УДК 343.431

Д. Б. САНАКОЄВ,
кандидат юридичних наук,
доцент кафедри спеціальної техніки
Запорізького юридичного інституту
Дніпропетровського державного університету внутрішніх справ

ПРОТИДІЯ ПОРНОГРАФІЇ В ІНТЕРНЕТ ПІДРОЗДІЛАМИ З БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ ТА ТОРГІВЛЕЮ ЛЮДЬМИ

Розглянуто порядок застосування механізмів контролю доступу до web-контенту; досліджено технології, типи інформації, що фільтрується, механізми фільтрації. Надано пропозиції щодо можливостей здійснення органами внутрішніх справ контролю доступу до web-контенту.

На сьогодні широке застосування комп'ютерних технологій і телекомунікаційних систем, створення на їх ґрунті глобальних комп'ютерних мереж не лише створило передумови, що полегшують учинення злочинів, але й дозволило перенести частину злочинних посягань безпосередньо у кіберпростір. Серед них значне місце посідає і розповсюдження порнографічних зображень неповнолітніх. За офіційними даними, у мережі Інтернет розповсюджується до 75 % усієї дитячої порнопродукції [1]. Виробники порнографії, знаючи про незадовільний стан правової оцінки цього виду злочинів в Україні, намагаються перемістити свої ресурси дитячої порнографії на територію української частини Інтернету.

Дослідженням проблем протидії злочинам, що вчиняються із використанням комп'ютерної техніки, зокрема розповсюдженню порнографічних матеріалів через Інтернет, присвячено чимало робіт вітчизняних та зарубіжних дослідників, зокрема: В. Б. Вєхова, В. О. Голубєва, В. Ю. Рогозіна, С. В. Хільченка, О. М. Яковлєва тощо. Однак стрімкий розвиток кіберзлочинності потребує постійного удосконалення існуючих та напрацювання нових заходів протидії, зокрема здійснення контролю доступу до web-контенту.

Отже, **мета** даної статті – надати пропозиції щодо можливостей здійснення органами внутрішніх справ контролю доступу до web-контенту. Мета зумовлює такі **завдання**: розглянути порядок застосування механізмів контролю доступу до web-контенту; дослідити технології, типи інформації, що фільтрується, а також окремі наслідки застосування механізмів фільтрації, у тому числі технології ухилення від такого контролю.

Спецпідрозділами ДБКТЛ МВС України здійснюється моніторинг мережі Інтернет із метою виявлення порнографічних зображень. Ця проблема пов'язана з труднощами автоматизації пошуку порносайтів у глобальній мережі. Враховуючи, що порнографією є не просто натуралістичне зображення фізіологічних елементів статевих актів, органів чи непристойних форм сексуальної поведінки, а лише тих, метою яких є збудження статевих інстинктів, то створити типову математичну модель такого зображення неможливо. Відповідно, неможливо задати параметри для програмного пошуку у мережі завідомо порнографічних зображень. Доки ця проблема не вирішина, пошук зрештою часто здійснюється вручну, що знижує ефективність такої роботи.

Суттєво ускладнює пошук та фіксацію порнографічних матеріалів в Інтернет специфічний спосіб учинення цього злочину. Шифрування, засоби збереження ключової ланки, однорангові об'єкти мережі, чат-реле, діалогові конференції та інші можливості Інтернет дозволяють злочинцям активно поширювати власні контенти, заплутуючи сліди та ускладнюючи встановлення власників сайтів.

Фільтрацію контенту в інтерактивному режимі може здійснювати будь-яка особа, яка входить до структури кінцевого користувача та працює на web-сервері, що підтримує контент. Компанії переважно обмежують доступ до певних відомостей, розміщених у web-мережі, для того, щоб підвищити продуктивність обладнання та уникнути можливих позовів чи претензій у випадку навмисного використання своїми працівниками будь-яких даних. Окрім того, громадські організації зазвичай обмежують доступ до відкритої інформації, якщо надають вільний вихід до Інтернету. Вказані ситуації об'єднує одна загальна обставина: для доступу в Інтернет користувач може без обмежень використовувати власну мережу. Проте в

деяких країнах за певних умов доступ до окремих web-сторінок обмежено.

