Литература

1. Рязанова Е.А. Денежно-кредитная политика Испании/ Рязанова Е.А. - М.: Русь, 2009. – 56с.
2. Collier Paul: WHY THE COUNTIRES ARE FAILING AND WHAT CAN BE DONE ABOUT IT/ Paul Collier// The Economist. – 2009.-№5.- p.10-12.
3. Официальный сайт Центрального банка Испании [http://www.bde.es/homee.htm]

УДК 351.746:007

ТЕОРЕТИЧЕСКИЕ И ПРАКТИЧЕСКИЕ АСПЕКТЫ ПРОТИВОДЕЙСТВИЯ ИНФОРМАЦИОННОМУ ТЕРРОРИЗМУ В УКРАИНЕ

Володавчик И.А.
Бычкова О. В.

В настоящее время проблема информационного терроризма начинает привлекать все больше внимания в современной науке. Это связано, в первую очередь, с постоянно ускоряющимся техническим прогрессом, нарастающей информатизацией общества и переходом мировой цивилизации в информационную эпоху. Современное общество немыслимо без коммуникаций, вся жизнь среднего европейца, американца, да и уже многих украинцев не возможна без информации. Нарушение работы информационных систем неизбежно влечет за собой потерю чувства реальности, хаос, как общественный, так и экономический упадок.

Сегодня, информация это уже один из основных активов бизнеса. Как известно, кто владеет информацией, тот владеет миром. Именно в период мирового кризиса самым ценным товаром становится информация, которая имеет коммерческую ценность. В руках конкурента такая информация становится самым сильным оружием. Действительно, в постиндустриальном обществе власть знаний и информации становится решающей в управлении обществом, оттесняя на второй план влияние денег и государственного принуждения.

Актуальность выбора темы обосновывается тем, что ближайшее будущее характеризуется неуклонно возрастающей ролью информационной компоненты. Как индустрия, обеспечивающая существование цивилизации, так и вся система общественной безопасности будут находиться в прямой зависимости от информационных систем.

Информационные каналы - это своего рода ключевые артерии современного общества. Поэтому и не удивительно, что именно они могут стать мишенью №1 для международных террористов. Но это лишь первый уровень проблемы. Информация - это ресурс, поэтому второй уровень подразумевает уже не атаку на разрушение, а тонкое использование

информационных потоков с целью направить развитие событий в нужном для себя направлении.

Даже самое мощное государство, которое ранее выдерживало революции, войны, страшные социальные потрясения, может оказаться беззащитным перед лицом новых угроз, порожденных информационной эрой.

Тема информационного терроризма еще пока очень нова, а потому в научной литературе ей уделено мало внимания. Много говорится об информационных технологиях и международном терроризме, но важность совместного их исследования в настоящее время не в полной мере осознана научной общественностью.

Наибольший теоретический материал к настоящему моменту наработан американской РЭНД-корпорацией и ее сотрудниками. Признанными авторитетами в рассматриваемой области являются Джон Аркуилла, Дэвид Ронфельдт и Габриэль Вейман. Среди украинских ученых указанная проблема рассматривается в работах Головченко В.И., Гондюла В.П. и Зернецкой О.В., которые изучают международную информационную безопасность, ее состояние и угрозы [1].

Поэтому, целью данной работы является изучение теоретических и практических аспектов нового социально-политического явления - информационного терроризма, в контексте проблем информационной безопасности как отдельного предприятия, так и всего государства в целом, а также определение мероприятий его противодействию. Отсюда вытекают следующие задачи работы:

- выделить информационный терроризм как самостоятельное явление, определить его природу;
- показать методы и технологии, применяемые террористами;
- проследить общемировые тенденции данного явления;
- выявить наиболее острые проблемы, связанные с информационным терроризмом;
- рассмотреть как непосредственные, так и скрытые угрозы информационной безопасности предприятия и государства.

