Коммуникативные аспекты информационной безопасности

Цифровая репутация

Старая пословица гласит «Написанное пером, не вырубишь и топором». В Интернете эта пословица получила название «Цифровая репутация».

Цифровая репутация - это негативная или позитивная информация в сети «Интернет» о пользователе.

Компрометирующая информация, размещенная в интернете, может серьезным образом отразиться на реальной жизни. К такой информации можно отнести место жительства, учебы, финансовое положение, особенности характера и рассказы о близких - все это накапливается в сети. "Цифровая репутация" - это имидж, который формируется из информации в интернете.

Многие молодые люди легкомысленно относятся к публикации личной информации в Интернете, не понимая возможных последствий:

- Уже сегодня существуют программы и сервисы, которые анализируют интересы, записи на стене, увлечения, высказывания, фотографии и другие данные, опубликованные потенциальными кандидатами на работу. В случаях несоответствия описания кандидата результатам, работодатели отказывают в работе.
- Имеются неоднократные примеры, когда за некорректные комментарии или фотографии уволены стюардессы, учителя, госслужащие, сотрудники крупных компаний.

Комментарии, размещенная информация и действия пользователя в сети «Интернет» не исчезают после их удаления самим пользователем – они сохраняются в поисковых системах и других сайтах, на которых любой желающий может с ними ознакомится, в том числе с намерением причинить вред.

Например, при отправке кому-либо фотографии:

- Ее могут переслать дальше или показать кому-нибудь еще.
- Ее могут разместить в интернете.
- Ее могут увидеть одноклассники, учителя, родители, совершенно чужие люди.
- Ее могут комментировать незнакомые люди, в частности присылать оскорбительные комментарии, подвергнуть унижению и террору и даже звонить.
- Ее могут увидеть ваши дети, ваш партнёр, работодатель, коллеги по работе или учебе в будущем.

Кроме этого, публикуя фотографии или другие медиафайлы, на которых вы или ваши друзья показаны не в очень выгодном свете, вы можете испортить репутацию не только себе, но и знакомым.

Необходимо помнить, что действия и слова пользователя в интернете могут повлечь за собой критику как обычных пользователей, так и киберхулиганов.

Отправляя какую-либо информацию незнакомым людям, например, участвуя в каких-либо обсуждениях в комментариях, на форумах и беседах,

можно сформировать негативное отношение к себе со стороны других людей, в частности у них может появится желание мести.

Так можно пожалеть о размещении комментария в виде замечания в группе новостей по отношению к человеку и, удалив его, крайне удивиться, что этот комментарий уже прочитан десятками или сотнями людей и столько же людей перенаправили его по разным адресам, а в адрес пользователя поступают угрозы, и он заблокирован сайтом или администрацией данной группы в социальной сети.

Для защиты своей информации в социальных сетях пользователи могут самостоятельно настроить свои настройки приватности, например, ограничив доступ к некоторой или всей информации на своем аккаунте для всех зарегистрированных и незарегистрированных пользователей, для своих друзей и подписчиков или к отдельной группе пользователей.

Основные советы по защите цифровой репутации:

- Перед публикацией любой информации, например, публикацией фотографии или осуществлении любого действия, например, комментирования какого-либо поста в сети «Интернет» необходимо подумать о возможных последствиях и защите себя и близких сейчас и в будущем;
- Установить в настройках профиля ограничения на просмотр профайла и его содержимого;
- Нельзя размещать и указывать информацию, которая может кого-либо оскорбить, обидеть или унизить.
- Сетевой этикет. Кибербуллинг
- В ходе сетевого общения необходимо придерживаться следующих правил поведения:
- Помнить о том, что ведется диалог с человеком и не забывать об эмоциональной сфере. В ходе дискуссии можно очень легко ошибиться в толковании слов собеседника, забыв, что собеседник имеет чувства, привычки, позицию и мировоззрение.
- Необходимо следить за формулировками и используемой лексикой, избегать жаргонной и ненормативной лексики и соблюдать правила орфографии и пунктуации, поскольку любая информация может быть включена в новый контекст и поменять смысл.
- Необходимо правильно выбирать модель поведения, ведь принимаемая в одном месте, она может быть неприемлема в другом. Оказавшись на новом сайте, в группе или новом блоге, сначала необходимо ознакомиться с правилами и прочитать, как и о чем говорят участники дискуссии, узнать методы и форматы общения и только после этого вступать в дискуссию. Также общение с друзьями может включать в себя некую расслабленность, но в коммуникации с коллегами, начальством или другими лицами - это не допускается.

