Основные социальные информационные технологии со скрытой целью

Социальные информационные технологии – это технологии, объектом которых являются отдельный человек, социальные группы или целые общества. Применение этих технологий ставит своей целью формирование у людей заранее заданных качеств.

Если последовательность действий в определенных условиях гарантирует получение заданного результата, можно говорить о *социальной информационной технологии*

Социальные информационные технологии в информационном обществе становятся главными рычагами управления людьми. Они постепенно заменили физические воздействия, которые долгое время считались единственным и непременным орудием управления.

В современном информационном обществе информация – это не только и не столько сведения, сколько инструмент управления.

Реклама.

Очень часто реклама выступает информационной технологией со скрытой целью. В рекламе всегда акцентируется внимание на привлекательных сторонах рекламируемого товара, в то же время ничего не говорится о возможном вреде, который он может принести. В этом, в частности, проявляется несоответствие рекламы реальному положению вещей.

Социальные сети.

На данный момент социальные сети по сути являются огромной неплохо структурированной базой данных с самой разнообразной информацией о сотнях миллионов людей по всему миру Чем больше человек общается в разнообразных социальных сетях, тем больше информации о нем можно собрать без каких-либо трудов. Современные социальные сети предлагают пользователям указать практически все о себе: фото; видео; связи (в том числе и по типам); интересы; образование; информацию о работе; места, в которых бывает человек; предпочитаемые продукты; личные мысли и т.д.

Доступ ко всей личной информации есть у довольно большой группы людей, и они могут в любой момент её просматривать, даже, если человек удалил что-то из сети.

Во-первых, это сотрудники самой социальной сети: у них есть доступ к базам данных, в которых содержится вся информация, а также специальные инструменты входа в аккаунты пользователей, как, например, специальный мастер-пароль в Facebook, который позволяет войти в любой аккаунт.

Во-вторых, доступ к информации также имеют правоохранительные органы, такие как ЦРУ в США или ФСБ в России. *Не так давно известный разоблачитель Джулиан Ассандж, основатель Wikileaks, заявил, что Facebook имеет специальный интерфейс, который использует разведка США, а в России ранее популярная сеть ВКонтакте уже успела публично признать факты сотрудничества с правоохранительными органами и передачи личных данных.*

«70% информации спецслужбы собирают из открытых источников»,

1. утечка личных данных по вине сети;
2. взлом отдельных аккаунтов должностных лиц определенной компании в целях промышленного шпионажа до личных целей (личная переписка);
3. получение доступа ко всей личной информации отдельного пользователя;
4. вирусы и фишинг, которые могут незаметно для пользователя воровать логины и пароли и после использовать их для незаконных действий;
5. наличие информации о себе в широком доступе – не всегда положительный момент. Такого рода информация может обернуться и против вас;
6. информационными ресурсами социальных сайтов начинают пользоваться кредиторы для поиска информации о своих должниках;
7. к услугам социальных сайтов стали прибегать и работодатели при приеме на работу кандидатов. Проверка сведения о вашей учебе, отзывы о своей профессии и о прежних работодателях (нет ли там негатива);
8. создание во всемирной паутине социальных сайтов от имени другого лица.

Интернет зависимость

Интернет-зависимость – это уже давно признанное психологическое заболевание, а зависимость от социальных сетей - её новая форма.

Причины этого явления вполне объяснимы: у каждого человека есть явные и скрытые потребности, которые он стремится удовлетворить, это может быть потребность в общении, самореализации, экономии времени или еще чего-то, а социальная сеть дает ощущение удовлетворения этих потребностей И все это кажется очень доступным, стоит написать красивую цитату и тебе отвечают 10 человек; стоит загрузить новое фото и тебе скажут 10 человек, какой ты красивый; стоит сделать пару кликов и в друзьях уже новый интересный знакомый… Однако по сути это уход от реальности, подмена реального на виртуальное, которое только дает ощущение удовлетворения потребностей, а на самом деле Интернет не может заменить реальной жизни Подобная зависимость постепенно развивается у многих людей, которые единожды попали в социальную сеть Человек «подсаживается на сеть», и чем больше времени он ею пользуется, тем сложнее ему жить реальной жизнью.

Киберэкстремизм

Социальная сеть является источником продвижения киберэкстремизма. Вербовка последователей и продвижение своих идей в широкие массы. И новые информационные технологии дают для этого благодатную почву – **блоги, твиттер, социальные сети, сайты, форумы, развлекательные порталы** и прочее. Наиболее «продвинутые» идеологи радикализма научились маскировать свои воззрения под юмор, развлечения, шутки.