В различных теоретических разработках под термином «информационный терроризм» понимается:

1) форма негативного воздействия на личность, общество и государство всеми видами информации [2];

2) умышленное применение отдельными лицами, террористическими группами или организациями средств информационного насилия с целью разрушения единого информационного поля, нанесения больших экономических потерь, создания атмосферы истерии в социуме, навязывания определенной линии поведения в процессе принятия решений [3].

Проанализировав различные определения термина, предлагается его уточненное понятие: информационный терроризм – это современное социально-политическое явление, которое включает противоправные действия, направленные на использование базы данных информационной системы

противника с целью нанесения ущерба и угрозы жизненно важным интересам личности, общества и государства.

В связи с этим, основными целями информационного терроризма являются:

- максимальное снижение уровня информационной защищенности объекта воздействия;

- несанкционированный доступ к информационным ресурсам с последующим похищением или искажением;

- формирование и массовое распространение по информационным каналам дезинформации населения.

В становление информационного терроризма свой вклад внесли хакеры. Самыми престижными и интересными объектами для них являются компьютерные сети силовых ведомств (прежде всего Пентагона) и НАСА.

Основоположником движения хакеров-разрушителей можно считать чикагца Герберта Зина, более известного под сетевым псевдонимом (ником) “Сумеречный ястреб”. В 1987 году, будучи 17-летним юношей, он совершил одно из самых опасных вторжений в компьютерные системы министерства обороны США. Был обнаружен лишь после того, как снял копии программного обеспечения, прорвавшись к файлам системы управления ракетами США и базы ВВС «Robbins».

Примеров информационного терроризма множество. В 1990 году группа австралийских хакеров проникла в информационную сеть НАСА, что привело к остановке работы всей системы на 24 часа.

В феврале 1998 года гражданин Израиля Эхуд Тенебаум, известный в хакерском мире под ником «Analyzer», организовал успешное нападение на компьютеры министерства обороны США. Для борьбы с хакером потребовались срочные усилия ФБР, ЦРУ, Агентства национальной безопасности, специальных исследовательских подразделений ВВС США, НАСА, Минюста и Агентства защиты информационных систем, которые провели специальную операцию под кодовым названием «Solar Sunrise» [4].

В январе 2001 года группа хакеров, именующая себя «Pentaguard», провела массовое ”обезличивание” (deface) WEB-сайтов ряда государственных и военных структур США, Великобритании и Австралии. Первые страницы взломанных сайтов были заменены текстами, рекламирующими спиртные напитки, или просто краткими сообщениями типа «Крупнейший в истории человечества массовый взлом военно-правительственных сайтов».

Последствия таких актов могут быть весьма трагичными для социума. Например, сколь крупной ни была система «Card Systems Solutions» (процессинговая служба, с которой работали «Master Card» и «Visa»), пережить падение репутации, связанное с утерей информации о 40 млн. кредитных карт в 2005 году, даже ей оказалось не под силу [2].

По оценке американских экспертов, эффективность информационного терроризма может быть сравнима с применением оружия массового уничтожения. В настоящее время для террористов легко уязвимы практически все компьютерные средства обработки и хранения информации (банковские,

исследовательские, управленческие системы, всевозможные базы персональных данных).

Согласно данным, распространенным в апреле 2000 г. в Вене на «X конгрессе по профилактике преступности», общий доход террористов от компьютерных преступлений составляет 500 млн. долл. в год. Ущерб от их деятельности достигает 3,5 млрд. долл. в год и увеличивается ежегодно на 35%. Средние убытки от одного акта информационного терроризма составляют сумму около 560 тыс. долларов.

Предугадать негативные последствия террористической атаки на информационную сферу представляется практически невозможным, а последствия таких атак могут быть катастрофическими. Американский эксперт Ф. Коэн подсчитал, что десять хакеров со ста тысячами долларов могут на протяжении нескольких недель нанести серьезный ущерб американской информационной структуре, вплоть до ее парализации. Двадцать хакеров с одним миллионом долларов в течение двух недель могут поставить США на колени. А сотни хакеров и тридцати миллионов долларов достаточно для разрушения всей информационной структуры США, после чего понадобится несколько лет для проведения комплекса восстановительных работ.

