Кіберзлочинність як одна із проблем інформаційного суспільства

Циб І.С.
курсант VI курсу факультету підготовки фахівців органів досудового розслідування Дніпропетровського державного університету внутрішніх справ
Краснобрижий І.В.
науковий керівник, к.ю.н., доцент кафедри економічної та інформаційної безпеки, ДДУВС

На сьогоднішній день у світовому просторі дуже бурхливо обговорюється питання інформаційного забезпечення суспільства. Сучасне суспільство досягло дуже високого рівня розвинутості з точки зору поінформованості/інформативності.

У світі налічується дуже багато засобів, способів, а також прийомів отриманої інформації. Вбачається широкий спектр впроваджень інформаційних технологій у всебічних проявах, таких як: державні органи, виробництво, банківська сфера, освіта та наука, а також повсякденне життя людей. Саме дане явище започаткувало так званий феномен інформаційно залежного суспільства, основним джерелом якого є загальновідома мережа «інтернет». Практично всі важливі для громадян служби, пошта та комунальні підприємства на пряму мають певну залежність від надійної роботи комп'ютерних систем, за допомогою яких здійснюється керування цими процесами, а також належне інформаційне забезпечення в цілому.

Тобто, можна вести мову про те, що виникає певна залежність від засобів інформації та зв'язку у світі. Загальновідомим є факт того, що рівень злочинності не тільки на території нашої держави, а й за кордоном зростає з кожним роком, статистика зафіксованих правопорушень збільшується все більше і більше, особливо у галузі «інформаційного забезпечення». Злочинні угрупування також стають більш модернізованими та використовуючи новітні засоби та знаряддя для скоєння злочинів.

Даному питанню присвятили свої наукові праці такі вчені, а саме: О. Бандурка, А. Губанова, О. Долженкова, Є. Желєзов, В. Заросил, В. Золотарева, І. Козаченка, В. Некрасов, В. Ортинський, В. Сапальов, М. Смирнова, М. Стащака, та ін.

Деякі з вище зазначених науковців ще кілька років тому вважали акти негативного впливу через інформаційні технології малоймовірними, особливо в Україні, після подій у грудні 2015 року, коли внаслідок кібератаки на Прикарпаття обленерго без світла залишилися близько 230 000 користувачів, сумніви розвіялися [1]. Указом Президента України від 15 березня 2016 року № 96/2016 з метою створення умов для безпечного функціонування кіберпростору була затверджена «Стратегія кібербезпеки України», у якій прямо зазначено, що сучасні інформаційно-комунікаційні технології можуть використовуватися для здійснення терористичних актів, зокрема шляхом порушення штатних режимів роботи автоматизованих систем керування технологічними процесами на об'єктах критичної інфраструктури [2].

Якщо брати до уваги закордонний досвід, то за кордоном вивчення даної проблеми активно розпочалося після подій 11 вересня 2001 року, коли з'ясувалося, що для організації терористичного акту злочинці користувалися Інтернетом, хоча самої кібератаки не було.

На сьогоднішній день за статистичними даними відомо, що терористи активно використовують інформаційно-комунікаційні технології та Інтернет не тільки для вчинення своїх злочинних намірів, а й для підшукування однодумців, використовуючи переконливі доводи та активно маніпулюючи. Для планування терористичних актів терористи можуть використовувати інформацію як з відкритих джерел, так і конфіденційну інформацію, яка не захищена відповідним чином. При цьому вони висловлюють загрози та обіцяють винагороди з метою залучення фахівців із хакерської спільноти для ефективного виконання ними різноманітних завдань. Для зв'язку між собою терористи можуть використовувати шифрування даних, що значно ускладнює роботу правоохоронців. Ще однією можливістю Інтернету терористи користуються для фінансування своїх операцій. Для цього вони можуть розміщувати різноманітні оголошення в мережі для своїх спонсорів, використовують віртуальні азартні ігри, а під час перерахунку коштів, здобутих злочинним шляхом, широко експлуатують фальшиві інтернет-магазини, які імітують операційну діяльність, проте жодних товарів фактично не продають. Для ефективного захисту від терористичних актів у інформаційному просторі необхідними є прийняття відповідного законодавства, підготовка спеціальних підрозділів по боротьбі з кіберзлочинністю, проведення технічних заходів щодо забезпечення відповідного рівня безпеки інформаційних ресурсів, особливо для об'єктів

