самих ИКТ причину такой дестабилизации, однако они выступают достаточно мощными инструментами ее осуществления, в связи с чем требуется выработка мер противодействия их применению в деструктивных целях.

Считаем, что к числу основных групп мер информационного противодействия использованию ИКТ для дестабилизации общественно-политической обстановки в государстве следует отнести следующие меры:

а) поискового и информационно-аналитического характера – направлены на обнаружение, сбор и анализ данных об информационной деятельности субъектов дестабилизации, выявление их замыслов и направлений деструктивной активности;

б) информационной изоляции и подавления – применяются для подавления или блокирования каналов коммуникации, используемых для дестабилизации, а также ограничения распространения через них деструктивной информации либо доступа к ней пользователей;

в) информационного реагирования и контрпропаганды – направлены на нейтрализацию враждебной пропаганды, разоблачение и дискредитацию в общественном сознании субъектов дестабилизации, на донесение до общества информации об истинном положении дел;

г) информационно-пропагандистского, обучающего и воспитательного воздействия – имеют долговременный характер и направлены на формирование «информационного иммунитета» населения к враждебной пропаганде и подрывным действиям в области массового сознания.

На наш взгляд, сам термин «противодействие» не должен ориентировать только на ответную реакцию государственных институтов на возникшую угрозу дестабилизации общественно-политической обстановки в стране. Полагаем, что основой стратегии деятельности государства в борьбе с данной угрозой должны быть наступательность и действия на опережение. Только так можно избежать стремительного развития событий по негативному сценарию в новом цифровом мире с присущими ему сверхвысокими скоростями передачи и распространения массовой информации.

1. Сунь-цзы. Искусство стратегии. М. : Эксмо ; Спб. : Мирград, 2007. 528 с.

2. Зенгер Х. фон. Стратагемы. О китайском искусстве жить и выживать : в 2 т. М. : Эксмо, 2006. 1024 с.

3. Яровая М. Цифровой Майдан: активисты запускают Twitter-шторм, нацеленный на мировую общественность [Электронный ресурс] // AIN.UA. 27.01.2014. URL: http://ain.ua/2014/01/27/510280 (дата обращения: 24.03.2014).

4. Сундиев И.Ю., Смирнов А.А. Обитаемый остров 2.0 [Электронный ресурс] // Сайт С.П. Курдюмова. URL: http://spkuryumov.ru/networks/obitaemyj-ostrov-2.0 (дата обращения: 26.03.2014).

УДК.343.985

А.Н. Тукало, Е.В. Трахимович

НЕКОТОРЫЕ АКТУАЛЬНЫЕ АСПЕКТЫ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСТНОСТИ СО СТОРОНЫ СОЦИАЛЬНЫХ СЕТЕЙ

В настоящее время социальные сети вытеснили традиционные средства массовой информации с информационного поля. Данный факт давно был осознан владельцами традиционных средств массовой информации и обусловлен тем, что охват одного поста в сообществе, например в социальной сети «ВКонтакте», может превышать совокупный охват аудитории телевидения, радио, газет и пр. (под охватом следует понимать число пользователей, которые увидели записи сообщества. Различают охват подписчиков и полный охват. Полный охват отражает число всех пользователей социальной сети, которые видели записи конкретного сообщества за определенный промежуток времени).

Опасность воздействия социальных сетей возрастает благодаря эффекту спящего (англ. sleepereffect, понятие заимствовано из области шпионажа). Данный эффект был открыт психологом Карлом Ховландом, который возглавлял исследования для американского военного министерства. Суть его – знание об источнике разрушается быстрее, чем приведенные аргументы. Иными словами, мозг относительно быстро забывает о том, откуда поступили сведения (из социальных сетей), но саму по себе информацию так быстро он не забывает. Поэтому информация из недостоверного источника со временем приобретает все бóльшую достоверность. Обесцененный элемент улетучивается из памяти прежде, чем содержание послания начнет забываться. Таким образом, социальные сети превращаются в мощный инструмент пропаганды, а с учетом того, что присутствие государственных органов и средств массовой информации в социальных сетях в Республике Беларусь носит формальный характер, то представляет серьезную угрозу не только информационной безопасности государства, но и его суверенитету. Достаточно вспомнить порядок использования социальных сетей во время событий Евромайдана в Украине, а также то, как они используются сейчас во время боевых действий на территории самопровозглашенной Донецкой Народной Республики. Для этого целесообразно взглянуть на сообщества двух лагерей: так называемого «Правого сектора» и «Сторонников федерализации» или «Антимайдана».

