

Коли проведений підготовчий етап, визначені цілі, терміни, завдання, шляхи виведення готівки, засоби прикриття і блокування сервісів ДБО, можна починати власне операцію: Злочинці отримують доступ безпосередньо до рахунку або картці клієнта і здійснюють несанкціонований переклад на заздалегідь підготовлений проміжний рахунок. Потім потрібна хороша ДОС-атака, яка обрушить сервіс, щоб клієнт не зміг своєчасно отримати інформацію про рух коштів на його рахунку. ДОС-атака повинна закінчитися в той момент, коли гроші будуть переведені в готівку.

Головне для запобігання цим злочинам - це підвищення обізнаності як самих клієнтів в області власної безпеки при використанні інтернет-сервісів, так і співробітників відділень банків під час роботи з ДБО. Це можуть бути різні наочні посібники для клієнтів, пам'ятки, спеціалізовані сторінки на сайтах банків, рекламні матеріали. Для співробітників - проведення тренінгів, створення систем мотивації. Ворога треба знати, щоб з ним боротися і застосовувати заходи самооборони. Банкам слід наполегливо оповіщати клієнтів - користувачів систем ДБО про заходи безпеки та давати їм докладні рекомендації про застосування захисних заходів, у тому числі антивірусного програмного забезпечення з функціями антихакер і антишпигун.

Наступні заходи носять більш технологічний характер і можуть бути віднесені до самих банків. Вважається, що чіпові карти більш захищені, ніж магнітні, тому в якості першої рекомендації банкам - пора переходити на чіпові картки. На даному етапі розвитку технологій чіпову карту можна скопіювати, тільки якщо її потримати в руках. Крім того, потрібно впроваджувати використання «електронних гаманців» або «віртуальних карт» для інтернет-платежів.

Література:

1. Попович В. М. Правові основи банківської справи та її захист від злочинних посягань / В. М. Попович. – К., 1995. – 325 с.
2. Про банки і банківську діяльність : закон України [Електронний ресурс]. – Режим доступу: <http://zakon2.rada.gov.ua/laws/show/2121-14>.
3. Скімінг у банкоматах [Електронний ресурс]. – Режим доступу : <http://www.chclub.ru/skimmingatm>.
4. Ваш електронний гаманець – під загрозою. Щомиті з нього можуть поцупити те, що нажите непосильною працею [Електронний ресурс]. – Режим доступу : <http://tsn.ua/groschi/kradizhok-groshey-z-kreditok-znachnopolbilshaye.html>.

Взаємодія суб'єктів боротьби з тероризмом щодо забезпечення кібербезпеки в Україні

Форноляк В.М.

кандидат психологічних наук
докторант Національної академії Служби безпеки України

На сьогоднішній день досить гостро постають питання забезпечення національної безпеки України від внутрішніх і зовнішніх загроз, а також адміністративно-правових засад діяльності відповідних правоохоронних та інших державних органів, що вимагають належного розв'язання і нормативного врегулювання. Одним із ключових елементів такої діяльності є закріплення організаційно-правових основ інформаційного забезпечення суб'єктів боротьби з тероризмом. Зазначене питання тісно пов'язане із практичними завданнями боротьби з кібертероризмом. Визначення і закріплення у законодавстві основ правового регулювання протидії даному виду злочинів сприятиме не лише ефективному виконанню покладених на кожен із суб'єктів завдань, а й реалізації комплексної системи щодо створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави.

Національна система кібербезпеки діє відповідно до Конституції України [1] та інших нормативно-правових актів, що регулюють суспільні відносини у сфері національної безпеки, зокрема: Закон України «Про основи національної безпеки України [2], Концепція розвитку сектору безпеки і оборони України [3], Положення про Національний координаційний центр кібербезпеки [4], Стратегія національної безпеки України [5], Стратегія кібербезпеки України [6], Воєнна доктрина України, доктрина інформаційної безпеки [7]. Забезпечення кібербезпеки повинно здійснюватися на національному рівні, відповідно до стандартів ЄС.

Відповідно до п. 3 Стратегії кібербезпеки України, основу національної системи кібербезпеки становлять Міністерство оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України, Національний банк України, розвідувальні органи [6], які, відповідно до ст. 4 Закону України «Про боротьбу з тероризмом» [8] є суб'єктами боротьби з тероризмом.

