DOI https://doi.org/10.30525/978-9934-26-451-1-3

REGARDING THE STRENGTHENING OF CRIMINAL LIABILITY DURING MARTIAL LAW FOR CRIMINAL OFFENSES IN THE FIELD OF USE OF INFORMATION AND COMMUNICATION SYSTEMS

ЩОДО ПОСИЛЕННЯ КРИМІНАЛЬНОЇ ВІДПОВІДАЛЬНОСТІ ПІД ЧАС ДІЇ ВОЄННОГО СТАНУ ЗА КРИМІНАЛЬНІ ПРАВОПОРУШЕННЯ У СФЕРІ ВИКОРИСТАННЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ

Gorun O. Yu.
Chief researcher
Ukrainian Scientific and Research Institute of Special Equipment and Forensic Expertise of the Security Service of Ukraine
Kyiv, Ukraine

Горун О. Ю.
головний науковий співробітник
Український науково-дослідний інститут спеціальної техніки та судових експертиз Служби безпеки України
м. Київ, Україна

В умовах глобальної російської агресії, будь-яка держава вживає заходів з метою запобігання та недопущення масштабів поширення кіберзлочинності. Так, наприклад, американське законодавство жорстко карає кіберзлочинців, однак подальший розвиток міжнародної координації в цій сфері залишається нагальною потребою, особливо в умовах війни, яку веде РФ, у тому числі й в кіберпросторі. З огляду на позитивні здобутки кращого європейського та американського досвіду, Україна може істотно посилити свою протидію кіберзагрозам, особливо щодо тих, які поширює РФ. Це потребує комплексних зусиль як державних так і правоохоронних органів, потенціалу ІТ-сектору та громадянського суспільства.

Для отримання об'єктивної картини стану кібербезпеки Україні, необхідна єдина державна система виявлення, обліку та аналізу кіберінцидентів. Вона має включати базу даних про кіберзагрози, статистику кіберзлочинів, аналітичні звіти. Це дозволить виявляти найуразливіші місця кіберзахисту та своєчасно реагувати на загрози. В сучасних умовах чинні статті Кримінального кодексу, зокрема, Розділ XVI (Кримінальні правопорушення у сфері використання

електронно-обчислювальних машин, систем та комп`ютерних мереж і мереж електрозв`язку) прямо не встановлюють відповідальність за порушення законодавства у сфері реєстрів щодо користування даними реєстрів, допущення несанкціонованого розповсюдження та/або нецільове використання даних з обмеженим доступом.

Тому, є необхідність оптимізації вітчизняної правової системи кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та компьютерних мереж з метою впровадженням більш дієвих кримінально-правових механізмів протидії порушення роботи публічних електронних реєстрів, несанкціоноване втручання в їх роботу, несанкціоновані збут або розповсюдження інформації з обмеженим доступом, що створить належні гарантії для захисту суспільства, вітчизняного ринку, економіки держави та забезпечували б надійність і безпеку використання цифрових послуг.

Також Верховна Рада України 16 січня 2024 року прийняла в першому читанні за основу проект Закону України «Про внесення змін до Кримінального кодексу України щодо встановлення кримінальної відповідальності за несанкціоноване втручання, збут або розповсюдження інформації, що оброблюється в публічних електронних реєстрах та посилення кримінальної відповідальності під час дії воєнного стану за кримінальні правопорушення у сфері використання інформаційно-комунікаційних систем» (законопроект № 10242) [1]. Основні положення цього законопроекту спрямовані на посилення кримінальної відповідальності за правопорушення у сфері інформаційно-комунікаційних систем та електронних реєстрів, і зокрема це:

1. Встановлення кримінальної відповідальності за неправомірне втручання в роботу електронних реєстрів – внесення змін до ст. 361 КК України.

2. Запровадження кримінальної відповідальності за незаконне заволодіння та поширення інформації з обмеженим доступом з електронних реєстрів – внесення змін до ст. 361-2 КК України.

3. Посилення покарання за зазначені злочини, вчинені під час дії воєнного стану – внесення змін до ст. 361-1, 361-2, 362 КК України.

4. Встановлення суворіших санкцій за втручання в роботу електронних реєстрів і поширення конфіденційної інформації з них, вчинені службовими особами – внесення змін до ст. 361, 361-2 КК України.