Использование приемов социальной инженерии, а также инструментов социального медиамаркетинга в социальных сетях, позволяет с минимальными материальными и временными затратами удаленно создавать сообщества лиц с отклоняющимся поведением, а также оказывать на них должное информационное воздействие, а в случае необходимости координировать их действия.

Правилами социальных сетей запрещено распространение информации, а также создание сообществ, целью которых является разжигание войны, пропаганда насилия, расового неравенства и т. п. Поэтому открытое продвижение таких сообществ невозможно либо затруднено. Однако возможны иные способы:

1. Деятельность под видом оппозиционных сообществ, которая позволяет осуществлять, с одной стороны, необходимую пропаганду, а с другой стороны, использовать внутренние инструменты социальной сети для расширения аудитории и распространения своих взглядов (таргетинг, ретаргетинг, реклама в сообществах, обмены и т. п.).

2. Продвижение неофициальными («серыми», «черными» методами). Это способ расширения своей целевой аудитории посредством спама в социальных сетях, массовых приглашений в конкретное сообщество, взлома страниц. Цены на данные услуги невелики: за тысячу участников придется выложить от 50 до 150 долларов США (цены зависят от применяемых методов, а также от критериев самой аудитории: страна, город, возраст, пол, интересы и т. п.). С другой стороны, данные операции можно осуществить самостоятельно, приобретая специальное программное обеспечение.

3. Парсинг данных пользователей социальной сети по интересующим критериям с целью привлечения в тематическую группу, а также получения интересующих данных, например номеров телефонов граждан, состоящих в определенном сообществе (возможно, для рассылки через зарубежные сервисы sms-спама, содержащего либо угрозы, либо призывы участвовать в массовых мероприятиях).

Кроме того, в целях информационной пропаганды используется не одно сообщество, а несколько (как правило, не меньше трех). Связано это с тем, что чтобы заставить человека поверить в конкретную информацию, необходимо, чтобы он столкнулся с данной информацией не менее трех раз, причем информация должна быть воспринята субъектом, на которого оказывается воздействие, из разных источников.

УДК 34:002

В.К. Фисенко, В.А. Дмитриев,
А.Б. Степанян, Е.П. Максимович

ОСОБЕННОСТИ НОВЫХ ВЕРСИЙ МЕЖДУНАРОДНЫХ СТАНДАРТОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Введением в действие новых версий базовых международных стандартов в области оценки информационной безопасности: ISO/IEC 15408-1:2009, ISO/IEC 15408-2:2008, ISO/IEC 15408-3:2008 и сопутствующих им документов ISO/IEC 18045:2008, ISO/IEC TR 15446:2009 требует адекватного обновления соответствующих национальных стандартов и делает актуальными работы в этом направлении. В докладе обсуждаются основные изменения в этих версиях и их влияние на методологию оценки безопасности информационных технологий.

Общая концепция – оценка безопасности информационных технологий (ИТ) путем проведения активного исследования объекта информационных технологий с целью независимой и достоверной оценки его фактических свойств безопасности сохранилась. Однако методы исследования претерпели ряд существенных изменений и стали более гибкими и предоставляют разработчику и эксперту бóльшую свободу действий.

Концептуальные изменения новой версии ISO/IEC 15408-1,2,3 состоят в следующем:

1) изменился объект оценки (ОО) – теперь это только продукты ИТ (ранее в качестве ОО рассматривались и продукты и системы ИТ. Теперь для продуктов и систем ИТ предполагается использовать разные стандарты);

2) появился новый вид деятельности – оценка составных ОО;

3) изменился подход к оценке таких важных аспектов безопасности, как разбиение на области, самозащита и невозможность обхода политики безопасности;

4) исключены анализ скрытых каналов и оценка стойкости средств безопасности;

5) допускается использование упрощенных профилей защиты (ПЗ) и заданий по безопасности (ЗБ), разработанных по первому уровню гарантии оценки, для которого по сравнению с обычным ЗБ: не требуется приводить описание проблемы безопасности и соответственно определения угроз, политики безопасности, предположений; не обязательно излагать задачи безопасности для ОО, но при этом задачи безопасности для среды функционирования должны быть изложены;