зу после смены, мы несем полную ответственность за своих сотрудников! Без начальника (ваш чат, вам решать как работать, но мы всегда рады помочь и подсказать если возникнут вопросы во время работы), график работы есть разный (три смены - утро, день, ночь), зарплата по курсу доллара (Можно получать в гривнах и в долларах зп, как удобно), мощный ПК, качественная камера, комфортная, современная студия.

У нас хороший коллектив, всегда можно пообщаться с девчонками на перерывах. Пишите мне, спрашивайте. Мы ценим ответственных, пунктуальных и жизнерадостных сотрудников) ХАРЬКОВ. ДНЕПР.

Одержано 01.11.2017

УДК 327.84 : 004

Анатолій Анатолійович РУСЕЦЬКИЙ,
кандидат юридичних наук, депутат Харківської обласної ради VII скликання

КІБЕРРОЗВІДКА В ПОЛІТИЧНІЙ ДІЯЛЬНОСТІ

Останнім часом майже усі політичні процеси стають тісно пов'язаними з інформаційним простором та інформаційними технологіями. Таким чином, зараз майже не зустрінеш політичного діяча або політичну партію, які б не мали власного сайту, або акантів в соціальних мережах для висвітлення результатів власної діяльності, програм та звернень до громадян.

Поняття кіберрозвідки необхідно розглядати у двох аспектах: як пошук інформації з відкритих джерел інформації (використання методології пошуку OSINT) та як несанкціоноване збирання інформації (кібершпигунство).

В першому випадку - використання методології пошуку OSINT, яка включає в себе пошук, вибір і збір інформації, отриманої із відкритих джерел і її аналіз. Така діяльність не містить ознак кримінального правопорушення, так як термін «відкритий» вказує на загальнодоступність джерела.

Процес збору інформації з відритих джерел інформації нажаль не врегульовано в національному законодавстві України, проте існує роз'яснення даного права Європейського суду з прав людини.

Таким чином, права на отримання інформації з відкритих джерел глобальної мережі Інтернет роз'яснено Європейським судом з прав людини, який у своїх постановах постійно підкреслює, що стаття 10 (1) Європейської конвенції з прав людини надає право на отримання тільки тієї інформації, яку особа

бажає передати. Виходячи з цього, особа, яка розміщує персональні дані в соціальних мережах, погоджуючись з Політикою конфіденційності такої соціальної мережі, розміщує відомості про себе у відкритому доступі глобальної мережі Інтернет, усвідомлюючи, що такі дані можуть бути використані іншими особами, для її персоніфікації.

Якщо розглядати другий випадок, то дана діяльність передбачає, несанкціоноване отримання будь-якої інформації з метою отримання особистої, економічної, політичної чи військової переваги, здійснюваний з використанням обходу (злому) систем комп'ютерної безпеки, з застосуванням шкідливого програмного забезпечення, включаючи вірусні програми і шпигунських програмне забезпчення . Кібершпигунство може здійснюватися як дистанційно, за допомогою глобальної мережі Інтернет, так і шляхом проникнення в комп'ютери і комп'ютерні мережі підприємств за допомогою працівників-інсайдерів, а також хакерами. В багатьох країнах Європейського союзу на даний час встановлено кримінальну відповідальність саме за кібершпигунство.

Підсумовуючи вищевикладене необхідно зауважити наступне:

1. Політичні діячі повинні забезпечити неперервний процес захисту інформації, яка є досить важливою для забезпечення максимального захисту організації (установи) від внутрішнього і зовнішнього, випадкового і навмисного деструктивного впливу.

2. Привертання уваги персоналу до питань безпеки, додержання персоналом вимог впровадженої в організації (установі) політики безпеки та застосування персоналом у роботі низки методів і дій, необхідних для підвищення захисту інформаційного забезпечення.

3. Введення кримінальної діяльності за ведення кібершпигунства.

Список використаних джерел:

1. Базенков Н. И., Губанов Д. А. Обзор информационных систем анализа социальных сетей. *Управление большими системами*: *сб. трудов*. 2013. № 41. С. 357-394.
2. Присяжнюк М. Жарков Я. Аналіз засобів ведення інформаційної боротьби з використанням інформаційних технологій, форм і способів їх застосування. URL: http://defpol.org.ua/site/index.php/uk/ (дата звернення: 18.10.2017).

Одержано 30.10.2017