5. Криміналізація дій щодо блокування та перешкоджання роботі інформаційно-комунікаційних систем і електронних реєстрів – внесення змін до ст. 363, 363-1 КК України.

6. Встановлення відповідальності за зловживання повноваженнями публічного реєстратора з корисливою метою – внесення змін до ст. 365-2 КК України.

7. Приведення законодавства про кримінальну відповідальність у відповідність до Закону України «Про публічні електронні реєстри».

8. Забезпечення ефективнішого кримінально-правового захисту електронних реєстрів та інших об`єктів критичної інформаційної інфраструктури.

9. Гармонізація національного законодавства з нормами міжнародного права у сфері кібербезпеки.

10. Посилення протидії кіберзлочинності та загрозам національній безпеці в інформаційній сфері.

Отже, прийняття цього законопроєкту сприятиме протидії факторам та масштабам поширення кіберзлочинності та забезпечить дотримання законності в кіберсфері. Цілком очікувано, що прискорення прийняття цього законопроекту дозволить встановити кримінальну відповідальність за несанкціоноване втручання, збут або розповсюдження інформації, що оброблюється в публічних електронних реєстрах та посилення кримінальної відповідальності під час дії воєнного стану за кримінальні правопорушення у сфері використання інформаційно-комунікаційних систем, розширить межі діяльності правоохоронних органів щодо розслідування кримінальних правопорушень, передбачених статями 361, 361-1, 361-2, 362 Кримінального кодексу України, а також підвищить гарантії захисту національної системи кібербезпеки у сучасному безпековому середовищі особливо в умовах правового режиму воєнного стану та активної фази кібервійни. Одночасно потребує посилення протидія російській кібер-агресії та загрозам державній національній безпеці в інформаційній сфері.

Література:

1. Про внесення змін до Кримінального кодексу України щодо встановлення кримінальної відповідальності за несанкціоноване втручання, збут або розповсюдження інформації, що оброблюється в публічних електронних реєстрах та посилення кримінальної відповідальності під час дії воєнного стану за кримінальні правопорушення у сфері використання інформаційно-комунікаційних

систем: проект Закону України від 16 січня 2024 року № 10242. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/43139

DOI https://doi.org/10.30525/978-9934-26-451-1-4

THE DIMENSIONS OF WAR: NATIONAL SUBJECTIVITY AGAINST THE "MYTH OF THE 21ST CENTURY"

ВИМІРИ ВІЙНИ: НАЦІОНАЛЬНА СУБ'ЄКТНІСТЬ ПРОТИ «МІФУ XXI СТОРІЧЧЯ»

Grabovska I. M.
Ph.D. in Philosophical Sciences,
Senior Researcher,
Senior Researcher
Research Institute of Ukrainian Studies
of Kyiv National University named after
Taras Shevchenko

Грабовська І. М.
кандидат філософських наук,
старший науковий співробітник,
старший науковий співробітник
Науково-дослідний інститут
українознавства Київського
національного університету
імені Тараса Шевченка

Hrabovsky S. I.
Ph.D. in Philosophical Sciences,
Senior Researcher,
Senior Researcher
H. Skovoroda Institute of Philosophy
of the National Academy
of Sciences of Ukraine
Kyiv, Ukraine

Грабовський С. І.
кандидат філософських наук,
старший науковий співробітник,
старший науковий співробітник
Інститут філософії Національної
академії наук України
імені Г. С. Сковороди
м. Київ, Україна

Одним із найважливіших вимірів російсько-української протистояння є той, що пов'язаний із національною суб'єктністю [1]. Філософська мода останніх десятиліть пов'язувала суб'єктність (у гіпертрофованому вигляді чи взагалі як таку) із тоталітаризмом як виявом доби Модерну. Проте це видається щонайменше непорозумінням. Адже тоталітаризм ґрунтується на поєднанні передусім техніко-технологічних здобутків модерну з зануренням соціуму в архаїку міжлюдських відносин, із позбавленням індивідів суб'єктності, із намаганням перетворити цих індивідів і соціальні спільноти на «ідеальних виконавців» (Б. Бательгейм) волі вождя, фюрера, дуче,