- Проверять достоверность фактов и информации перед публикацией. Недостоверная информация способна вызвать негативную оценку со стороны собеседников.
- Необходимо обратить внимание на логичность текста, который должен быть выстроен так, чтобы в нем не было ни одной «логической дыры» и обобщений, чем могут воспользоваться для опровержения собеседники.
- Нельзя распространять личные данные, позволяющие идентифицировать пользователя, поскольку в реальной жизни его могут найти для причинения вреда его здоровью, а в сети невозможно быть абсолютно уверенным в том, что собеседник - это тот человек, за которого он себя выдает.
- Помнить об отсутствии анонимности в сети и действии законов в сетевом пространстве. Выдавая себя за кого-то другого, оскорбляя и запугивая других пользователей, распространяя запрещенную информацию и осуществляя другие действия, незаконные или запрещенные администрацией сайта или сервиса, помнить о том, что администрация сайта или сервиса и правоохранительные органы могут определить любого пользователя по его IP-адресу.

При ответе на замечания в сети «Интернет» необходимо придерживаться следующих правил:

- избегать открытого противоречия;
- сохранять спокойный, доброжелательный тон;
- с уважением относиться к позиции собеседника;
- подчеркивать позитивные моменты, признавать правоту собеседника;
- быть лаконичным.

Однако в сети «Интернете» пользователь может стать жертвой издевательств, хулиганства и бойкота, а также преследоваться сообщениями, содержащими оскорбления, агрессию и запугивание. Такие действия имеют общее название – это **кибербуллинг** или виртуальное издевательство.

Английское слово буллинг (bullying, от bully – драчун, задира, грубиян, насильник) обозначает запугивание, унижение, травлю, физический или психологический террор, направленный на то, чтобы вызвать у другого страх и тем самым подчинить его себе.

Зачастую кибербуллинг рассматривается специалистами как социальное давление, перенесенное в плоскость электронного общения путем использования электронной почты, социальных сетей, смс-сообщений, мессенджеров и других средств коммуникации в Интернете.

Независимо от формы проявления кибербуллинг может причинить значительный вред жертве, а в крайних случаях привести к самым трагическим последствиям.

Обычно выделяют следующие виды кибербуллинга:

- Оскорбление происходит посредством оскорбительных комментариев и вульгарных обращений, происходящих в публичном пространстве интернета;

- Домогательство от незнакомцев, адресованное конкретно пользователю;
- Клевета путем выставления жертв в неблагоприятном свете с помощью различных материалов или информацией;
- Использование фиктивного имени, когда кто-то выдает себя за другого человека, используя пароль жертвы, либо создает поддельную страницу на ее имя, где размещает лживый и унизительный контент или отправляет различные сообщения друзьям и знакомым жертвы негативного характера для ухудшения отношения к жертве.
- Публичное разглашение личной информации осуществляется путем распространения личной информации для шантажа или оскорбления жертвы.

Чтобы противостоять кибербуллингу, необходимо следовать ряду правил.

Одноразовые оскорбительные сообщения лучше игнорировать, поскольку обычно агрессия прекращается на начальной стадии.

В случае их продолжения, в том числе регулярного, необходимо игнорировать такие сообщения и не стоит угрожать хулигану «найти и наказать». Это лишь спровоцирует хулигана на продолжение конфликта и социального давления, что усугубит ситуацию.

Неоднократно в практике имеются случаи, когда киберхулиганы могут специально создавать поводы, заставляя сердиться свою жертву до такой степени, что она рано или поздно отвечает разгневанным или оскорбительным замечанием. После такой реакции киберхулиган уведомляет администраторов сайта или сервиса о недопустимом содержимом и нарушении правил пользования услугами сети, после чего аккаунт жертвы блокируется.