критичної інфраструктури. Значним кроком у виконанні цих завдань стала затверджена Указом Президента України від 15 березня 2016 року № 96/2016 «Стратегія кібербезпеки України». Розпорядженням Кабінету Міністрів України від 24 червня 2016 року № 440-р. затверджено План заходів на 2016 рік із реалізації Стратегії кібербезпеки України [3]. Важливим документом для створення відповідної нормативно-правової бази стала постанова Кабінету Міністрів України від 23 серпня 2016 року № 563 «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави».

Питання інформаційного забезпечення поліції є актуальним у світовому просторі. Поліцейські структури різних країн дедалі частіше взаємодіють між собою у службово-бойовій протидії міжнародній злочинності, тероризму тощо. Також поліцейські структури співпрацюють із миротворчими місіями ООН, двосторонні угоди між країнами та багатосторонні договори, укладені міжнародними організаціями, дозволяють поліцейським із різних країн обмінюватися інформацією та накопиченим досвідом, завдяки чому збільшується ефективність службової діяльності. Саме для протидії даному явищу працівникам поліції особливо органам досудового розслідування, суду, прокуратурі необхідно весь час поширювати свій рівень знань та підвищувати кваліфікаційний рівень під час виконання службових обов'язків, здебільшого при роботі з доказовою базою яка зберігається на електронних носіях, або яка передається іншим підрозділам через мережу «Інтернет».

Спираючись на все вище викладене, варто зазначити, що наше суспільство дійсно дуже розвинуте саме з точки зору інформаційності. Інформація є основним джерелом для спілкування, передачі даних та виконання певними службами своїх обов'язків. З урахуванням цього факту, з'явилася нова, модернізована форма злочинності, а саме кіберзлочинність. З даною проблемою зіштовхнулася не тільки наша держава, а й цілий світ. Злочинні угрупування стали більш винахідливими, про що свідчить статистика скоєння злочинів через мережу «Інтернет». З огляду на це, працівникам правоохоронної сфери необхідно розвивати свої навички, постійно підвищувати свій кваліфікаційний рівень, та вміння прораховувати на перед злочинні наміри. За допомогою даних вмінь можна буде з використанням комп'ютерних технологій та інформації створювати обмежувальні пастки для злочинців та передувати злочинам.

Важливою також безумовно залишається домовленість та співпраця між усіма державами-членами шляхом створення групи співпраці з метою надання підтримки і сприяння стратегічній співпраці та обміну інформацією між державами-членами; – високий рівень безпеки в усіх секторах, які мають життєво важливе значення для економіки і суспільства та, до того ж, значною мірою залежать від інформаційно-комунікаційних технологій.

1. Розслідування Wired: як відбувалася атака на Прикарпаттяобленерго [Електронний ресурс]. – Режим доступу: http://firtka.if.ua/?action=show&id=101335

2. Стратегія кібербезпеки України, затверджена Указом Президента України від 15 берез- ня 2016 року № 96/2016 [Електронний ресурс]. – Режим доступу: http://www.president.gov.ua/ documents/962016-198363

3. Розпорядженням Кабінету Міністрів України від 24 червня 2016 року № 440-р. [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/440-2016-%D1%80

Інформаційне забезпечення спеціальної поліцейської діяльності

Чанцева Т.П.
слухачка магістратури юридичного факультету ДДУВС
Косиченко О.О.
науковий керівник, к.т.н., доцент кафедри економічної та інформаційної безпеки ДДУВС

Інформаційне забезпечення сил охорони правопорядку є актуальним питанням не тільки для України, але й для багатьох зарубіжних країн, в яких значна увага приділяється створенню і використанню інформаційних систем спеціальної поліцейської діяльності. Поліцейські структури різних країн дедалі частіше взаємодіють між собою у протидії міжнародній злочинності, тероризму тощо. Також поліцейські структури співпрацюють із миротворчими місіями ООН, двосторонні угоди між країнами та багатосторонні договори, укладені міжнародними організаціями, дозволяють