ВЫ УВЕРЕНЫ В СВОЕЙ КИБЕРБЕЗОПАСНОСТИ?

Понятие кибербезопасность было сформулировано относительно недавно. Оно включает в себя борьбу с вирусами, спамом, удаленным взломом и утечкой данных. Но сегодня мир вышел далеко за пределы этого понятия. К киберугрозам относится уже не только незаконное вредоносное проникновение в информационные системы, но и наполнение смыслами и идеями информационного пространства, которые воздействуют на всех вовлечённых пользователей. Наибольшая угроза идет со стороны внедрения информационных «вирусов» в сознание людей, которые начинают развивать деградационные процессы. Сложность заключается в том, что эти «вирусы» неразличимы человеческим сознанием в современном информационном пространстве, в котором люди воспринимают лишь техническую составляющую — не виден сам механизм формирования общественного мнения и методов работы социальной инженерии.

Основная масса людей, особенно молодёжь сегодня большую часть времени проводят в социальных сетях. Социальные сети мощнейший инструмент вовлечения, через которые у людей формируются образы, смыслы и алгоритмы поведения. Зачастую пользователи распространяют контент, не задумываясь, какой смысл закладывают в той или иной информации.

Сегодня обработкой и анализом данных в режиме «онлайн» занимаются специальные киберцентры, формирующие контент. Они способны вбрасывать и распространять его с огромной скоростью, одновременно воздействуя на миллионы людей. В своей работе центры используют киберботов (роботов), которые занимаются комментированием новостей, троллингом, рассылкой и

прочее. Их действия сложно отличить от действий обычных людей в интернете. Киберботы могут очень быстро развивать любые тематики.
На сегодняшний день одной из ведущих стран в этом вопросе является США, там работает 7 киберцентров, обслуживанием которых занимаются порядка 50 000 киберботов. Формирование общественного мнения происходит за счет массированной подачи информации и бессознательного доверия пользователя к полученным данным. Боты ведут пропаганду через рекламу, комментарии и прочие методы вброса информации, а через мультфильмы, игры, фильмы формируются алгоритмы поведения населения. Многолетняя агрессивно направленная пропаганда американских спецслужб против русских на Украине неизбежно привела к вооруженному конфликту внутри Украины. Продолжение подобной пропаганды на территории России против Украины может привести к военному столкновению России и Украины. Нагнетание негатива в интернет пространстве приводит к тому, что негатив проявляется в жизни.
Следует обратить внимание, что расход бюджета США на кибербезопасность в 2015 году составляет 13 млрд. долл. В проекте бюджета на 2016 год заложено 14 млрд. долл. В 2009 году было создано киберкомандование США – United States Cyber Command, которое состоит из 11 структурных подразделений. Единое киберкомандование по сути выполняет управление над всеми специальными структурами США. Стоит отметить, что подготовка кадров для создания и обеспечения данного процесса является системой и ведется достаточно давно. Ведущими вузами в США по подготовке кадров в этом направлении являются Государственный Университет Дакоты, Военно-морская школа последипломного образования в Калифорнии, Северо-Восточный Университет в Бостоне, Университет Талсы, штат Оклахома check these guys out. Также примером выборки кадров является то, что с 1977 года крупнейшая корпорация IBM, которая вслед за Apple, AT&T и Microsoft стали генеральным спонсором мирового чемпионата по программированию, после которого они приглашают всех финалистов на стажировку.
На современном этапе руководство нашего государства акцентирует особое внимание на вопросах кибербезопасности. Эти вопросы оглашаются не только на внутреполитическом контуре, но и на внешнеполитическом. В мае 2015 года Президент РФ В.В. Путин и Председатель КНР Си Цзиньпин подписали соглашение в области обеспечения международной информационной безопасности. Также на VI Международном Форуме безопасного интернета, который состоялся 12 мая 2015 года в Москве помощник президента И.О.Щеголев в своем выступлении отметил необходимость выработки глобального консенсуса и определения ответственных сил в связи с нарастанием напряженностей в мире, новых угроз, в том числе связанных с киберпространством. Таким образом, на данный момент Россия находится на этапе выработки решений по формированию системы обеспечения информационной безопасности общества. Для сравнения в 2014 году затраты России на обеспечение кибербезопасности совокупно составили порядка 140 млн рублей. Также руководство нашей страны акцентирует внимание в направлении развития собственной технической составляющей для

обеспечения кибернезависимости России. Но самой сложной проблемой на сегодняшний день в сфере кибербезопасности является выявление скрытой социально-культурной угрозы, ведущей к разрушению культурного кода России, а, соответственно, выработке действий по сохранению культуры.

Поэтому на наш взгляд социально-инженерный подход является направлением без которого невозможно обеспечить кибербезопасность общества. В целом он представляет собой внедрение в практическую деятельность системы методик по работе с малыми, средними и большими группами населения, а также индивидуально, для формирования определённых алгоритмов поведения в соответствии с выставленными целями; разработку и внедрение теоретико-методологического и аналитического материала для обеспечения данной деятельности.

Социально-инженерная деятельность в области кибербезопасности подразделяется на два контура, имеющих свою специфику.

Первый контур – внутренний – обеспечивает сохранение культурного кода конкретной культурной группы путём формирования определённого информационного пространства на основе образов, транслирующих заданный культурный код и доступных для любых возрастных и социальных групп данной общности. Он имеет оборонительную специфику – служит для защиты культурной общности от вторжения в её информационное культурное пространство чуждого культурного кода.

Второй контур – внешний – служит для внедрения и распространения культурного кода конкретной общности на территорию другой культурной группы. Его задачи являются разнокачественными и проявляются в:

— симбиотическом взаимодействии различных культурных групп (установлению межкультурного диалога и партнёрства через культурное сотрудничество);

— трансформации культурного кода другой общности (культурное сотрудничество с целью возможности проведения на территории другой культурной группы определённых действий социального, экономического, политического и др. характера в интересах своей культурной общности);

— деструкции культурного кода (культурное сотрудничество вплоть до полного уничтожения культурного кода иной культурной группы).

Нас интересует полномасштабное решение социально-инженерных задач в области кибербезопасности на внутреннем контуре и решение задачи по установлению партнёрских связей и межкультурного диалога с иными культурными группами на внешнем контуре.

Центр СИ является структурой, которая разрабатывает подходы и методики по обеспечению кибербезопасности российского общества и осуществляет экспертные заключения по данным вопросам.

Таким образом, необходимо:

— осуществление широкой просветительской работы с населением по вопросам кибербезопасности и разъяснению методов противодействия современным угрозам, обучение сохранению своего культурного кода;

— формирование системы подготовки кадров в области информационной безопасности;
— создание отечественных экспертных информационно-аналитических центров, которые в состоянии решать вопросы кибербезопасности во всех направлениях.

Информационно-алгоритмическое обеспечение
от Центра СИ