Следующим этапом является бан или внесение в черный список агрессора, функция которого предусмотрена во всех сервисах, имеющих функцию общения. В программах обмена мгновенными сообщениями есть возможность блокировки отправки сообщений с определенных адресов, а для смс-сообщений для этого достаточно обратиться по телефону в службу поддержки оператора.

Пользователь также имеет возможность заблокировать самого хулигана, обратившись с жалобой в адрес администрации сайта, потребовав применить санкции в отношении обидчика и даже удаление его аккаунта. Жалобу необходимо сопроводить скопированной или сохраненной информацией фактов поступивших сообщений, в частности угроз.

При наличии угроз жизни и здоровью кибербулинг может перейти в реальную жизнь, вместе с подтверждениями можно обратиться в правоохранительные органы для защиты пользователя и его близких, действия обидчиков могут попадать под статьи действия Уголовного кодекса и Кодекса об административных правонарушениях Российской Федерации.

Если же пользователь стал свидетелем кибербуллинга, то ему необходимо:

- выступить против преследователя или хулиганов, указав на правовые последствия данных действий;
- поддержать жертву, которой нужна психологическая помощь;
- сообщить администрации сайта или сервиса о случившемся с просьбой предпринять соответствующие меры.

Технологии информационного воздействия

В идеологическом противоборстве большое место занимают технологии информационно-психологического воздействия (манипулирования).

Технология в современной коммуникативной науке – это совокупность приемов, методов и средств, используемых для достижения конкретных целей, в частности для осуществления деятельности на основе рационального ее «расчленения» на процедуры и операции с их последующей координацией, синхронизацией и выбором оптимальных средств и методов их выполнения.

Технологии информационно-психологического воздействия в массовых информационных процессах базируются на использовании возможностей для воздействия на массовое и индивидуальное сознание аудитории и молодежи в частности.

Организации, группы лиц и отдельные лица в сети «Интернет» зачастую используют в своем арсенале воздействия на личность самые разные средства – от способствующих процессу формирования террористических позиций, так и вызывающих реакции страха, неуверенности, психологической напряженности. Эти технологии применяются в качестве средства разрушения политической стабильности в обществе, а также формирования террористической идеологии.

Основные технологии воздействия на общественное сознание через Интернет

- Манипулирование истинной информацией.
- Тенденциозный подбор тем и материалов.
- Эмоциональное комментирование, представление происходящего.
- Технология влияния на деформацию образов, внедрение в общественное сознание элементов нестабильности, дезорганизованности, хаоса, неуверенности и страха.
- Использование контента как канала доведения до населения дезинформации.
- Технологии манипуляции с опросами общественного мнения.
- «Эффект CNN» (тенденциозное представление информации).
- Эксплуатация всевозможных слухов, которые могут целенаправленно влиять на информационно-психологический климат в обществе.
- Использование контента как инструмента непосредственного доведения до отдельной личности, общества и органов государственной власти угроз, ультиматумов, «импульсов» диктата и устрашения.

Рассмотрим некоторые технологии более подробно.

Технология «манипулирования с истинной информацией» является одной из наиболее широко распространенных технологий информационно-

психологического воздействия на общественное сознание. Так, организованное блокирование части информации или запрет на выражение точки зрения противоположной стороны при акцентировании политически выгодных тем может вызвать у пользователей реакцию, которая будет неадекватной происходящим в действительности событиям.

Технология влияния контента на деформацию архетипических образов – одна из технологий для воздействия на общественное сознание, посредством которой осуществляется внедрение в общественное сознание элементов нестабильности, дезорганизованности, хаоса, неуверенности и страха. Эта технология состоит в воздействии на стереотипы, установки, сложившиеся у населения конкретной страны, в вытеснении из общественного сознания доминирующей национальной идеи, объединяющего морального начала и рассчитана на реализацию в долгосрочном, стратегическом плане.

«Эффект CNN» – одна из технологий для воздействия на общественное сознание через СМИ, заключается в демонстрации потрясающих психику аудитории актуальных событий в реальном масштабе времени. Благодаря эффекту «присутствия» пользователя в гуще событий (например, при бомбардировках городов) достигается эмоциональное усиление оказываемого на аудиторию психологического воздействия, которое закрепляется нацеленным комментарием.