Для забезпечення кібербезпеки зазначені суб'єкти, як і всі інші державні органи, їх посадові особи зобов'язані діяти лише на підставі, в межах повноважень та у спосіб, що передбачені Конституцією та законами України [1] та положення законів України: "Про Збройні Сили України" [9], Державну службу спеціального зв'язку та захисту інформації України [10], "Про Службу безпеки України" [11], "Про Національну поліцію" [12], «Про Національний Банк» [13], «Про Службу зовнішньої розвідки України» [14], "Про оперативно-розшукову діяльність" [15], "Про контррозвідувальну діяльність" [16], а також Закону України "Про інформацію" [17], що визначають основоположні засади інформаційно-правового забезпечення взаємодії суб'єктів боротьби з тероризмом. Тому, формування організаційно-правових основ інформаційного забезпечення вказаних суб'єктів, насамперед, відбувається на законодавчому рівні. Зокрема, у Законі України "Про Службу безпеки України" вказано, що СБ України взаємодіє з правоохоронними та митними органами України у порядку і на засадах, визначених законами, указами Президента України та прийнятими на їх основі актами Служби безпеки України і взаємодіє з державними органами, підприємствами, установами, організаціями та посадовими особами, які сприяють виконанню покладених на неї завдань [11, ст. 8]. Згідно із Законом України "Про Національну поліцію", поліція у процесі своєї діяльності взаємодіє з органами правопорядку та іншими органами державної влади, а також органами місцевого самоврядування відповідно до закону та інших нормативно-правових актів [12, ст. 5].

Важливим для формування системи організаційно-правових основ забезпечення кібербезпеки є положення Закону України "Про оперативно-розшукову діяльність" про те, що підрозділи, які здійснюють оперативно-розшукову діяльність, мають право знімати інформацію з каналів зв'язку, застосовувати інші технічні засоби отримання інформації; отримувати від юридичних та фізичних осіб безкоштовно або за винагороду інформацію про злочини, які готуються або вчинені, та загрозу безпеці суспільства і держави; створювати і застосовувати автоматизовані інформаційні системи тощо [15].

Ефективна протидія кібертероризму в Україні неможлива без добре налагодженої співпраці суб'єктів, які залучаються до протидії даному виду злочинів. Основними засадами для організації та здійснення взаємодії суб'єктів боротьби з тероризмом є: чітке розуміння задуму, змісту завдань таких заходів і шляхів їх виконання; спільне розроблення ключових документів і своєчасний контроль за виконанням їх вимог.

В цілому така взаємодія полягає передусім у тому, що вона дає змогу комплексно, оперативно та ефективно використовувати наявні сили, засоби й можливості різних відомств, органів, служб і підрозділів з урахуванням їх специфіки та компетенції. Належна їй організація забезпечує успішне виконання завдань, визначених чинним законодавством, певним колом відповідних суб'єктів. Реалізація зазначених завдань, в свою чергу, потребує належного інформаційного забезпечення. Саме інформація і чітка взаємодія виступають основою забезпечення ефективності проведення заходів щодо забезпечення кібербезпеки в Україні.

Механізми взаємодії суб'єктів боротьби з тероризмом доцільно розглядати як послідовну реалізацію комплексу правових та організаційних дій, що базуються на основоположних принципах, цільовій орієнтації та використанні відповідних методів управління, спрямованих на задоволення їх інформаційно-комунікативних потреб. У структурі механізму взаємодії можна виділити чотири основних блоки: правовий, організаційний, інформаційний та ресурсний.

Правове забезпечення взаємодії суб'єктів боротьби з тероризмом передбачає: всебічне використання засобів і форм співробітництва з метою підвищення ефективності протидії кібертероризму (зокрема, опрацювання нормативних актів, що регулюють функціональні і правові відносини у процесі задоволення інформаційно-комунікативних потреб співробітників, сукупність правових норм, втілених у внутрішні документи); державне регулювання їх діяльності.

Організаційний блок взаємодії включає упорядкування, формування організаційної структури відповідних підрозділів суб'єктів боротьби з тероризмом, безпосереднє внутрішні організаційне управління шляхом реалізації функцій прогнозування, планування, організації, мотивації, контролю, координації.

До **інформаційного** блоку, відповідно до ст.2 Закону України "Про інформацію", можуть бути віднесені: одержання, використання, поширення, зберігання інформації [17].

