Противодействие кибертерроризму

Быстрое развитие информационно-коммуникационных технологий и широкое распространение услуг, предоставляемых киберпространством, заставляют задуматься над вопросом: «Как обеспечить безопасность киберпространства?». Все информационные технологии взаимосвязаны друг с другом, и доступ к ним возможен из любой точки мира. В современном кибермире широкий спектр критически важных инфраструктур - от водоснабжения до транспорта, от энергетики до коммуникационных технологий - уязвим для кибератак. Эти инфраструктуры практически не имеют киберзащиты и полагаются на устаревшие традиционные решения в области безопасности. Террористическая кибератака на эти отрасли может привести к экологическим катастрофам, экономическим потерям, утрате имущества или гибели людей. В связи с этим, странам всего мира необходимо подготовиться к возможной кибератаке в любую минуту.

На протяжении нескольких веков страны инвестировали в развитие защиты от классического террористического насилия, но при этом, остаются крайне уязвимыми для кибер-атак на компьютерные сети, которые имеют решающее значение для национальной и экономической безопасности. Растущая сложность и взаимосвязанность этих инфраструктурных систем, а также их зависимость от компьютеров не только делают их более уязвимыми для атак, но и увеличивают потенциальный масштаб последствий атаки. Этот страх побудил правительства направить значительные ресурсы на защиту критически важных национальных инфраструктур.

Чтобы защитить свои жизненно важные интересы, многие технологически зависимые страны концентрируют внимание на организации своей политики кибербезопасности. Большинство из этих стран приняли те или иные национально-правовые и военные меры. Но без международного сотрудничества эти национальные меры бессильны в борьбе с кибертерроризмом.

Существует множество причин, по которым киберпространство является привлекательным выбором для террористических целей. Кибератаки открывают возможности для террористической деятельности с более широкими последствиями. Используя кибератаки, террористы могут нанести гораздо больший ущерб стране, чем физическим насилием.

При традиционной террористической деятельности, такой как взрывы, последствия наступают в пределах конкретных физических мест и сообществ. Большая часть населения выступает лишь в качестве наблюдателей, и они не подвергаются прямому воздействию террористических актов.

Способность кибертеррористической деятельности воздействовать на более широкую часть населения может дать террористическим организациям больше рычагов для достижения своих политических и социальных целей.

Мотивация кибертеррористов проистекает из их политической программы. Их атаки политически мотивированы и направлены на конкретные критически важные системы и инфраструктуры. Эта общая повестка дня объединяет всех хакеров в террористической организации для достижения одной цели. Такие коллективные действия принесут больше вреда, чем действия отдельных хакеров.

Существуют различные причины, по которым кибератаки являются привлекательным выбором для террористов, например;

— Поскольку террористы располагают ограниченным количеством средств, кибер-атаки более заманчивы, поскольку для их осуществления требуется меньше людей и ресурсов (а значит, меньше средств). С другой стороны, они могут быть направлены на большое количество людей и воздействовать на них при том же количестве средств. Другими словами, соотношение выгоды и затрат чрезвычайно высоко.

— Это позволяет террористам оставаться неизвестными, поскольку они могут находиться далеко от физического места, где осуществляется терроризм. Поскольку террористы обычно разбивают лагерь в стране со слабым правительством, кибертеррорист может расположиться где угодно и остаться неизвестным .

— В основном, атаки легко осуществить, потому что многие цели плохо защищены. Поэтому злоумышленники могут выбирать из большого количества целей.

— Когда атака подготовлена, ее можно быстро осуществить без необходимости дальнейшей подготовки.

— Не существует физических барьеров или контрольных пунктов, которые они должны пересечь.

В связи с этим необходимо также выявить, как сайты террористических организаций способствуют совершению терактов. Террористические группы все чаще используют новые информационные технологии (ИТ) и Интернет для того, чтобы создать все необходимые условия для поддержания террористической организации. Как правило это:

— Формирование планов,

— Сбор и отмывание средств,

— Распространения пропаганды,

— Безопасное общение с членами запрещенных организаций (внутреннее общение),

— Обмен информацией и знаниями с аналогичными группами (внешнее общение),

— Командование и управление,

— Проводение исследования и разработки,

— Вербовка новых членов,

— Формирование международной поддержки,

— Сбор разведывательных данных,

— Ведение информационной войны от имени государств.

В дополнение к вышесказанному, Интернет предлагает;

- малое или полное отсутствие регулирования,

- потенциально огромную аудиторию,

- анонимность общения,

- быстрый поток информации [10].

Одним из ярких примеров использования веб-сайтов террористами являются сайты террористической организации Рабочей партии Курдистана - PKK/KONGRA-GEL. Существует 37 различных веб-сайтов, связанных с этой организацией. Эти сайты обычно включают: историю организации, биографии влиятельных людей и убитых террористов, а также информацию о политических целях террористической сети. Содержание этих сайтов направлено на создание и внедрение сепаратизма в общество. Один из веб-сайтов под названием "pajkonline.com" направлен на женщин, которые в прошлом в основном использовались в качестве террористов-смертников. Другой посвящен кибератакам и призывает своих членов изучать методы взлома и предоставляет информацию об уязвимостях компьютерных операционных систем. Этот многомерный пример ярко демонстрирует способы влияния запрещенных организаций, посредством свободного доступа к ним.

До сегодняшнего дня был предпринят ряд шагов как на правительственном, так и на международном уровне. Правительства организуют свою деятельность для противостояния новой угрозе. В некоторых странах созданы группы реагирования на компьютерные чрезвычайные ситуации (CERT) для реагирования на инциденты. США и Великобритания являются ведущими образцами для других стран, составляющих свою политику кибербезопасности. Многие правительства продолжают бороться с проблемой организационной структуры, но некоторые страны смогли успешно сформировать национальную организацию по борьбе с киберугрозами. Например, в Бразилии федеральное правительство в августе 2009 года создало Рабочую группу по информационной безопасности защиты критической инфраструктуры при Департаменте информационной и коммуникационной безопасности. Эта группа работает над планами информационной безопасности и реагирования на инциденты. В Австралии в 2009 году в отчете правительства по вопросам обороны было объявлено о создании национального операционного центра кибербезопасности в рамках Управления военных сигналов. В Турции "Совет по научным и технологическим исследованиям Турции" является организацией-координатором по кибербезопасности. В 2009 году им удалось сформировать национальную политику безопасности киберпространства.