Он-лайн фільтрація істотно не відрізняється від інших типів цензури, проте пов'язана з технічними труднощами, зумовленими децентралізацією Інтернету. Однак навіть якщо у правоохоронних органів виникає необхідність легально протистояти розміщенню певного контенту у web-мережі своєї країни, небажану інформацію всього за декілька хвилин можна фізично перемістити на закордонний сервер. Якщо переміщений контент відповідає законодавству іноземної країни або якщо від її владних структур неможливо вимагати видалення цієї інформації з мережі, єдиним засобом обмеження доступу до неї своїх громадян є застосування певної системи фільтрації.

При цьому важливо розмежовувати кримінальне переслідування через розміщення протизаконного контенту в Інтернеті та фільтрацію інформаційного наповнення web-сайтів, завдання якої обмежуються забороною доступу до певних сайтів та застосування схем, що його ускладнюють. Предметом нашого аналізу є другий підхід.

Існує низка мотивів, що викликають потребу у встановленні цензури контенту web-сайтів. Вони варіюють від елементарного бажання убезпечити потерпілих від таких злочинів чи правопорушень від збитків, що завдаються їм постійним перебуванням шкідливої інформації в Інтернеті (перш за все йдеться про дитячу сексуальну експлуатацію та осіб, постраждалих від будь-яких інших умисних дій), бажання обмежити вільне використання певних висловів, до введення заборони на доступ до інформаційного наповнення політичного змісту. Окрім того, часто на перший план виступають такі проблеми, як захист економічних інтересів, що стосується переважно мультимедійного контенту, який розповсюджується без дозволу власників авторських прав із використанням різних прикладних програм, наприклад голосового зв'язку через IP-протокол (VOIP). Подібні проблеми створюють загрозу телекомунікаційним монополіям, тому, наприклад, в Об'єднаних Арабських Еміратах такі прикладні програми заборонені [2].

Там, де держава жорстко контролює контент ЗМІ, також уводяться й суворі обмеження, що передбачають заборону на законодавчому рівні на розміщення у web-мережі певних відомостей, блокування доступу до окремих сайтів та контроль користувачів, які намагаються їх відкрити. Країни з жорстким контролем розташовуються переважно у трьох регіонах: Східній та Центральній Азії, на Близькому Сході та Північній Африці [3]. Ці держави виявляють найбільшу активність щодо обмеження доступу до інтерактивної інформації, проте у низці інших країн заборонено доступ до сайтів певного змісту, наприклад до сайтів з дитячою порнографією чи до web-сторінок, де можна знайти шкідливе програмне забезпечення. Принаймні питання про введення заборон там розглядається, причому планується використовувати ті самі технології, які застосовуються для обмеження свободи слова в Інтернеті. Розглянемо такі технології.

1. **Технологія фільтрації.** Через те, що в мережі Інтернет полегшено розповсюдження певного контенту та забезпечено його постійну наявність, введення будь-яких обмежень на доступ до інформації є складним завданням. Для фільтрації web-контенту, доступного кінцевим користувачам для перегляду, пропонуються два різних підходи: перший – провайдер надає доступ до Інтернету лише тим користувачам, які за діючим законодавством повинні (або їм рекомендовано) застосовувати механізми фільтрації; другий – інфраструктура фільтрації встановлюється у пунктах стратегічного призначення, тобто між національними мережами та міжнародною магістральною мережею та становлять різновид віртуального кордону. Останньому варіанту надають перевагу країни з уже розгорнутою телекомунікаційною мережею чи з існуючим суворим державним наглядом та контролем, де від початку необхідність застосування фільтрації web-контенту так чи інакше була очевидною.