Основными видами информационного оружия можно считать:

- компьютерные ”вирусы”;
- “логические бомбы” - программные закладные устройства, которые заранее внедряют в информационно-управляющие центры инфраструктуры, чтобы по сигналу или в установленное время привести их в действие;
- различного рода ошибки, сознательно вводимые в программное обеспечение объекта.

Сегодня методы информационного терроризма ориентированы не на разрушение важных стратегических и экономических объектов, а на широкомасштабное нарушение работы финансовых и коммуникационных сетей, частичное разрушение экономической инфраструктуры и навязывание властным структурам своей воли. Деньги - капитал вчерашнего дня, информация - сегодняшнего и завтрашнего.

К примеру, террористический информационный удар по крупному банку способен вызвать системный кризис всей финансовой системы любой развитой страны, так как лишает общество доверия к современным технологиям денежного рынка.

Приостановка глобальных информационных потоков даже на короткое время способна привести к не меньшему кризису, чем разрыв межгосударственных экономических отношений. По заявлениям некоторых иностранных экспертов, отключение компьютерных систем приведет к разорению 20% средних компаний и около 33% банков в течение нескольких часов, соответственно 48% и 50% потерпят крах в течение нескольких суток.

Согласно данным Агентства национальной безопасности, США сильнее других стран зависят от сетевой инфраструктуры: здесь сосредоточено более 40% вычислительных ресурсов мира и около 60% информационных ресурсов

Интернет. Кроме того, в США 90% всей информации, в том числе и важной военной, передается по сетям связи общего пользования типа Интернет [5].

По состоянию на 1 октября 2010 года аудитория украинского Интернета составляет около 12 млн. пользователей. Об этом свидетельствуют данные исследования, проведенного по заказу Украинской ассоциации Интернет-рекламы (УАИР) [6].

С точки зрения национальной безопасности Украины в области информационной безопасности существует опасная тенденция, связанная с увеличением технической и технологической зависимости нашего государства:

- практически не развивается отечественное производство конкурентоспособных средств информатизации и связи;
- информатизация как государственных, так и коммерческих структур осуществляется в основном на базе зарубежной технологии и компьютерной техники;
- отсутствует достаточная государственная поддержка фундаментальных и прикладных отечественных исследований в сфере предупреждения и борьбы с информационной преступностью, что не позволяет нашему государству на равноправной основе включиться в мировую информационную систему [3].

В сфере предоставления финансовых услуг в Украине в течение ряда последних лет, как и во всем мире, также используется новый вид платежных средств - «электронные деньги» на основе применения пластиковых карт (магнитных и смарт-карт). В то же время это создает сложные проблемы, приводит к появлению новых, нетрадиционных для банка угроз, связанных с уязвимостью компьютерной информации, возможностью ее умышленного искажения и совершения экономических компьютерных преступлений.

Примером такой угрозы может быть ситуация с «Проминвестбанком» в сентябре 2008 года, когда слухи о возможном банкротстве банка вызвали панику в рядах его вкладчиков, которые ринулись снимать деньги со своих счетов.

Неопределенные люди утверждали, что «Проминвестбанк» неплатежеспособен, и рекомендовали людям снимать деньги полностью. В результате деньги в банкоматах в шахтерских городах (Торез, Снежное, Шахтерск) закончились в течение 1-1,5 часа. Паника пошла повсеместно, она достигла города Донецка, где появились очереди до 300 человек у банкоматов. Вкладчиками было снято около 180-200 млн. грн. за несколько дней, что составило размер трехнедельного снятия денег.

Для данной ситуации четко подходит термин - “Brain washing” - промывание мозгов. С его помощью осуществляется зомбирование людей, создание пассивного послушного человека, превращение народа в легко управляемую массу.

