Одеський державний університет внутрішніх справ
«Кібербезпека в Україні: правові та організаційні питання»

Інформаційна та кібернетична безпека: роль та місце в умовах гібридної війни

Грищук Р.В.
доктор технічних наук, старший науковий співробітник
начальник науково-дослідного відділу інформаційної та кібернетичної безпеки
наукового центру Житомирського військового інституту імені С. П. Корольова

Кардинальна зміна форм та способів збройного протистояння внаслідок повсюдного поширення надбань високих технологій, суттєво вплинула на виконання завдань за призначенням силовими та спеціальними структурами будь-якої розвиненої держави світу [1, с. 555]. При цьому Україна прагне увійти до кола держав з розвиненою економікою, а тому активно впроваджує в усіх сферах технологічні інновації, які окрім усіх інших позитивних аспектів створюють передумови для виникнення нових й нетипових до сьогодні для силових та спеціальних структур держави викликів й загроз безпеці. Наприклад, комп'ютеризація економічної, військової, соціальної та інших сфер породжує такі нові виклики та загрози для силових та спеціальних структур держави: для Служби безпеки України – проблему боротьби з кібертероризмом; для Міністерства внутрішніх справ України – проблему боротьби з кіберзлочинністю; для Міністерства оборони України – проблему забезпечення кібероборони держави; для Державної служби спеціального зв'язку та захисту інформації України – проблему кіберзахисту державних інформаційних ресурсів тощо.

Таким чином, кожна силова або спеціальна структура держави постала перед фактом: противник (кібертерорист, кіберзлочинець тощо) застосовує нові гібридні форми для досягнення своїх цілей, при цьому для досягнення максимального ефекту, вкладає в них новий зміст – діє асиметрично. Отже, проблема забезпечення кібербезпеки держави на сьогодні є актуальною. Особливо її значення зростає, коли проявляються елементи гібридизації – не нові за сутністю але унікальні за узгодженістю цілей, динамічністю їх досягнення, зростанням ролі інформаційної та кібернетичної складової на усіх рівнях.

На сьогодні, як відомо [2, с. 1], в державі відбувається становлення національної системи кібербезпеки. Але суттєвим стримуючим чинником на шляху її практичного впровадження є розрізненість не тільки суто технічних підходів та технологічних прийомів, а й в першу чергу непорозуміння обумовлене дефініційною невизначеністю. Відбувається розмиття та взаємопідміна таких понять як кібербезпека, інформаційна безпека, безпека інформації та технічний захист інформації.

Якщо виходити з того, що інформаційна безпека – це стан захищеності людини, суспільства та держави від зовнішніх та внутрішніх деструктивних інформаційних (інформаційно-психологічних) впливів, а кібербезпека (у вузькому сенсі цього слова) – це стан захищеності процесів управління в кіберпросторі від явних та потенційних кіберзагроз, за якого забезпечується сталий розвиток суспільства, держави та особистості, то в умовах гібридної війни, незалежно від сфери її ведення, під інформаційними та кібернетичними діями слід розуміти наступне [3, с. 133]. Інформаційні дії – це дії, які спрямовані на зміну масової та індивідуальної свідомості суб'єкта впливу (соціуму) з метою стимулювання у нього заданого типу поведінки. Кібернетичні дії – це дії, які спрямовані на об'єкти та суб'єкти кіберпростору (соціум, технічні та соціотехнічні системи), у вигляді різноманітних деструктивних впливів, наприклад кібератак, реалізація яких призводить до контрольованого управління згаданими об'єктами та суб'єктами.

У доповіді подано приклади [4, с. 9], що підтверджують справедливість наведених вище тез. Зокрема, розкрито технологію першого в сучасній світовій історії потужного кібернападу на Естонію 2007 року, який паралізував практично всі її критичні кібернетичні інфраструктури й супроводжувався інтенсивною підтримкою інформаційних дій. Також яскравим прикладом протиборства в кіберпросторі, який наведений в доповіді є інформаційні та кібернетичні дії, що здійснювалися під час Російсько-грузинської війни в 2008 році. Типовим актом несилового протистояння в кіберпросторі є й кібернапад на іранські ядерні об'єкти за допомогою мережевого хробака «Stuxnet» у рамках американської програми під кодовою назвою «Олімпійські ігри» 2010 року. Окремо показано роль та місце інформаційних та кібернетичних дій під час організації та проведення «кольорових революцій» та заворушень на близькому сході у 2010 р. під час «Арабської весни».