Найбільш яскравим прикладом у цьому контексті є китайська система «Great Firewall»: у Китаї вся мережна інфраструктура, що надає доступ до міжнародного Інтернету, належить державі чи підконтрольним організаціям, наприклад Міністерству інформаційної промисловості, державній компанії China Telecom та ChinaNET. Вони контролюють абсолютно всі з'єднання із зовнішніми мережами та видають ліцензії на діяльність інтернет-провайдерам лише в якості ліцензіатів цієї інфраструктури. У країні використовується централізована система фільтрації, тому її критерії єдині. Звісно, така єдність неможлива, якщо обов'язок фільтрувати інформацію покладається на окремих інтернет-провайдерів. Проте й за такої ситуації можна застосувати загальний комплекс критеріїв із використанням різноманітних технічних засобів.

Так, у 2009 р. влада Китаю повідомила, що всі виробники комп'ютерів повинні встановлювати програму «Green Dam/Youth Escort» [4], функції якої передбачають фільтрацію всього контенту в інтерактивному режимі. Однак через протести заводів-виробників набрання рішенням законної сили було відкладено. Ця програма в цілому підтримує ті самі функції фільтрації, що й інші комерційні продукти, які є на ринку. Відмінність її полягає в адаптованості до параметрів конфігурації, які встановлені керівництвом країни.

Іншим прикладом примусового встановлення в апаратурі користувачів програмного забезпечення, що прямо не стосується фільтрації, є вимога місцевого телекомунікаційного оператора з ОАЕ встановлювати останню версію прикладної програми, розробленої у Blackberry, та бажання правоохоронних органів Німеччини використовувати троянські програми для перехоплення повідомлень у комп'ютерах, які використовуються підозрілими особами чи організаціями [5]. Однак фільтрація контенту, як правило, відбувається на мережному рівні, до передачі кінцевому користувачеві інформаційного наповнення, та ґрунтується на технології т. зв. чорних списків заборонених ресурсів, до яких можуть належати IP-адреси, імена доменів чи ключові слова, а також детальні пояснення.

1.1. *Блокування за IP-адресою.* Метод передбачає введення заборони на доступ до певних IP-адрес, включених до списку заборонених. Це найбільш проста та примітивна у використанні технологія. Вона не вимагає значних капіталовкладень у спеціалізоване обладнання (адже її функції обмежуються перевіркою заголовків TCP/IP) та практично не впливають на продуктивність мережі. Ця технологія досить корисна в екстремальних ситуаціях, коли провайдер або органи влади вимагають терміново блокувати доступ до певного ресурсу. Через це блокування однієї чи кількох IP-адрес, на сайтах яких розташовується інформація певного змісту, стає першим заходом, після якого можуть застосовуватись більш складні та вартісні технології. Основний недолік даного методу полягає в тому, що він здатен забезпечити незначний рівень деталізації, оскільки розрахований на фільтрацію окремих компонентів web-сайту. Так, коли йдеться про системи пошуку та великі обсяги інформації, наприклад про інтерактивні енциклопедії, приховання чи блокування не можливо застосувати до вибіркових результатів пошуку чи окремих статей: доводиться обирати між необмеженим доступом та обмеженим доступом до всього сайту в цілому.

Окрім того, коли декілька web-сайтів мають одну IP-адресу, то блокування, застосоване щодо одного з них, буде поширюватиметься і на інших. Недоліком даного методу є також його нездатність забезпечити необхідну ефективність роботи з сайтами, які використовують пул IP-адрес для розподілення навантаження між кількома серверами, а також із сайтами, які досить часто навмисно змінюють IP-адреси, намагаючись уникнути блокування IP-адреси так, щоб це бачив кінцевий користувач. Проте, незважаючи на свою простоту та відсталість, метод доволі широко застосовують провайдери, організації та різні країни, особливо для блокування відомих джерел шкідливого програмного забезпечення та спаму.

