службы в одном клиенте и при необходимости переключаться между профилями.

2.3. Как работает служба мгновенных сообщений:

Вы осуществляете вход в свою учетную запись службы мгновенных сообщений с помощью программного обеспечения, загруженного с сайта сети, которую вы выбрали, или инициируете сессию с помощью браузера, ничего не загружая.

Последний подход становится все более распространенным, так как все больше приложений реализуются в виде веб-служб, как альтернатива программным средствам для настольных систем. Например, Google Talk предоставляет такую возможность.

Существует два способа отправки сообщения через сеть службы мгновенных сообщений: с использованием IM-сервера в качестве посредника при передаче данных или прямой обмен данными между клиентами (peer-to-peer).

В первом случае, информация, которой обмениваются два клиента, проходит через центральный IM-сервер, который затем направляет соответствующие сообщения указанным в них адресатам.

Во втором, сервер способствует инициации соединения, «объясняя» клиентам, каким образом им следует «общаться» между собой (предоставляя им соответствующие IP-адреса и номера коммуникационных портов).

В дальнейшем обмен сообщениями происходит напрямую между клиентами, без участия сервера. Этот вариант более эффективен в смысле расходования ресурсов, так как не требуется серверных ресурсов для обработки и передачи данных.

Он также является более безопасным, так как сообщения проходят меньший путь, если клиенты находятся недалеко друг от друга, и поэтому менее подвержены риску быть перехваченными.

При данном подходе, если двое людей, находящиеся в одной корпоративной или домашней сети, захотят обменяться сообщениями по ICQ, их сообщения не будут покидать границы этой сети, делая практически невозможным перехват их разговора кем-то вне ее пределов.

Тем не менее, наиболее часто используемый способ соединения - это конфигурация клиент-сервер-клиент, используемая большинством интернет-протоколов.

Однако, передача больших файлов или сессия по работе с удаленным рабочим столом через службу мгновенных сообщений происходит исключительно как peer-to-peer соединение для снижения нагрузки на сервер.

2.4. Процедура входа:

Большинство служб мгновенных сообщений используют стандартную комбинация логин/пароль, предоставленную клиентом для авторизации на сервере при попытке пользователя подключиться к службе.

Эта информация отправляется в незашифрованном виде, то есть любой, кто сможет внедриться в сессию авторизации, сможет легко перехватить данные входа и украсть учетную запись. Более безопасный способ идентификации пользователей – использование возможности «безопасного входа», доступной в некоторых IM-службах, таких как ICQ.

По сути, это означает, что IM-клиент шифрует учетные данные с помощью специального ключа, выпущенного сервером при соединении. Это снижает вероятность перехвата сетевых пакетов и извлечения из них учетных данных.

При успешной проверке система впускает пользователя и он может видеть список своих «друзей», а также другую существенную информацию, такую как статус людей в списке контактов.

3. Элементы безопасности IM-служб

3.1. Ваш IM-профиль:

При выборе отображаемого имени (или псевдонима) старайтесь использовать имена, которые не могут быть однозначно ассоциированы с вами, например, "vp_krutoj26" вместо "vasyapupkin26".

Также, никогда не разглашайте свои персональные данные, такие как домашний адрес, номер телефона и иную существенную информацию в вашем сетевом профиле.

При выборе пароля убедитесь, что его длина не меньше 6 символов и используйте комбинацию, отличающуюся от используемых в других учетных записях (например, пароля к электронному почтовому ящику, на который будет отправлено письмо с паролем от IM-аккаунта, в случае, если вы его забудете).

Большинство IM-клиентов хранят ваш пароль в локальном кэше для автоматизации последующих входов.

Мы рекомендуем вам вводить пароль вручную каждый раз при входе в сеть (иными словами, не сохраняйте ваш пароль), но если вы поступаете иначе, убедитесь, что пароль не виден на экране входа или в локальном кэше, обычно хранящемся в реестре Windows.

Обратитесь к разработчику вашей IM-службы за информацией о том, каким образом производится работа с кэшированными паролями.

Избегайте использования службы мгновенных сообщений в публичных местах, таких как библиотеки или интернет-кафе. Если этого не избежать, никогда не сохраняйте пароль при входе.

Убедитесь, что ваша система не заражена вирусами, кейлоггерами или иным вредоносным ПО, так как они способны полностью свести на нет все ваши усилия по сокрытию пароля - с помощью прямой записи вашей клавиатурной активности и передачи ее мошенникам.