В политических процессах активно используются манипулятивные технологии. Все политические технологии манипулирования поведением человека действуют в ограниченном временном и функциональном диапазоне. Степень их эффективности определяется духовной зрелостью людей, их готовностью обманываться. Глубинной основой политических манипулятивных технологий является конструирование мифов, обращение не к разуму человека, а к глубинам подсознания. Люди позволяют собой манипулировать, сбрасывая ответственность за свои поступки на так называемых манипуляторов. Метод политических мифов – направлен на изменение основы ориентации человека, в качестве которой служит складывающаяся в мозгу определенная картина мира, с которой сравниваются явления, наблюдаемые в окружающей среде. Изменение картины мира может происходить внедрением в сознание политических мифов, позволяющих заменить целостное мировоззрение фрагментарным, изменить объективную картину мира, приводя к неадекватному искаженному пониманию реальности, своего рода психическим сдвигам.

Примеры технологий воздействия, которые могут влиять на ценностные установки пользователей Интернета:

- Анонимный авторитет – излюбленный прием введения в заблуждение, активно используемый в различных группах. Одним из самых эффективных методов влияния является обращение к авторитету, который может быть религиозным или политическим деятелем, ученым или представителем другой профессии.
- «Будничный рассказ» – «будничное» или «обыденное» изложение информации используется, например, для адаптации человека к

информации явно негативного, вызывающего отрицание, содержания. Предполагается, что пользователь, многократно сталкиваясь с информацией такого рода, перестает реагировать на самые чудовищные преступления и массовые убийства, происходящие в обществе. Наступает психологический эффект привыкания.

- «Забалтывание» – метод используется, когда необходимо снизить актуальность или вызвать негативную реакцию к какому-либо явлению. Метод «забалтывания» нередко применяется для создания «информационного шума», когда нужно скрыть какое-то важное событие или главную проблему, в его основе лежит эффект размытия внимания, за счет большого объема текста с малой информационной нагрузкой.
- Эмоциональный резонанс – данную технику определяют как способ создания у пользователей определенного настроения с одновременной передачей пропагандистской информации. Эмоциональный резонанс позволяет снять психологическую защиту, которую на мыслительном уровне выстраивает человек, сознательно пытаясь оградиться от пропагандистского или рекламного «промывания мозгов».
- Эффект бумеранга – организация тотальной травли своего оппонента, она приводит к тому, что в итоге он начинает вызывать жалость и симпатию у широкой аудитории.
- Эффект ореола – базируется на коварном психологическом свойстве – человеческой склонности мыслить «ложными аналогиями» и состоит из двух распространенных стереотипов–заблуждений: 1. «Рядом – значит вместе». Вследствие этого феномена нахождение рядом со знаменитым или высокопоставленным человеком несколько повышает статус в глазах окружающих. 2. Второй стереотип – человека, добившегося весомых успехов в какой-то конкретной области, окружающие считают способным на большее и в других делах.
- Эффект первичности – в современной пропаганде существует принцип: человек, сказавший миру первое слово, всегда прав. Здесь срабатывает один из эффектов восприятия: мы склонны отдавать предпочтение той информации, что поступила первой. Изменить уже сформировавшееся мнение очень трудно.
- Информационная блокада – замалчивание или заведомо искаженное описание происходящего.

Инструменты коммуникации: электронная почта, социальные сети и мессенджеры

Электронная почта - это технология и предоставляемые ею услуги по пересылке и получению электронных сообщений, которые распределяются в компьютерной сети.

Обычно электронный почтовый ящик выглядит следующим образом: имя пользователя @имя домена. Также кроме передачи простого текста, имеется возможность передавать файлы.

В первую очередь необходимо выбрать правильный сервис электронной почты. Рекомендуется использовать бесплатные почтовые сервисы, которые представлены на рынке достаточно долгое время и соответствуют следующим условиям:

- Имеют авторизацию через защищенное соединение https;
- Имеют двухэтапную авторизацию;
- Имеют функцию «Секретного вопроса»;
- Имеют функцию отключения рекламы в профайле;
- Имеют возможность привязать к аккаунту номер мобильного телефона;
- Имеют функцию защиты от спама и проверки сообщений, приходящих на почту, на предмет наличия вирусного программного обеспечения.