Один зі способів, що дозволяє подолати перераховані обмеження, передбачає використання модуля доступу web-мережі, який здійснює запит зарубіжного сервера про пошук необхідного контенту та передачі його кінцевому користувачеві. Такі сервери популярні у провайдерів та корпорацій для швидкісної передачі статичного контенту численним клієнтам, для фільтрації тієї інформації, яка може бути надана, та для використання модуля доступу (проксі-серверу), не внесеного до «чорного списку», що дозволяє легко уникнути блокування за IP-адресами.

Пошук у Google за параметрами *free open proxy* («безкоштовний відкритий проксі») дозволяє отримати низку проксі-серверів, які надають свої послуги безкоштовно заради здійснення свободи слова, інші пропонують безкоштовно лише деякі інструменти, але з більш широкими сучасними функціональними можливостями. Багато серверів, змінивши конфігурацію відповідним чином, або слугують модулями доступу, або навмисно діють як перехоплювачі потрібної інформації, наприклад рекомендацій чи номерів кредитних карт користувача.

1.2. *Блокування за доменом.* Первинна форма методики блокування трансформувалась у метод блокування із використанням імені домена як критерію фільтрації. Новий підхід підвищив вибірковість фільтрації, але не вплинув на «законослухняні домени», що користуються послугами одного й того самого хостинг-провайдера та списками заборонених IP-адрес. Проте метод все ж передбачає вибір між повним блокуванням чи доступом до кожного імені домена. Вказане обмеження найчастіше здійснюють шляхом внесення змін у режим роботи DNS-серверів, яким дають завдання

повертати результати неправильного оброблення з вказуванням помилки на сторінці або не давати жодних результатів, коли мова йде про заборонені ресурси.

Однією з країн, що надають перевагу саме цьому методу, є Німеччина, де нещодавно прийнято закон [6], за яким передбачено можливість провайдерів блокувати DNS-запити, що стосуються імен доменів, включених правоохоронцями до спеціального списку, що постійно оновлюється з тим, щоб блокувати доступ до сайтів із дитячою порнографією у максимально стислі терміни після їх ідентифікації. Австралія, Великобританія, Норвегія також застосовують блокування за DNS. У випадках, коли користувач запитує IP-адресу, віднесену до «чорного списку» імен доменів, DNS-сервер повертає адресу на статичну web-сторінку з попередженням про те, щоб сторона запиту звернула увагу на інформаційне наповнення сторінки, яка її цікавить. Щодо технічної сторони питання, то тут існує вірогідність реєстрації DNS-сервером IP-адрес усіх користувачів, які здійснюють запит цього контенту. Уникнути такого блокування просто: достатньо лише змінити конфігурацію комп'ютера так, щоб він звертався до DNS-сервера іншої країни (наприклад, до OpenDNS).

1.3. *Блокування за URL.* Більш ефективними методом блокування є перевірка повної адреси запитуваного ресурсу у мережі (URL) та надання доступу чи відмова в цьому на підставі більш складних правил. Це дозволяє блокувати доступ лише до певних частин сайту. З технічної точки зору такий метод фільтрації, як правило, здійснюється шляхом встановлення проксі-серверу, який може бути прозорим чи непрозорим, але обов'язковим для застосування. Проксі-сервер блокує всі спроби отримати web-контент, оминаючи його. Оскільки такий сервер стає єдиним джерелом web-контенту для всіх користувачів, можна легко створити правила, що контролюватимуть режим його роботи залежно від запитуваного домену, сторінки чи навіть параметрів інформації. Наприклад можна блокувати інтерактивні запити, в яких містяться ключові слова з «чорного списку» та виконуються через пошукову систему, оскільки умови пошуку будуть відображатися як параметри «get» («надіслати») в URL, що надає доступ до отриманих результатів. Ця технологія, що використовувалась у деяких комерційних рішеннях, призначених для корпоративних мереж, використовується і окремими країнами для фільтрації web-контенту. Зокрема це прикладні програми, розроблені компанією *McAfee* [7]. Істотним недоліком цих рішень є необхідність оброблення занадто великого обсягу інформації, що вимагає чіткого розрахунку інфраструктури, без якого може утворитися «вузьке місце», яке уповільнюватиме навігацію усіх користувачів у мережі. Проблему зазвичай вирішують за допомогою відкритих проксі-серверів чи інших серверів, спроможних знаходити контент у web-мережі та скеровувати їх за запитуваною адресою.

