

УДК 67.401

ДОСЛІДЖЕННЯ ПРОБЛЕМАТИКИ КІБЕРБЕЗПЕКИ УКРАЇНИ

Войтович В.С.

Гриник Р.О.

Львівський державний університет безпеки життєдіяльності

В даний час рівень кіберзлочинності продовжує зростати надзвичайно швидкими темпами, тому поняття кібербезпеки все частіше розглядається, як стратегічна проблема держави яка завдає суттєвої шкоди економіці не тільки окремих суб'єктів господарювання, а й економіці держави в цілому. Це призводить до того, що кіберпростір перетворюється на окрему сферу бойових дій, у якій діють збройні сили високорозвинених держав, терористичні та злочинні організації.

На сьогодні проблематика забезпечення безпеки у кіберпросторі активно досліджується та обговорюється. Одною з причин цього є те, що кіберпростір знайшов широке застосування в галузі безпеки і оборони. Кібербезпека України на даний момент знаходиться на низькому рівні, а кіберпростір є надзвичайно уразливий до різноманітних кібератак[2]. Виною цього є широка, здебільшого домінуюча, наявність в інформаційній інфраструктурі України осіб, організацій чи груп, які прямо чи опосередковано співпрацюють з іншими державами [1].

Найчастіше кібератаки здійснюються на інформаційні ресурси фінансових установ, урядові інформаційні ресурси та на електронні ресурси компаній та установ життєзабезпечення. Для прикладу я наведу нещодавні кібератаки на Україну. У грудні 2015 року була проведена масштабна атака на енергетичні компанії нашої держави, найбільший удар отримали споживачі «Прикарпаттяобленерго», а саме, було вимкнено біля 30 підстанцій, близько 230 тисяч громадян залишилися без світла інтервалом до шести годин. Дана атака була застосована з використанням троянської програми BlackEnergy. З меншими втратами одночасно зазнали атаки «Чернівціобленерго» та «Київобленерго». Щодо фінансових організацій, то в минулому році 6 грудня, була здійснена кібератака на урядові сайти: Держказначейства України та інших, а також на внутрішні мережі державних органів, що потягнула за собою до великої затримки бюджетних виплат. Відповідно на дану атаку, Кабінет міністрів на наступний день виділив 80 млн. гривень для відповідного захисту від кібератак, хакерів, зловмисників.

Кожен громадянин нашої країни стикається щодня з загрозами в інформаційному світі, тому компетентність користувача та розуміння ним основних і базових постулат безпечного користування мережею неабияк підвищуватимуть стійкість системи кібербезпеки України. Основними помилками користувачів є надання персональних даних третій стороні, так як досить часто їх використовують для розсилання вірусної реклами, а головною небезпечкою є те, що дані про людину застосовують для нелегальних і сумнівних операцій, а саме, відкриття таємних підприємств, відмивання грошей, взяття кредитів та інші злочини.

Подальший розвиток системи захисту кіберпростору України від кібератак залежить від рівня взаємодії зацікавлених сторін: держави, громадян, науково-технічних систем, приватних господарств і полягає у розробленні новітніх інформаційно-комунікаційних технологій, законодавчої та нормативної бази, системи навчання населення безпечному використанню кіберпростору. Дане питання є актуальним тому, що в дію вступає нове поняття – «кібервійна», що у своєму роді показує використання мережі Інтернет, технічних та інформаційних засобів будь-якою країною-агресором, що за мету має заподіяння шкоди економічній, політичній, технічній, військовій та інформаційній безпеці та суверенітету нашої держави.

Література:

1. Дубов, Дмитро Володимирович. "Стратегічні аспекти кібербезпеки України." Стратегічні пріоритети 4 (2013): 29.
2. Гриник, Р. О. Дослідження проблем захисту сучасного кіберпростору України / Р. О. Гриник, М. В. Маржан // Актуальні задачі та досягнення у галузі кібербезпеки : матеріали Всеукр. наук.-практ. конф., м. Кропивницький, 23–25 листоп. 2016 р. – Кропивницький : КНТУ, 2016. – С. 30–31.

УДК 656.1

АНАЛІЗ СУЧАСНИХ МЕТОДІВ ТРАНСПОРТНИХ ДОСЛІДЖЕНЬ

Грицюк С.А., Грицай Д.В.
Паснак І.В., канд. техн. наук

Львівський державний університет безпеки життєдіяльності

Протягом останніх років в Україні відбувається збільшення кількості міського автомобільного транспорту, а особливо приватних легкових автомобілів, що призвело до вичерпання пропускної спроможності вулично-дорожньої мережі (ВДМ) міста, яка проектувалася в період, коли кількість автомобільного транспорту була незначною [3]. Також спостерігається відсутність сучасної системи управління, організації і контролю за рухом транспортних засобів і пішоходів.

Вирішення цієї проблеми вимагає оптимізації руху транспортних засобів на ВДМ міста, що включає комплекс планувальних, інженерно-технічних, управлінських та організаційних заходів [3]. Проте кожна розробка щодо покращення організації дорожнього руху ґрунтується на аналізі необхідних вихідних даних.

Транспортні дослідження являються важливою та невід'ємною частиною процесу управління, без них неможливе оптимальне функціонування і розвиток дорожнього руху. Для прийняття управлінських рішень необхідно володіти повною та достовірною інформацією, яку можна отримати лише в результаті досліджень.

У різних країнах відомо багато методів досліджень дорожнього руху, їхній діапазон сягає від найпростіших, виконання яких доступно одній людині без спеціальних приладів та обладнання, і до складних та трудомістких, які виконуються із застосуванням сучасної електронної апаратури та рухомих лабораторій.