На следующем этапе необходимо правильно выбрать адрес электронной почты - почтовый адрес должен быть удобен в произнесении и понятен.

В названии своего ящика можно использовать реальные имя и фамилию, что позволит облегчить связь с пользователем, однако в названии почты не стоит употреблять посторонние слова, т.к. это может скомпрометировать пользователя. Например, если пользователя зовут Екатерина Иванова, то ее почтовый ящик следует назвать KateIvanova или EkaterinaIvanova, если такие почтовые ящики уже существуют, то следует добавить год рождения или две последние цифры (KateIvanova76 или EkaterinaIvanova1976). Неправильным примером может стать электронная почта с названием «Kotenok1976».

Вместе с тем специалисты рекомендуют:

- Не указывать в личной почте личную информацию, например, лучше выбрать "музыкальный_фанат@" или "рок2013" вместо "Коля2012"
- Использовать несколько почтовых ящиков: первый для частной переписки с адресатами, к которым имеется доверие, и второй для регистрации на форумах и сайтах.
- Не рекомендуется использовать для регистрации на важных сайтах сервисы, предоставляющие адрес электронной почты на время, поскольку в дальнейшем восстановить доступ к такой почте будет невозможно.
- После получения адреса электронной почты можно пройти регистрацию в социальных сетях.

Первоначально социальные сети были созданы для упрощения общения между людьми. В них можно делится своими мыслями, идеями, заводить новые знакомства и поддерживать общение со старыми друзьями.

Теперь страничка в социальных сетях – это не только виртуальное Я человека, но и инструмент формирования имиджа пользователя, поэтому так необходимо внимательно относиться к тому, как она выглядит.

Чтобы обезопасить себя в социальных сетях, пользователю нужно придерживаться различных правил.

Перед регистрацией в социальных сетях необходимо ознакомиться с политикой конфиденциальности, условиями использования и безопасности, а также другими условиями, поскольку данному ресурсу будут предоставлены

не только персональные данные, но и, скорее всего, через него будут осуществляться покупки.

При регистрации необходимо указание реальных имени и фамилии, поскольку в случае утери доступа к аккаунту паспортные данные пользователя смогут стать подтверждением факта принадлежности аккаунта. При публикации аватара необходимо помнить, что использование для этой цели чужой фотографии может привести к блокировке аккаунта со стороны администрации.

При регистрации в новой социальной сети или сервисе обычно запрашивается возможность поиска друзей или коллег по электронной почте, которые уже зарегистрированы на сайте или сервисе. Рекомендуется не раскрывать адреса электронной почты друзей и знакомых, поскольку, используя полученные данные, сайты или сервисы смогут рассылать электронные сообщения от имени пользователя всем пользователям из списка контактов.

При работе в социальной сети в первую очередь необходимо ограничить список друзей. В друзьях любого пользователя не должно быть случайных и незнакомых людей. Мошенники могут создавать фальшивые профили, чтобы получить от пользователя или его друзей информацию.

Публикуя информацию, необходимо помнить о цифровой репутации и не размещать информацию личного характера, которая может быть использована против пользователя: пароли, телефон, адрес, и другую личную информацию, которая позволяет узнать окружение, интересы и виды активности пользователя. Стоит заполнять только обязательные пункты раздела «о себе», которые помечены звездочкой.

В частности, именно через социальные сети злоумышленники ищут данные, которые используются в качестве секретного слова или пароля.

Особенно необходимо обратить внимание на настройки геолокации. Собрав информацию о перемещениях пользователя и его частых местах пребывания, злоумышленники смогут спланировать любое преступление. Кроме этого, лучше избегать размещения фотографий в Интернете, где по местности можно определить местоположение, кроме публичных и туристических мест.