Основні акценти в доповіді розставлено на ролі та місці інформаційної та кібернетичної безпеки під час гібридної війни в Україні [5, с. 84]. Показано поетапність нарощення сил та засобів протиборчою стороною, розкрито технологію здійснення інформаційних та кібернетичних дій, приведено можливі сценарії розвитку подій. Крім того, подано результати практичних дій з питань забезпечення інформаційної та кібернетичної безпеки [6, с. 11]. Розкрито сутність та зміст

синергетичного підходу – як основи для прогнозування можливих подій унаслідок інформаційної та кібернетичної взаємодії [7, с. 66].

Література:

1. Грищук Р.В. Основи кібернетичної безпеки : Монографія / Ю.Г. Даник, Р.В. Грищук ; за заг. ред. проф. Ю.Г. Даника. – Житомир : ЖНАЕУ, 2016. – 636 с.

2. Указ Президента України №96/2016 Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України" [Електронний ресурс]. – Режим доступу : http://www.president.gov.ua/
documents/962016-19836 . – Назва з екрану.

3. Грищук Р.В. Синергія інформаційних та кібернетичних дій / Р. В. Грищук, Ю. Г. Даник // Труди університету. – К. : НУОУ, 2014. – № 6 (127). – С. 132–143.

4. Грищук Р.В. Кіберінциденти: передумови скоєння та наслідки / Р. В. Грищук // Перша міжнар. наук.-практ. конф. ["Проблеми науково-технічного та правового забезпечення кібербезпеки у сучасному світі"] (Харків, 30 бер. – 1 квітн.). – Харків : ХТУ "ХПІ", 2016 р. – С. 9–10.

5. Грищук Р.В. Технологічні аспекти інформаційного протиборства на сучасному етапі / Р.В. Грищук, І.О. Канкін, В.В. Охрімчук // Захист інформації. – 2015. – Том 17. – № 1 – С. 80–86.

6. Грищук Р.В. Синергетика безпекових кластерів: теорія та практика / 5 міжнар. наук.-техн. конф. ["Захист інформації і безпека інформаційних систем"] (Львів, 02– 03 черв. 2016 р.). – Л. : НУ ЛП, 2016. – С. 10–11.

7. Hryshchuk R. The Synergetic Approach for Providing Bank Information Security: The Problem Formulation / Ruslan Hryshchuk, Sergii Yevseiev // Безпека інформації. – 2016. – Том 22. – № 1 – С. 64–74.

Місце кібертероризму у структурі кіберзлочинності та напрями боротьбі з ним

Пядишев В.Г.
кандидат технічних наук, доцент,
доцент кафедри кібербезпеки та інформаційного забезпечення
Одеського державного університету внутрішніх справ

На думку науковців наразі найбільшу загрозу для всієї міжнародної спільноти становить саме кібер-тероризм. Це жахливе явище має два крила: кіберзлочинність та тероризм.

Кіберзлочинність доцільно розглядати як дві сфери: 1) низка старих відомих злочинів, які значно "вдосконалилися" через підтримку останніх комп'ютерних технологій; 2) нові злочини, які були б принципово неможливі без досягнень в інформаційно-телекомунікаційній галузі. Причому вже наразі кіберзлочинність по прибутковості посідає одне з перших місць серед всіх видів злочинності. Як і всі види над-прибуткової злочинності, вона впевнено переростає в організовану та транснаціональну.

Одночасне все більш зловісні ознаки і розміри розпочала проявляти сукупність відомих зі стародавньої історії таких злочинів, як тероризм, структура якого з кожним роком ускладнюється.

Саме наразі спостерігається драматичне зрощування зазначених явищ — кіберзлочинності та тероризму: тероризм набуває нових сучасних можливостей свого втілення.

Зауважимо, що в зонах локальних збройних конфліктів, тобто в умовах послаблення правоохоронного контролю, спостерігається значне зростання рівню і різноманіття всіх видів злочинності. Це торгівля наркотиками, зброєю, природними ресурсами, награбованими витворами мистецтва, людьми, людськими органами... Вся ця злочинність набуває індустріальної організованості та транснаціонального розмаху. Також розвівається і тероризм. Саме тут він набуває поширення аж до рівню домінування у державі. Більш того, він стає транснаціональним, тобто таким, що його агенти скоординовано працюють у багатьох державах світу.

Транснаціональний тероризм такого легко підкорює всі види організованої злочинності: з одного боку він надає їй захист, з іншого він її експлуатує.

Ми вважаємо, що транснаціональний тероризм характеризується наступними ознаками.-компонентами:

- звичайною практикою його є геноцид;
- методом досягнення цілей є насильницький екстремізм;
- здійснюється вербування, професійна підготовка і впровадження своїх агентів до всіх страт суспільства;