1.4. *Блокування за ключовими словами.* Зазначені у цій статті методи базуються на використанні великих списків заборонених ресурсів, які наповнюються вручну та які, безумовно, не можуть охопити всі існуючі контенти тієї чи іншої категорії, в умовах стрімких темпів та простоти нарощування обсягів інформаційного наповнення сайтів. Для вирішення цієї проблеми застосовуються такі прийоми: перегляд всієї інформації до її передачі кінцевому користувачеві та блокування контенту, якщо в ньому містяться слова, внесені до «чорного списку». Така технологія має назву «пакетна фільтрація», або «глибока перевірка пакетів», оскільки передбачає контроль усіх пакетних даних, що передаються.

При використанні пакетної фільтрації блокується більший обсяг контенту, аніж це потрібно. Так, може блокуватися доступ до навчальних матеріалів з репродуктивної біології, оскільки інформаційне наповнення за цими темами зазвичай містить слова, що асоціюються із порнографією. Таку інформацію, як правило, використовують у поєднанні з «білими списками» доменів, що викликають довіру, де обмеження за ключовими словами не здійснюється. Проте і цей метод потребує занадто багато ресурсів. Окрім того, якщо контент не змінюється і при цьому щоденно реєструють тисячі звернень до нього, то такий контроль стає просто зайвим. Тому такі країни, як Китай, застосовують пакетну фільтрацію в поєднанні з методами, які використовують її як джерело інформації для створення в автоматичному режимі правил, що визначають параметри блокування за IP чи URL.

Отже, окрім блокування обміну повідомленнями певного характеру, створюються і статичні правила заборони шкідливої інформації, які поширюються на весь трафік. Другий спосіб, спрямований на пом'якшення негативних наслідків такої ретельної перевірки, – створення паралельної інфраструктури, яка дозволить передавати контент кінцевому користувачеві у звичні терміни без затримки на його аналіз. І лише якщо при діючій інфраструктурі за результатами перевірки будуть виявлені заборонені терміни, можна буде

передати пакети TCP/IP щоб перервати з'єднання та не дозволити передачу забороненої інформації кінцевому користувачеві при з'єднанні з віртуальною приватною мережею (VPN) [8]. При організації такого з'єднання виникає безпечний кодований канал між кінцевим користувачем та віддаленим сервером, який знайде необхідний контент та надішле його у зворотному напрямку. За такої ситуації жоден із розташованих поруч вузлів не бачитиме фактичної інформації, яка проходитиме каналом VPN. Єдиний спосіб переконатися в тому, що для обходу механізмів фільтрації ця технологія недоцільна, полягає в тому, щоб перевіряти весь трафік та блокувати інформацію (у тому числі кодовані дані), яку не в змозі обробити обладнання фільтрації. Однак багато компаній використовують пакетну фільтрацію у своїй діяльності. Через це слід враховувати економічні наслідки застосування такої технології і той факт, що кодовану інформацію не фільтрують, оскільки більшість населення не має потрібних знань чи ресурсів, щоб кодувати відомості для обходу механізмів блокування контенту. На ринку комп'ютерних технологій є велика кількість різноманітних комерційних рішень з кодування інформації для нейтралізації механізмів контролю, що застосовуються органами державної влади. Зокрема, Tor і FreeNet – дві аналогічні прикладні програми, що використовуються для ухилення від механізмів фільтрації. Вони здатні приховати певні дії користувача так, щоб доступною була лише інформація про з'єднання з вузлом, який належить цим мережам, проте конкретних відомостей про отриманий контент у контролюючих підрозділів не буде.