Если ваш IM-аккаунт был захвачен, известите всех своих коррепондентов и постарайтесь восстановить его, предоставив как можно более полную информацию в специальном разделе восстановления учетных записей на сайте IM-службы.

3.2. Использование:

Самое главное, о чем стоит помнить при использовании служб мгновенных сообщений, что любая информация, которую вы отправляете или получаете, передается в явном, легко читаемом текстовом формате, поэтому никогда не передавайте конфиденциальную или частную информацию по каналам IM.

Многие недооценивают этот риск до того момента, когда становится уже слишком поздно и их учетная запись захвачена, данные кредитки украдены, а личная информация раскрыта или использована не по назначению.

Хакер или неблагонадежный ISP могут легко «подслушивать» IM-сессии, записывая разговоры и продавая их за финансовое вознаграждение или публикуя их на форумах просто с целью развлечься.

Такое вторжение весьма вероятно, так как, используя изощренные "подслушивающие" программы, которые перехватывают сетевой трафик, или уязвимости протокола TCP/IP, хакеры могут имитировать как отправляющую, так и принимающую сторону без их ведома.

Вы можете частично избежать этого, установив дополнительный модуль, шифрующий IM-трафик с помощью PGP-ключа. Бесплатный мультипротокольный IM-клиент Miranda предоставляет опциональную возможность шифрования данных для конфиденциального обмена информацией.

Считается, что организаторы терактов 11 сентября использовали шифрование в своей переписке для обмена данными о будущих нападениях, поэтому ФБР не могло перехватить их сообщения.

Как и в случае с любой другой сетевой программой ошибки и уязвимости могут подвергнуть систему риску. Убедитесь, что ваша система и программа-клиент обновляются

должным образом.

IM-черви используют уязвимости в программном обеспечении служб мгновенных сообщений и крайне быстро способны пересылать собственные копии всем пользователям из списка контактов жертвы.

Другое важное правило - никогда не загружать и не открывать исполняемые файлы, полученные через службу IM, и, если возможно, проверять все файлы обновленным антивирусом.

Никогда не щелкайте по ссылкам в сообщениях, особенно если сообщение от неизвестного источника; также полезно быть начеку при получении сообщений от друзей – они также могут быть отправлены с зараженной системы.

Интернет-ссылки могут вести на зараженные сайты и, щелкнув по ним, вы можете непреднамеренно заразить свой компьютер. Так как загрузка файлов обычно осуществляется на основе технологии peer-to-peer, ваш IP-адрес доступен противоположной стороне, что не исключает возможность удаленного вторжения в том случае, если ваша сеть не защищена брандмауэром.

Более древние клиенты, такие как ICQ 2003, могут по умолчанию раскрывать ваш внешний IP-адрес, так что стоит помнить о том, что необходимо вовремя обновлять ваш IM-клиент до последней версии.

Многие IM-клиенты локально сохраняют все ваши беседы, чтобы позже вы могли их при желании просмотреть. Вы можете выключить данную функцию через опцию настройки IM-клиента.

Еще одна неприятность - спам по каналам служб мгновенных сообщений (SpIM, spam over IM). Эти сообщения могут содержать что угодно – от предложений купить что-то до попыток заражения вашего ПК через загрузку файла.

Многие IM-клиенты имеют защиту от спама, которая может оказаться крайне полезной. Однако, наиболее разумный ответ на спам – это отсутствие реакции или ответа - сам факт ответа говорит спамеру (человеку или программе) о том, что данный электронный адрес существует и действует.

Некоторые клиенты предлагают внедрить систему запроса и подтверждения, которая передаст вам сообщение от неизвестного пользователя только если он ответит на простой вопрос, что позволяет убедиться, что это не спам-бот.

К запросам на авторизацию от новых пользователей стоит относиться с подозрением и необходимо исследовать информацию о пользователе до того, как авторизовать его. О попытках обмана стоит сообщать в соответствующие инстанции. Не отвечайте на «письма счастья» и другие провокации неизвестных пользователей.

4. Заключение:

Службы мгновенных сообщений - очень эффективный и удобный способ общения, так как сообщения достигают адресата крайне быстро.

Существует несколько правил, которым стоит следовать при использовании IM:

- никогда не отправляйте незашифрованную важную информацию (ведь по умолчанию ваши сообщения отправляются в незашифрованном виде);
- никогда не запускайте исполняемые файлы, полученные из неизвестных или сомнительных источников;
- используйте антивирус и брандмауэр для защиты от распространяющихся угроз и сетевых вторжений и подозрительно относитесь к ссылкам, присылаемым вашими контактами.