Неопытный пользователь «развлекаясь» незаметно для себя впитывает такие идеи, проникается ими, распространяет и становится их сторонником. На наш взгляд, наиболее опасным источником продвижения киберэкстремизма является социальная сеть, а точнее – система «одобрения» – «лайк и перепост». Суть этой системы в том, что пользователь социальной сети, встречая понравившуюся цитату или картинку «репостит» (публикует на своей странице) или «лайкает» (то есть одобряет) ее, тем самым, распространяя ее по своим друзьям и подписчикам. Часто бывает сложно остановить лавину информации, распространяемой таким способом, особенно, если информация содержит в себе остросоциальную проблему. Даже если администраторы ресурса оперативно отреагировали и удалили или заблокировали данный контент – он уже нашел своих читателей и обосновался на их страницах и в их мыслях. Таким образом, как показывает практика, зачастую пользователь Интернета, ставя «лайк» или размещая у себя на странице или в блоге картинку, фото или высказывание – не имеет понятия о том, что эта информация может относиться к экстремисткой.

Основные способы Интернет-мошенничества.

Сайты download-тематики

Самые частые источники вирусов и нежелательных программ. Готовые домашние задания, рефераты, драйверы или музыку с фильмами часто сопровождает специальная. «обертка» – скрытая программа, которая незаметно запускается на вашем компьютере.

*Чем опасно**:***

- можно «поймать» вирус-вымогатель
- Ваш компьютер может стать частью ботнета – в том числе через него злоумышленники будут проводить кибер-атаки.

Фишинг через сайты-подделки

Злоумышленники получают логины и пароли от Ваших аккаунтов. Бывают сайты-клоны банковских страничек или платежных систем. Тут мошенники охотятся за Вашими сбережениями.

Чем опасно:

- теряете деньги;
- теряете контроль над своим аккаунтом в соцсетях;
- есть риск раскрыть важную информацию о себе

Кликджекинг

Поверх страницы сайта размещают невидимый слой. Пользователь, прокручивая страницу, случайно кликает в любое место страницы, для него в этот момент ничего не происходит. Но на невидимом слое была установлена какая-нибудь поделяшка (кнопка share - Ред.) социальной сети, и своим кликом пользователь полайкал группу этого магазина. Дальше работа менеджера магазина сопоставить лайк и страницу товара, теперь

у него есть ссылка на ваш профиль, а там указан ваш телефон. Вы получаете магический звонок!

Такой агрессивный маркетинг формально не запрещён и широко используется.

Чем опасно:

- Вас агрессивно подталкивают к покупке, используя нечестные методы

Геоспам

Физический адрес магазина, клиники, любой другой компании не соответствует указанному на карте.

Вас уговаривают изменить планы и приехать за услугой по другому адресу.

Чем опасно:

- Вас изначально вводят в заблуждение – это первый признак того, что и сама учлуга будет оказана недобросовестно.

Способы защиты от названных видов информационных угроз.

1. Установите антивирус. *В Яндексе вы можете найти бесплатные версии популярных антивирусов, которые хорошо справляются с подавляющим большинством интернет-угроз*.
2. Не скачивайте ничего с подозрительных сайтов низкого качества.
3. Не игнорируйте предупреждениями поисковых компаний об угрозах. *Поисковые помпании проверяют сайты на безопасность.*
4. Никогда не заходите в соцсети или банковские кабинеты через ссылки с чужих сайтов. *Лучше каждый раз пользоваться поиском или закладками в браузере, которые вы сделали сами.*
5. Обращайте внимание на то, как написан адрес подозрительного сайта. *Вместо настоящего sberbank.ru может быть sberlbank или sberbonk. Разница минимальна, но ее нетрудно заметить.*
6. Не реагируйте на «желтую» рекламу. *За баннерами не бывает полезной информации.*
7. Не оставляйте номер своего телефона в открытом доступе в социальных сетях.
8. Необходима подготовка молодежи к жизни, работе, саморазвитию в виртуальном мире без опасения быть вовлеченным в негативную или преступную деятельность. В контексте этой задачи, помимо обязательного минимума знаний по основам информатики и ИКТ, должны преподаваться базовые знания в области предупреждения возможного вовлечения в киберэкстремисткую деятельность:
    - виды экстремизма и киберэкстремизма, их особенности, признаки и истоки;
    - особенности проявления киберэкстремизма в ИКТ-среде, особенно в молодежной;
    - законодательные, нормативные, правовые, этические, моральные нормы работы в сфере ИКТ, нормы информационной этики и права;
    - механизмы защиты от манипулятивных технологий, обеспечение личной безопасности в ИКТ-сфере.