1.5. *Зміна результатів пошуку*. Як варіант замість/окрім механізмів блокування доступу до інформації можна прописати команду видаляти протизаконний чи небажаний контент із результатів пошуку в Інтернеті. Як правило, такі відомості теж фільтрують за допомогою деяких зазначених нами методів, а мета видалення такого контенту полягає в тому, щоб приховати сам факт існування будь-якої цензури.

2. **Прозорість та інформація кінцевого користувача**. Слід розрізняти не лише методи перевірки контенту, але й країни, які намагаються забезпечити прозорість механізмів фільтрації та контролю, та країни, де маршрути запиту чи параметри фільтрації змінюються без пояснень. Так, у тому ж Китаї при блокуванні контенту користувач отримує технічне повідомлення про помилку на зразок «З'єднання неможливе» або «Час для з'єднання вийшов» [9].

Протилежний підхід застосовується, зокрема, у Саудівській Аравії, де, незважаючи на застосування фільтрації до значного за обсягами контенту, користувачу, окрім повідомлення про причини блокування інформації, пропонують механізми звернення до державних органів для перегляду правил заборон [10]. У будь-якому випадку повного «чорного списку» ресурсів, що підлягають фільтрації, не існує ані у відкритому, ані в обмеженому доступі для спеціальних органів влади, через що систему часто зламують із конкретною метою, наприклад для фільтрації сексуальних знімків неповнолітніх або для інших потреб, окрім прямої [11].

Отже, за останні кілька років органи державної влади різних країн суттєво активізували діяльність, спрямовану на фільтрацію web-контенту. Імовірно найближчим часом ця тенденція зберігатиметься, незважаючи на те, що механізми фільтрації може обійти навіть користувач, який має мінімальні знання. Фільтрація контенту стала останнім часом однією з основних тем, що активно обговорюються особами та організаціями, які виступають за більш жорстке регулювання Інтернету, і правозахисними організаціями, які виступають за збереження Інтернету в його первинному стані. Саме тому вітчизняні спеціалізовані підрозділи з боротьби з кіберзлочинністю та торгівлею людьми мають враховувати ці тенденції та напрацьовувати досвід зарубіжних країн із метою протидії цим злочинам, передусім поширенню дитячої порнографії мережею Інтернет.

Список використаної літератури

1. Сухаренко А. Детская порнография в Интернете – проблемы остаются [Электронный ресурс] / А. Сухаренко. – Режим доступа: http://www.crime-research.ru/news/17.04.2004/81.

2. Internet Filtering in the United Arab Emirates in 2004–2005: A Country Study [Электронный ресурс]. – Режим доступа: http://opennet.net/studies/uae.

3. Access Denied : The Practice and Policy of Global Internet Filtering [Электронный ресурс] / ed. by Ronald Deibert, John Palfrey, Rofal Rohozinski, Jonathan Zittrain. – Cambridge : MIT Press, 2008. – Режим доступа: http://opennet.net/accessdenied.

4. Green Dam Youth Escort – китайский веб-фильтр [Электронный ресурс]. – Режим доступа: http://www.oszone.net/9586/Green_Dam_Youth_Escort.

5. The German «Federal Trojan» – challenges between law and technology [Електронний ресурс]. – Режим доступу: http://www.teutas.it/societa-informazione/prova-elettronica/634-the-german-federal-trojan-challenges-between-law-and- technology-wiebke-abel-llm-university-of-edpean-uni.html.

6. Entwurf eines Gesetzes zur Bekämpfung der Kinderpornographie in Kommunikationsnetzen [Електронний ресурс]. – Режим доступу: http://dip21.bundestag.de/dip21/btd/16/128/1612850.pdf.

7. McAfee SmartFilter [Електронний ресурс]. – Режим доступу: http://www.bartec.kiev.ua/index.php/mcafee/188-mcafee-smartfilter.

