СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ПРАВА

РЕФОРМУВАННЯ ПРАВОВОЇ СИСТЕМИ В КОНТЕКСТІ ЄВРОІНТЕГРАЦІЙНИХ ПРОЦЕСІВ

МАТЕРІАЛИ
VI Міжнародної науково-практичної конференції
(Суми, 19–20 травня 2022 року)

Суми
Сумський державний університет
2022

5. Антошкіна Л.І. Науково-методичні основи державного регулювання вищої освіти: автореф. дис. на здобуття наук. ступеня док. екон. наук спец. 08.02.03. «Організація управління, планування і регулювання економікою». Київ. 2006. 28 с.
6. Хомишин І.Ю. Адміністративно-правове регулювання освіти в Україні. *Науковий вісник публічного та приватного права.* № 2. 2016. С.189-193.
7. Національна стратегія розвитку освіти в Україні на період до 2021 року: Указ Президента України. Відомості Верховної Ради України. 2013. № 344/2013. URL: https://zakon.rada.gov.ua/laws/show/344/2013
8. Дідківська Л.І. Державне регулювання економіки: навч. посіб. Дідківська Л.І., Головко Л.С. *ЗнанняПрес*. Київ. 2002. 214 с.

ПЕРСПЕКТИВИ ВПРОВАДЖЕННЯ ІНСТИТУТУ ОФІЦЕРА З КІБЕРЗАХИСТУ В УКРАЇНІ

Малетов Д. В.
доктор філософії з права, викладач-стажист кафедри КПДС ННІ права Сумського державного університету
Ковтун А. А.
студентка ІІ курсу ННІ права Сумського державного університету

Збільшення кількості кіберзагроз на економічну соціальну складову нашої держави все актуальнішим робить питання оптимізації правового регулювання даної сфери. В світлі повномасштабної війни з Росією та євроінтеграційних процесів важливою для України є демонстрація того, що ми готові протистояти загрозам найстрімкіше зростаючому виду злочинності. Окрім того, в сучасних умовах важливою є готовність приймати необхідні зміни, що відповідатимуть стандартам, встановленим на європейському та світовому рівнях.

Явище «безпека» нерозривно пов’язане з поняттям «національні інтереси» і, можливо, в якомусь сенсі є похідним від нього, тому що, перш за все, функція національної безпеки – це забезпечення гарантій невразливості найголовніших інтересів національного суверенітету, територіальної цілісності держави, захисту населення – власне, тих інтересів, через які держава бореться і не погоджується на поступки. Національна безпека – це стратегія, необхідна для забезпечення інтересів держави [1,с. 37].

У науковій літературі відсутній єдиний усталений погляд на зміст поняття «кібербезпека».

Ряд дослідників на чолі з В.В. Остроуховим пропонують наступне авторське визначення «кібербезпеки» — це стан захищеності особи, держави і суспільства, при якому досягається інформаційний розвиток (технічний, інтелектуальний, соціально-політичний, морально-етичний), за якого сторонні інформаційні впливи не завдають їм суттєвої шкоди [2, с. 10].

В.М. Петрик тлумачить кібербезпеку як стан захищеності об'єктів (особистого, суспільства, держави, інформаційно-технічної інфраструктури), за якого досягається його нормальне функціонування незалежно від наявності внутрішніх і зовнішніх інформаційних впливів [3, с. 160–161].

Кібербезпека — це стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігається нанесення шкоди через:

- неповноту, невчасність та невірогідність інформації, що використовується;
- негативний інформаційний вплив;
- негативні наслідки застосування інформаційних технологій;
- несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [4].

Джерелами загроз та викликів національній безпеці України в інформаційній сфері можуть бути міжнародні злочинні групи хакерів, окремі підготовлені у сфері ІТ злочинці, іноземні державні органи, терористичні угруповання, недержавні організації, політичні структури та неформальні об'єднання екстремістського спрямування, транснаціональні корпорації та фінансово-промислові групи тощо. Зростає загроза використання проти інтересів України кібернетичних засобів як із середини держави, так і з-за меж її кордонів. Такою ж реальною є загроза використання української інформаційної інфраструктури як «транзитного майданчику» для приховування атаки на інформаційні ресурси третьої сторони, що може розцінюватись провідними країнами як дії держави з відповідними наслідками політичного, економічного, правового, а в перспективі, не виключено, і воєнного характеру [5].