Ресурсне забезпечення взаємодії суб'єктів боротьби з тероризмом включає кадрове, технічне та науково-методичне забезпечення, форми, методи, технології, підбір, розстановку, просування кадрів, їх перепідготовка та підвищення кваліфікації, фінансування програм розвитку взаємодії.

Узагальнюючи вищевикладене можна зробити такі висновки. Взаємодію суб'єктів боротьби з тероризмом спрямовану на забезпечення кібербезпеки, в загальному вигляді можна визначити як процес обміну інформацією, що об'єднує в єдине ціле представників різних відомств; зміцнює необхідний зворотний зв'язок між ними. Вона є складним багатогранним процесом, що передбачає: забезпечення інформаційного обслуговування діяльності системи боротьби з кібертероризмом; налагодження тісних як внутрівідомчих так і міжвідомчих зв'язків; використання інноваційних комунікативних форм і технологій налагодження взаємодії.

Література:

1. Конституція України [Електронний ресурс]: Закон України від 28 черв. 1996 р. № 254к. – Режим доступу: <http://zakon2.rada.gov.ua/laws/show/254к/96-вр>.
2. Про основи національної безпеки : Закон України від 19.06.2003 р. [Електронний ресурс].- Режим доступу: <http://zakon0.rada.gov.ua/laws/show/964-15>.
3. Концепція розвитку сектору безпеки і оборони України від 14.03.2016р. [Електронний ресурс].- Режим доступу: <http://zakon3.rada.gov.ua/laws/show/92-2016>.
4. Положення про Національний координаційний центр кібербезпеки від 07.06.2016 р. [Електронний ресурс]. - Режим доступу: <http://zakon2.rada.gov.ua/laws/show/242-2016>.
5. Стратегія національної безпеки України від 26.05.2015 р. [Електронний ресурс].- Режим доступу: <http://zakon2.rada.gov.ua/laws/show/555-2015>.
6. Стратегія кібербезпеки від 15.03.2016 р. [Електронний ресурс].- Режим доступу: <http://zakon3.rada.gov.ua/laws/show/96-2016>.
7. Доктрина інформаційної безпеки України. [Електронний ресурс].- Режим доступу: <http://www.president.gov.ua/documents/472017-21374>.
8. Про боротьбу з тероризмом [Електронний ресурс]: Закон України від 20.03.2003 р. № 638-IV. – Режим доступу: <http://zakon.rada.gov.ua /laws/show/638-15>.
9. Про Збройні Сили України [Електронний ресурс] : Закон України від 6.12.1991 р. № 1934-XII. – Режим доступу: <http://zakon2.rada.gov.ua/laws/show/1934-12>.
10. Про Державну службу спеціального зв'язку та захисту інформації України [Електронний ресурс] : Закон України від 23.02.2006 р. № 3475-IV. – Режим доступу: <http://zakon3.rada.gov.ua /laws/show/3475-15>.
11. Про службу безпеки України [Електронний ресурс]: Закон України від 25.03.1992 р. № 2229-XII. – Режим доступу: <http://zakon.rada.gov.ua/laws/show/2229-12>.
12. Про Національну поліцію [Електронний ресурс]: Закон України від 2.07.2015 р. № 580-VIII. – Режим доступу: <http://zakon5.rada.gov.ua/laws/show/580-19>.
13. Про Національний Банк [Електронний ресурс]: Закон України від 20.05.1999 р. №679-XIV/ – Режим доступу: <http://zakon0.rada.gov.ua/laws/show/679-14>.
14. Про Службу зовнішньої розвідки України [Електронний ресурс] : Закон України від 1.12.2005 р. № 3160-IV. – Режим доступу: <http://zakon2.rada.gov.ua/laws/show/3160-15>.
15. Про оперативно-розшукову діяльність: Закон України від 18.02.1992 року № 2135-XII. – Верховна Рада України. – Офіційний веб-сайт. – Режим доступу: <http://zakon3.rada.gov.ua/laws/show/2135-12>.
16. Про контррозвідувальну діяльність [Електронний ресурс]: Закон України від 26.12.2002 р. №374- IV. – Режим доступу: <http://zakon0.rada.gov.ua/laws/show/374-125>.
17. Про інформацію [Електронний ресурс]: Закон України від 2.10.1992 р. №2657- XII. – Режим доступу: <http://zakon20.rada.gov.ua/laws/show/2657-12>.