4. Хавронюк М.І. Військові злочини: коментар законодавства / М. І. Хавронюк, С. І. Дячук, М. І. Мельник; відп. ред. М. Д. Дрига, В. І. Кравченко. К. : СК, 2003. 272 с.

5. Бодаєвський В. П. «Воєнний стан», «бойова обстановка» та «час перебування на військовій службі» як особливі обставини чинності кримінального закону щодо військових злочинів у часі. *Ученые записки Таврического национального университета им. В. И. Вернадского.* 2013. Т. 25(64). № 2. С. 180–186. *Серия «Юридические науки».*

6. Злочини проти встановленого порядку несення військової служби (військові злочини) : навч. посіб. / Г. М. Анісімов, Ю. П. Дзюба, В. І. Касинюк та ін. ; за ред. М. І. Панова. Х. : Право, 2011. 184 с.

7. Дячук С. І. Злочини проти встановленого порядку несення військової служби (військові злочини): науково-практичний коментар до Кримінального кодексу України : у 3 кн. Київ, 2005. Кн. 3: Особлива частина. Коментарі до статей 255–447 Кримінального кодексу України. 584 с.

DOI https://doi.org/10.36059/978-966-397-395-1-26

ПРОТИДІЯ КІБЕРАТАКАМ В ПЕРІОД РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

Марчук Олександр Миколайович
здобувач освітньо-наукового рівня (доктор філософії),
Науково-дослідний інститут публічного права
м. Київ, Україна

Богатько Денис Олегович
здобувач освітньо-наукового рівня (доктор філософії),
Науково-дослідний інститут публічного права
м. Київ, Україна

Від початку війни стало відомо про велику кількість кібератак на Україну:

Варто згадати невдалу спробу атаки хакерського угруповання Strontium, які намагалися отримати доступ до комп'ютерних мереж в Україні, США та ЄС, щоб забезпечити тактичну підтримку фізичного вторгнення росії в Україну та викрасти конфіденційну інформацію.

До цього Держспецзв'язку попереджувало про розповсюдження електронних листів з назвою «Військові злочинці РФ.htm», відкриття

яких призводить до того, що зловмисники отримують віддалений доступ до комп'ютера жертви.

Під прицілом знаходяться також об'єкти критичної інфраструктури. Український провайдер Укртелеком зазнав потужної атаки 28 березня 2022 року, під час якої хакери намагались проаналізувати, як влаштована ІТ-інфраструктура, вивести з ладу обладнання та сервіси, а також отримати контроль над мережею та обладнанням компанії.

23 березня ворог намагався здійснити кібератаку на державні установи України з використанням шкідливої програми Cobalt Strike Beacon, яка уражає комп'ютер у випадку її відкриття.

Це приклади лише масованих атак. Ймовірно, про атаки менших масштабів та окремі випадки персональних зламів просто не повідомляється.

Кожна сучасна соціально активна людина в Україні використовує мобільні пристрої та користується інтернетом, державні органи переходять на електронний документообіг, стабільна діяльність банківського сектору, залізниці й авіатранспорту, великих підприємств залежить від стабільності кіберпростору, з яким вони працюють, та базується на комунікації за допомогою електронних засобів зв'язку.

Відповідальність за кіберзлочини передбачена розділом XVI ККУ, саме 2 норми із цього розділу і зазнали змін відповідно до нового Закону 2149-IX.

Також Закон 2149-IX передбачає, що втручання в роботу інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж не вважатиметься несанкціонованим, якщо таке втручання вчинено відповідно до Порядку пошуку та виявлення потенційних вразливостей таких систем чи мереж, текст якого Держспецзв'язку зараз активно напрацьовує.

Ще до початку війни, після кібератак 14 січня на сайти державних органів влади, відчувалася необхідність запровадження невідкладних змін в українському законодавстві для узаконення процедури Bug Bounty (залучення зовнішніх фахівців до пошуку помилок і вразливостей програмних продуктів, інформаційно-комунікаційних систем тощо). Тож на сьогодні ІТ-спільнота зможе легально тестувати державні інформаційні системи на наявність вразливостей, а держава отримає інструмент для значного підвищення ступеня захисту таких систем.

З іншого боку, запровадження ч. 6 ст. 361 ККУ є логічним продовженням змін у конструкції ч. 1 ст. 361 ККУ. Адже те, про що вказано у частині 6, раніше не визнавалося злочином відповідно до частини 1.