Не стоит афишировать свое финансовое благосостояние: информация о приобретении машины, квартиры и путешествии может послужить мотивацией для грабителей. Примером данной ситуации служит история, когда злоумышленники ограбили квартиру во время отпуска ее хозяев, узнав о планируемом отпуске и его сроках из аккаунта сына в социальной сети.

Данное правило также распространяется на всю публикуемую на странице информацию, в том числе на репосты из публичных страниц либо со страниц своих друзей, добавленные видео и фотографии и список групп и страниц, на которые подписан пользователь.

Таким образом, перед публикацией необходимо проводить внутреннюю модерацию, оценивая уровень уверенности, безопасности и адекватности публикуемой информации.

В этой связи особую актуальность приобретает установка настроек приватности, которые рекомендуется установить на максимальном уровне, предоставив возможность доступа к информации, публикуемой на аккаунте, только друзьям. Рекомендуется также разграничить информацию, которую могут увидеть друзья, коллеги или одноклассники, родители, коллеги, педагоги и другие лица, что позволит не смешивать среди ваших друзей работу/учебу и отдых, а некоторые лица не должны знать все.

Получая от своего друга странное или подозрительное сообщение, нельзя быть уверенным в том, что его аккаунт не был взломан. Также необходимо относиться с осторожностью к приглашениям зарегистрироваться в той или иной социальной сети, вступить в какое-либо сообщество, скачать файл, проверяя ведет ли присланная ссылка на безопасный сайт или страницу. Рекомендуется оперативно связаться с отправителем альтернативным способом, например, по телефону, чтобы убедиться в том, что именно этот человек отправил вам данное сообщение.

Многие социальные сервисы предоставляют возможность использования внутри социальной сети различные приложения, в том числе игры, а авторизацию через социальную сеть использовать при посещении других сайтов. Перед использованием такой функции необходимо удостовериться в безопасности данного приложения или сайта, поскольку через данный канал злоумышленникам могут перейти различные личные данные.

Особая категория аккаунтов в социальных сетях – это фейки. Фейки - это поддельные страницы реальных людей с идентичными фотографиями и данными. Чаще всего фейковые страницы создают под профайлы известных людей. **Как отличить фейк от оригинала?**

- Фотографии, «вырванные» из других социальных сетей или поисковых сервисов. Многие социальные сети помечают закаченные фотографии своим логотипом либо уменьшают качество фотографии.
- Пустой профайл, на котором не указана подробная личная информация.
- В общении с другими людьми обладатель фейковой страницы обычно пишет общими фразами, никогда не указывает детали.
- От фейковых страниц приходит много спама, так как многие мошенники создают такие странички для накрутки голосов или приглашения людей на свои сайты или группы.
- Если указана школа/университет и год окончания, то проверьте, есть ли в друзьях у данного аккаунта пользователи, указавшие данную школу или вуз. Зачастую фейковые аккаунты создают и раскручивают аккаунт в короткие сроки, а фотографии загружают в одно время.

В конце отметим, что необходимо помнить, что быть и казаться – разные понятия. То, что демонстрируется в социальных сетях, не всегда соответствует реальности.

Вместе с социальными сетями многие пользователи используют различные мессенджеры для общения, однако в большинстве мессенджеров

можно не только обмениваться текстовыми и фото сообщениями, но и звонить, подписываться на информационные каналы, общаться в чатах, осуществлять покупки и другие действия.

Как и в социальных сетях, сервисах почт и мессенджерах вопросы сохранения пользовательских данных от коммерческого использования крайне актуальны. Так некоторые сервисы используют полученные данные и продают третьим лицам и рекламодателям, чтобы обеспечить персонализированную рекламу товара или услуги, которой пользователь интересовался или даже обсуждал с другими пользователями.

Необходимо учитывать данный вопрос при выборе сервиса, в частности многие мессенджеры предоставляют функцию сквозного шифрования, предполагающую возможность прочтения текста только отправителем и получателем, и предполагают удаление сообщений и другого контента с серверов после отправления.

Многие мессенджеры предоставляют возможность самоуничтожения сообщений после получения их адресатом. Сообщение будет удалено как на устройстве пользователя, так и устройстве получателя, что позволяет обеспечить безопасность переписки и сохранение личных данных.

Источник: единыйурок.рф