Помимо ажиотажа у банкоматов, у владельцев пластиковых карт возникли и другие проблемы. Банкоматы некоторых банков отказывали в авторизации карточек «Проминвестбанка» несмотря на то, что это карточки международных платежных систем. Кроме того, в некоторых крупных магазинах продавцы

отказывались принимать карточки для оплаты товаров через терминал, ссылаясь на то, что руководство дало указание приостановить прием к оплате.

Дезинформация, распространенная среди населения о неплатежеспособности «Проминвестбанка», была спланированной акцией, направленной на подрыв имиджа банка. Причина дезинформации состояла в том, что «Проминвестбанк» уже около полугода вел войну с группой мелких акционеров, пытающихся получить контроль над одним из крупнейших банков страны. Эта акция была предпринята с целью доведения до банкротства и выкупа банка за бесценок.

Этот нездоровый ажиотаж возник именно вокруг Донецкого отделения банка, потому что он самый крупный филиал в системе «Проминвестбанка» и те, кто планировал эту акцию, об этом были уведомлены, поэтому решили с меньшими затратами сделать больше шума, ударив по одной области. Это было рассчитано на то, что банк не успеет подкрепиться наличностью и банкоматы будут пустые.

Отток денег был настолько массовым, что заставил Нацбанк Украины экстренно выделить 5 млрд. грн. для спасения банка [7]. Хотя международные рейтинги на то время показывали стабильность банка и признавали его одним из 1000 крупнейших банков в мире и вторым по надежности в Украине.

Кроме того, выйдя на мировой рынок вооружений, Украина еще столкнулась с широко используемым в конкурентной борьбе «черным пиаром». Все эти годы наш ВПК периодически обвиняли в поставках оружия в зоны конфликтов, в страны, на которые распространяется эмбарго международных организаций, в демпинге, «сбивании цен».

Совершенно понятно, что, делая экспорт вооружений одной из важных составляющих внешней торгово-экономической политики, Украине необходим государственный подход в деле контроля над информацией касательно экспорта вооружений и военной техники. Безусловно, подключая разведывательное сообщество и спецслужбы к обеспечению торговли оружием, Украина должна уделять самое большое внимание рекламе и нейтрализации негативной информации. В этом, в том числе, видится залог успешной украинской экспортной политики.

Выполненные теоретические исследования и анализ конкретных ситуаций позволяют сделать вывод, что надежность корпоративных систем украинских предприятий сегодня напрямую зависит как от применяемых технологий защиты, так и от наличия в организации комплексной стратегии в области информационной безопасности. Поэтому для украинских предприятий следует выделить следующие рекомендации по сохранению информации:

1. Правовые меры - включают в себя разработку нормативно-правовых актов, регламентирующих отношения в информационной сфере.

Особое значение имеет тот факт, что в соответствии с рекомендациями Европейского комитета по проблемам преступности Совета Европы на базе Национального центрального бюро Интерпола в Украине создан Национальный центральный консультативный пункт (НЦКП) по проблемам информационной преступности.

Кроме того, разумно было бы разработать и внедрить специальную Концепцию “Минимальной обязательной информационной инфраструктуры” (МОИИ), которая задумана как минимальная инфраструктура информационных систем, процедур, законов и налоговых стимулов, гарантирующих длительное функционирование государства даже в период сложной сетевой атаки [3].

2. Технологические меры, направленные на:

1) разработку, использование и совершенствование средств защиты информации;

2) создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации.

Так, ведущие западные фирмы постоянно наращивают объемы производства по выпуску специальных технических средств защиты входа в служебные помещения (системы кодируемых карточек, биометрические системы, реагирующие на голос, отпечатки пальцев, узоры кровеносных сосудов сетчатки глаза).

3. Административные меры подразумевают создание оптимального режима доступа к информации - перечень работников, имеющих доступ к конфиденциальной информации, должен быть максимально сужен. Кроме того, необходим контроль за действиями персонала в защищенных информационных системах, подготовка кадров в области обеспечения информационной безопасности.