Електронна система публічних закупівель Prozorro заявила, що тимчасово призупиняє програму Bug Bounty у зв'язку з введенням воєнного стану в Україні до завершення воєнних подій. Незважаючи на припинення програми, дії багхантерів не будуть вважатися правопорушеннями, а нові звіти про знайдені вразливості будуть прийняті до розгляду після завершення воєнного стану та відновлення програми пошуку вразливостей Bug Bounty.

Варто визнати й певну неповноту закону в цій частині. Від початку війни в Україні активізувався неофіційний громадський рух кіберопору ворогові, так звана "КіберАрмія". Звичайні люди, поряд із професіоналами сфери ІТ, атакують ворога у кіберпросторі, завдаючи йому збитків та зриваючи плани. Формально такі дії можуть підпадати під ознаки складів злочинів, що передбачені ст. ст. 361, 361-1 ККУ. Ймовірно, що навіть при ініціюванні відповідного кримінального провадження проти таких осіб, правоохоронні органи та суди використовуватимуть загальні механізми їх звільнення від відповідальності, адже дії таких осіб відповідають інтересам України та українського народу та не є суспільно небезпечними. Незважаючи на це, формалізація подібного звільнення від відповідальності на рівні приміток чи окремих частин відповідних спеціальних статей ККУ є бажаною у майбутньому, аби правоохоронні органи не витрачали власних зусиль на "дружній вогонь" чи пошук юридичних шляхів його уникнення.

Отже підвищення ефективності боротьби з кіберзлочинністю під час війни та посилення відповідальності за відповідні злочини є давно назрілим кроком. Новий закон розширює межі діяльності правоохоронних органів щодо розслідування кіберзлочинів, передбачених статями 361, 361-1 ККУ. Посилення санкцій та додаткова криміналізація окремих діянь здатні частково стримати потенційних злочинців від вчинення нових злочинів.

Виправданим є й запровадження відповідальності за злочини, що скоєні у воєнний час. Настільки суворі санкції за їх вчинення продиктовані поточною ситуацією в країні, адже особа, яка завдає шкоди національним інтересам України чи українцям у кіберпросторі, тим самим допомагаючи агресору у цій війні, не може нести відповідальності меншої, ніж військові злочинці.

Сфера кіберпростору і раніше потребувала посиленого захисту та змін. Відкрите вторгнення росії стимулювало вдосконалення чинного законодавства та гарантій безпеки у сучасному інформаційному середовищі.

На підставі викладеного можемо констатувати, що під час війни в зоні ризику перебувають державні органи, великі підприємства, підприємства оборонної та критичної інфраструктури, а також

підприємства, які забезпечують населення та оборону усім необхідним в умовах війни. Є ризики й для місцевих жителів, які перебувають в зоні бойових дій.

Література:

1. Боротьба з кіберзлочинністю в умовах дії воєнного стану: Закон 2149-IX. – LigaZakon: сайт. URL: https://jurliga.ligazakon.net/analitycs/210562_borotba-z-kberzlochinnstyu-v-umovakh-d-vonnogo-stanu-zakon-2149-ix

2. Кримінальний кодекс України. – Законодавство України : сайт Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text

DOI https://doi.org/10.36059/978-966-397-395-1-27

РЕАЛІЗАЦІЯ ПРАВА НА ШЛЮБ У МІЖНАРОДНОМУ ПРИВАТНОМУ ПРАВІ: ОСОБЛИВОСТІ ТА ВИКЛИКИ

Мельник Олексій Сергійович
студент СО «Магістр»,
Науковий керівник: **Деркач Елла Михайлівна**
доктор юридичних наук, професор кафедри конституційного, міжнародного і кримінального права,
Донецький національний університет імені Василя Стуса
м. Вінниця, Україна

Одним з основних видів приватно-правових відносин з іноземним елементом, що регулюються міжнародним приватним правом, є шлюбно-сімейні відносини. В наш час глобалізаційних та міграційних процесів у різних країнах зазначені відносини зазнають постійної трансформації, що знаходить відображення в законодавстві, зокрема в Україні.

Наша держава гарантує захист соціальних прав громадян, у тому числі й права на шлюб, що обумовлює необхідність запровадження на законодавчому рівні ефективного механізму захисту зазначених прав.

У юридичній літературі питанням колізійного регулювання шлюбних і сімейних відносин приділено достатньо уваги таких науковців, як В. Гербута, О. Грабовської, А. Довгерта, О. Бурлай, О. Мережка, О. Розгон, М. Менджули, В. Ткаченко, О. Чумака, І. Шкурської та ін.

Важливим завданням міжнародно-правового врегулювання шлюбно-сімейних відносин є уніфікація правового регулювання у даній сфері.