УДК 343.98

# ПРОБЛЕМИ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ: МІЖНАРОДНИЙ ДОСВІД ТА УКРАЇНСЬКІ РЕАЛІЇ

**Петровський О.М., Лівчук С.Ю.**
Національний університет водного господарства та природокористування

У статті проведено дослідження у сфері боротьби з кіберзлочинами в ЄС і США, виділено позитивні сторони, які було б доцільно запровадити в Україні. Також проаналізовано проблеми, що виникають в області боротьби з комп'ютерними злочинами в Україні і надано пропозиції шляхів їх вирішення.
**Ключові слова:** кіберзлочинність, інформаційний злочин, інформація, боротьба, протидія, Стратегія, NERC CIP.

**Постановка проблеми у загальному вигляді.** Верховною Радою України було зроблено спробу врегулювати відносини, що виникають у кіберпросторі, а саме ухвалено Закон України «Про основні засади забезпечення кібербезпеки в Україні». Незважаючи на ці кроки Україна постійно стає жертвою кібератак, в зв'язку з чим питання протидії кіберзлочинності набуває особливої актуальності.

**Метою статті** є аналіз та дослідження проблемних питань протидії кіберзлочинності в Україні та на цій основі надати пропозиції щодо їх вирішення.

Виклад основних положень. Сьогодні у багатьох зарубіжних країнах налагоджена система співробітництва, що обумовлюється необхідністю обміну досвідом на міжнародному рівні. Ці питання координуються кожною країною відповідно до розробленої та діючої стратегії кібербезпеки: США та більшість країн-учасниць ЄС у своїх стратегіях виносять питання боротьби з кіберзлочинністю на передові позиції. Саме США стала першою країною, яка прийняла відповідний закон та створила Національну стратегію безпеки в кіберпросторі. Причиною написання даного документу стала терористична атака 11 вересня 2001 року. Стратегія була частиною більш загальної Стратегії забезпечення національної безпеки (National Strategy for Homeland Security). Крім того, за оцінками фахівців, саме в США щорічно втрати корпорацій від злочинності перевищують 200 млрд, а від комп'ютерних злочинів – 6 млрд. дол., тому питання боротьби з кіберзлочинністю для цієї країни є надзвичайно актуальним [9].

На державному рівні в США були прийняті такі важливі програмні документи, які створюють фундамент для боротьби з кіберзлочинністю, як: Міжнародна стратегія для кіберпростору «Процвітання, безпека, відкритість у мережевому світі» (2011); Кіберстратегія Міністерства оборони від квітня 2015 року; Міжвідомчий план дій з кібербезпеки систем управління (Cross-Sector Roadmap for Cybersecurity of Control Systems); План дій з посилення кібербезпеки найважливіших об'єктів інфраструктури (Roadmap for Improving Critical Infrastructure Cybersecurity, 2014); План дій з забезпечення кібербезпеки систем енергопостачання (Roadmap to Achieve Energy Delivery Systems Cybersecurity). Загалом у США проводиться виважена політика щодо боротьби з кіберзлочинністю, що дозволяє залучати до співпраці урядові організації та зацікавлених осіб, таким чином об'єднуючи їх зусилля.

Щодо кримінального законодавства США у сфері кіберзлочинності, то воно включає в себе Закон «Про боротьбу зі спамом» (Controlling the Assault of Non-solicited Pornography and Marketing, 2003); Закон «Про злочини, пов'язані з засобами доступу» (Fraud and related activity in connection with access devices); Закон «Про злочини, пов'язані з комп'ютерами» (Fraud and related activity in connection with computers); Закон «Про злочини, пов'язані з електронною поштою» (Fraud and related activity in connection with electronic mail); Закон «Про перехоплення електронних повідомлень та прослуховування переговорів» (Wire and Electronic Communications in Terception and Interception of Oral Communications); Закон «Про зберігання повідомлень та доступ до записів транзакцій» (Stored Wire and Electronic Communications and Transactional Record Access) [6]. Усі види кіберзлочинів поділяються на три групи: злочини проти інтелектуальної власності; злочини, що завдають шкоди комп'ютерному обладнанню; злочини проти користувачів комп'ютерної мережі.

Для протидії кіберзлочинності в США були створені спеціальні підрозділи та відомства:

1. Electronic Crimes Task Forces ECTF підрозділ Секретна служба США (United States Secret Service USSS), що було створене у 1865 році для розслідування і запобігання фальшивомонетництва. Проте з роками відбулась еволюція її функцій і на сьогоднішній день Секретна служба США бореться з економічними та комп'ютерними злочинами [3].

2. Федеральне агентство США, що підпорядковане міністерству внутрішньої безпеки США (уведено в підпорядкування в 2003 р. до цього було підпорядковано міністерству фінансів США). Воно утворює взаємодію між службами, правоохоронними органами (федерального рівня, рівня штату, локальними), приватним сектором, академічним співтовариством, що в свою чергу виявляють і запобігають кіберзлочинам.

3. US Cyber Command (Військовий підрозділ, який здійснює свою діяльність у кіберпросторі).

4. United States Computer Emergency Readiness Team (Національний відділ кіберзахисту Департаменту внутрішньої безпеки США).

5. Computer Crime and Intellectual Property Section (Відділ комп'ютерної злочинності і інтелектуальної власності).