УДК 004.056

А. В. Дудатьєв

ФЕНОМЕН ІНФОРМАЦІЙНОГО ТЕРОРИЗМУ

Вінницький національний технічний університет;

Анотація

Виконано аналіз інформаційного тероризму, як різновиду інформаційного протиборства. Розглянуто моделі інформаційного тероризму. Представлено об'єкти інформаційного тероризму, а також основні компоненти системи протидії терористичним операціям.

Ключові слова: інформаційний тероризм, соціотехнічна система.

Abstract

The analysis of information terrorism as a type of information struggle was carried out. Models of information terrorism are considered. The objects of information terrorism are presented, as well as the main components of the system of countering terrorist operations.

Keywords: information terrorism, sociotechnical system.

Вступ

Потреба ефективного протидії спеціальним інформаційним операціям, що нав'язуються ззовні викликає необхідність створення ефективного «інформаційного управління» що впливає на соціальну частину СТС і запобігає виникненню «керованому хаосу» та загальної дестабілізації суспільства та держави в цілому. Проблема інформаційного тероризму, як одного з різновидів інформаційного тероризму, широко розповсюдилася за останні роки. Ця загроза стає все більш актуальною, оскільки тероризм, особливо інформаційний стає все більш значною загрозою для безпеки, життєдіяльності та інтересів як держави так і населення в цілому. Терористична діяльність в сфері інформації як складне, багатоаспектне і вкрай негативне соціально явище давно переросла межі національних кордонів і перетворилася на масштабну загрозу для безпеки всього людства.

Результати дослідження

Кібертероризм - комплекс незаконних дій у кіберпросторі, що створюють загрозу державній безпеці, особистості та суспільству. Може призвести до псування матеріальних об'єктів, спотворення інформації або інших проблем. Основною метою кібертероризму є вплив на вирішення соціальних, економічних та політичних завдань. У світі швидко зростає кількість «розумних» пристроїв інтернету речей. Всі вони дають ґрунт для цілеспрямованих атак з метою терору або шантажу — тим більше, що зараз велика кількість підприємств використовує такі пристрої в автоматизованих системах управління технологічним процесом (АСУ ТП). Особливо ця проблема актуальна для об'єктів критичної інформаційної інфраструктури. Отримавши несанкціонований доступ до систем управління таких об'єктів, наприклад атомних електростанцій (АЕС), терористи можуть це використовувати для шантажу населення, керівництва держави тощо.

Дії кібертерористів спрямовані на:

1. Нанесення шкоди окремим елементам кіберпростору, руйнування мереж лектроживлення, створення перешкод, використання спеціальних програм що стимулюють вихід з ладу апаратних засобів;
2. Викрадення або знищення програмних, інформаційних та технічних ресурсів в кіберпросторі що мають стратегічне значення, шляхом подолання систем захисту, впровадження вірусів, програмних закладок;
3. Вплив на програмне забезпечення та інформацію з метою їх спотворення або модифікації в інформаційних системах та системах управління;
4. Возкриття та загроза опублікування закритої інформації про функціонування інформаційної інфраструктури держави, суспільно значущих та військових інформаційних систем, кодів шифрування, принципи роботи систем шифрування;
5. Захоплення каналів телекомунікаційного мовлення з метою поширення дезінформації, чуток, демонстрації потужності терористичної організації та оголошення своїх вимог;

6. Знищення та активне придушення ліній зв'язку, неправильна адресація, штучне навантаження вузлів комунікації, вплив на операторів, розробників інформаційних та телекомунікаційних систем з метою вчинення ними перерахованих вище дій.

Мотивом терористичної діяльності як правило є наступні відносини. Якщо R_s – інтегральний ресурс що включає економічний, політичний, інформаційний, екологічний, демографічний та інші ресурси, то $R_s(S) \gg R_s(S_t)$. При цьому інтегральна шкода ресурсу в результаті вірогідного теракту U_s(наявність вразливостей критично важливих об'єктів, взяття яких під контроль терористичною організацією принципово змінить політичну обстановку в S) істотно перевищує витратиU_{S_T} для S_T, тобто $U_S \gg U_{S_T}$. При цьому рівень ризику виникнення теракту для S перевищує допустиму норму в результаті наявності професійних терористичних організацій, необхідних для теракту фінансових, технічних та кадрових ресурсів, що як правило надходять із зовні S_0. В такому випадку відповідна інформаційна обробка соціальної бази терористів (людей що їх підтримують) відкриває перспективи для успішної терористичної діяльності.

На основі аналізу практики протидії тероризму в країнах антитерористичної коаліції можна побудувати типові структурні моделі державних систем що поєднують взаємодіючі структури і міри. Типова державна система організації боротьби з тероризмом включає в себе наступні основні компоненти:

1. Освітлення антитерористичних дій уряду в ЗМІ;
2. Міри по зменшенню впливу пропаганди тероризму;
3. Допомога жертвам терору;
4. Законодавство по боротьбі з тероризмом
5. Охорона критичної інфраструктури
6. Координація антитерористичних дій спеціальних державних органів.

Типові напрямки прийняття мір протидії тероризму включають правові міри, захисні міри, інформаційно-аналітичні міри.

Висновки

Було проаналізовано феномен інформаційного тероризму, як різновиду інформаційного протиборства. Наведено принципи формалізації інформаційного тероризму, а також складові системи протидії деструктивним терористичним інформаційним операціям.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Дудатьєв А.В., Войтович О.П., Миронюк В.В. МОДЕЛЬ ЗАГРОЗ СОЦІОТЕХНІЧНОЇ СИСТЕМИ: СОЦІАЛЬНИЙ АСПЕКТ. Вчені записки ТНУ імені В.І. Вернадського. Серія: технічні науки. 2019. Том 30 (69) ч. 1. С. 97-101.
2. Горбулін В. П., Додонов О. Г., Ланде Д. В. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія. Київ: Інтертехнологія, 2009. 64 с.

Дудатьєв Андрій Веніамінович — к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, email: dudatyev.av@gmail.com

Andriy Dudatyev —PhD (eng), associated professor of information protection department, Vinnytsia National Technical University, Vinnytsia, email: dudatyev.av@gmail.com