8. Clayton R. Ignoring the Great Firewall of China [Електронний ресурс] / R. Clayton, S. J. Murdoch, R. Watson. – Режим доступу: http://petworkshop.org/2006/preproc/preproc_02.pdf.

9. Цензура и фильтрация Web [Электронный ресурс]. – Режим доступа: http://www.osp.ru/os/2010/04/13002405.

10. Internet Filtering in Saudi Arabia in 2004 [Електронний ресурс]. – Режим доступу: http://opennet.net/studies/saudi.

11. Wikileaks: Italian secret internet censorship list, 287 site subset, 21 Jun 2009 : [Електронний ресурс]. – Режим доступу: http://cyberlaw.org.uk/2009/06/29/wikileaks-italian-secret-internet-censorship-list-287-site-subset-21-jun-2009.

Надійшла до редколегії 28.05.2011

САНАКОЕВ Д. Б. ПРОТИВОДЕЙСТВИЕ ПОРНОГРАФИИ В ИНТЕРНЕТ ПОДРАЗДЕЛЕНИЯМИ ПО БОРЬБЕ С КИБЕРПРЕСТУПНОСТЬЮ И ТОРГОВЛЕЙ ЛЮДЬМИ

Рассмотрен порядок применения механизмов контроля доступа к web-контенту; исследованы технологии, типы фильтруемой информации, механизмы фильтрации. Даны предложения относительно возможностей осуществления органами внутренних дел контроля доступа к web-контенту.

SANAKOYEV D. COUNTERACTION TO PORNOGRAPHY ON THE INTERNET BY UNITS ON COMBATING CYBERCRIME AND HUMAN TRAFFICKING

The mechanisms of access control to web-content are considered; technologies, types of the filtered information, and also separate consequences of mechanisms filtration; represented suggestions in relation to possibility of internal affairs to manage access to web-content.

УДК 621.373.54

Г. Г. ГУБАРЄВ,
кандидат технічних наук, старший науковий співробітник,
доцент кафедри інформаційної безпеки
факулетету психології, менеджменту, соціальних та інформаційних технологій
Харківського національного університету внутрішніх справ

ЕНЕРГЕТИЧНИЙ КРИТЕРІЙ БЕЗПЕЧНОСТІ ЕЛЕКТРИЧНИХ РОЗРЯДІВ ТА ВИБІР ДОПУСТИМИХ ВИХІДНИХ ПАРАМЕТРІВ ЕЛЕКТРОШОКОВИХ ПРИСТРОЇВ[1]

Обґрунтовано енергетичний критерій несмертельності електричних розрядів, що діють на людей. Показано можливість визначення допустимих вихідних параметрів електрошокових пристроїв на основі цього критерію.

Проблема дослідження і оцінки впливу електрошокових пристроїв на організм людини – приклад ситуації, коли практика випереджає теорію, змушуючи проводити наукові дослідження після впровадження технічних пристроїв.

Аналогічна ситуація виникла в електротехніці та електроенергетиці стосовно питання оцінювання вражаючої дії електричних струмів промислової частоти на організм людини. Можна стверджувати, що тільки в другій половині XX ст. стала зрозумілою ситуація впливу електричних струмів промислової частоти на організм людини [1].

Такої чіткості дотепер немає стосовно дії імпульсних і короткочасних струмів, до яких належать і електрошокові пристрої [2; 3]. Зрозуміло, що поки не будуть визначені вражаючі фактори електричних розрядів і рівні впливу їх на організм людини, не можуть бути встановлені вимоги до допустимих вихідних параметрів

[1] Дана публікація є продовженням роботи автора, опублікованої у № 2 (34) журналу за 2010 рік, і ставить за мету ознайомити читача з проблематикою законодавчого врегулювання використання електрошокових пристроїв та необхідності створення національного закону «Про зброю» і державного стандарту «Електрошокові пристрої».