4. Корпоративные и социально-психологические меры: правильный подбор и расстановка кадров, использование материальных и моральных стимулов для формирования лояльного отношения персонала к компании. Ведь на украинских предприятиях люди, отвечающие за безопасность, часто плохо подготовлены к такой работе, изолированы от важных служб.

Западные специалисты по экономической безопасности считают, что от правильного подбора, расстановки и стимулирования персонала сохранность секретов зависит как минимум на 80% . Для этого агентство информационных систем министерства обороны США в целях проверки провело 38 тысяч “атак” по собственным компьютерным сетям - только 4% персонала, отвечающего за них, поняли, что производится “атака”, и лишь каждый 150-й сообщил в вышестоящую инстанцию о “вторжении”.

Подводя итог рассмотрению проблемы информационного терроризма, можно смело утверждать, что это социально опасное явление не миф, а реальность, как для всего мирового сообщества, так и для нашего государства.

Анализ мировых тенденций развития информационного терроризма с большой долей вероятности позволяет прогнозировать, что его угроза с каждым годом будет возрастать. Дальнейшее развитие НТП, жесткость конкуренции как «войны всех против всех» делают похищение чужой информации особенно прибыльной сферой деятельности.

Поэтому защита национального информационного пространства должна стать приоритетным направлением в осуществлении концепции национальной безопасности современного государства. Все это, в свою очередь, вызывает необходимость активной разработки проблематики информационной

безопасности общества и государства, что невозможно без тщательного рассмотрения нового вида терроризма, рожденного в условиях тотальной глобализации и информатизации.

Литература

1. Головченко В.І., Гондюл В.П., Зернецька О.В. та ін. Міжнародна інформаційна безпека: сучасні виклики та загрози. – К.: Центр вільної преси, 2006. – 915 с.
2. http://www.cio-world.ru
3. www.Crime-reserarch.org
4. http://ataman-off.narod.ru/INDEXx-file.htm
5. Попов М.О., Лукъянец А.Г. Обеспечение военной безопасности в контексте информационной войны // Наука и оборона. - 1999. - №2. - С.39-40.
6. www.biz.liga.net
7. www.24.ua

УДК94(477):376.64

РЯДЯНСЬКА СИСТЕМА ЗАКЛАДІВ ДЛЯ БЕЗПРИТУЛЬНИХ ДІТЕЙ В ДОНЕЦЬКІЙ ГУБЕРНІЇ В 20-ті рр. XX ст.

Волошинова А.В.
Лихачова Л.Б.

В Україні проблема дитячої безпритульності за останні роки значно загострилася. Інтенсивно йде формування дитячого соціального низу зі своєю агресивною субкультурою, чужою для оточуючих. Однак визначене негативне явище не є продуктом сучасності. Воно було і в дореволюційній Україні, існувало й в роки громадянської війни, під час та після закінчення Великої Вітчизняної війни, рецидиви дитячої безпритульності спостерігалися й в 1970 – 1980-ті роки. З часом змінюються причини безпритульності, її кількісний склад, але сутність залишається та ж сама – нікому непотрібні діти живуть на вулиці, порушуючи правові й моральні норми поведінки.

Зараз в Україні налічується більше 160 тисяч дітей у віці 8 - 16 років, які мають потребу у турботі держави, або у прийомних батьках [1]. Лише 20 % з них є біологічними сиротами; усі інші – сироти соціальні. Значне погіршення рівня життя привело до актуалізації проблеми дитячої наркоманії, проституції, бродяжництва. Аналіз реальних кроків, котрі застосовуються органами державної влади по відношенню до захисту прав та інтересів майбутнього покоління показує, що затрачені зусилля в цьому напрямку неможна назвати адекватними. Тому нашій державі поки не вдається впоратися із проблемою безпритульності. Однак керівництво нарешті визнало її величезну значущість і почало вживати певних зусиль для поліпшення ситуації. Так, 11 травня 2006