Одним із прикладів кібератак на теренах України є те, що у січні 2022 року на одному з "чорних" онлайн-ринків з'явилося оголошення про продаж особистих даних двох мільйонів українців, які нібито зберігались сервісом "Дія". Міністерство цифрової трансформації заперечує "злив" даних та стверджує, що вони надійно захищені.

У ніч з 13 на 14 січня хакери атакували урядові сайти. Також станом на 8 ранку був тимчасово недоступний портал "Дія". Водночас витоку даних українців не було, заявили в Держспецзв'язку.

Окрім того у ніч проти 14 січня хакери масово атакували українські урядові сайти, зокрема вебресурси МОН, МЗС, Мінмолодьспорту, Міненерго, Мінагрополітики, Мінветеранів, Мінекології, ДСНС та Держказначейства.

За інформацією СБУ, загалом було атаковано понад 70 державних вебсайтів, 10 з яких зазнали несанкціонованого втручання. Контент сайтів при цьому змінено не було, а витоку персональних даних не відбулося [6].

«В ніч проти 26 січня на офіційний сайт України Ukraine.ua здійснено кібератаку. Внаслідок атаки сайт протягом кількох годин був недоступний для користувачів», - зазначають у зовнішньополітичному відомстві [6].

Проте атака на портал «Дія», що відбулась у січні, була не єдиною. На портал «Дія» ввечері 15 лютого вчинено потужну DDoS-атаку, яку вдалося відбити - для користувачів вона залишилася непомітною.

Окрім того 15 лютого DDoS-атак зазнали сайти Міністерства оборони та Збройних сил України. Були також зафіксовані перебої в роботі вебсервісів державних Ощадбанку і ПриватБанку.

Зараз на тлі повномасштабного вторгнення російських військ в Україну та через інформаційну війну, яка відбувається проти України такі новини сприймаються особливо гостро. Асиметричну відсіч країні-агресору можуть дати кібервійська, які слід було створити ще на початку гібридної агресії.

З початку повномасштабної агресії з боку Росії оперативно виявлено та нейтралізовано більше 120 потужних кібератак на ресурси органів державної влади та військового управління України.

«Найбільша їх кількість припала на ніч вторгнення – саме тоді ворог хотів знищити весь кіберзахист України. Втім ефективна робота СБУ та інших органів кібербезпеки не дозволила агресору використати кіберпростір для отримання військових переваг», – сказав речник СБУ Артем Дехтяренко у відеоповідомленні [7].

За місяць війни вже сталося майже втричі більше різного виду хакерських атак, ніж за аналогічний період минулого року.

Попри зростання кількості хакерських атак, більшість з них «безуспішні та майже не впливають на роботу критичної інформаційної інфраструктури», запевнили у відомстві.

Як зазначає голова Держспецзв’язку Юрій Щиголь, атакують передусім державні установи, фінансовий, оборонний сектор, операторів зв'язку, місцеві органи влади, логістичні компанії, медіа.

Враховуючи всі кібератаки, Державна служба спеціального зв’язку та захисту інформації пропонує створити посаду офіцера з кіберзахисту в усіх органах держвлади та

на усіх об’єктах критичної інфраструктури після нещодавньої кібератаки на державні сайти.

24 січня 2022 року голова Держспецзв’язку Юрій Щиголь на брифінгу повідомив: «з метою покращення системи кібербезпеки у державі було прийнято рішення щодо невідкладного внесення законодавчих змін, спрямованих на узаконення так званого багбаунті, або розкриття вразливості органів держвлади, шляхом внесення змін до Кримінального кодексу в частині статей 361 та 361^{-1}, введення в органах державної влади та на об’єктах критичної інфраструктури посад офіцерів з кіберзахисту» [8].

Офіцери кіберзахисту будуть підпорядковуватись службі захисту інформації. Їхня зарплата має бути не нижче за ринкову. Щиголь наголосив, що це основна проблема, бо відповідні фахівці не мають відповідного забезпечення.

Також вирішили створити можливості для заохочення співробітників, що виконують адміністрування ІТ-систем для держорганів. При цьому збільшать і відповідальність працівників за невиконання вимог з кіберзахисту в органах державної влади [9].

24 березня 2022 року Верховна Рада ухвалила Закон «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану».

Зміни були внесені до статтей 360 та 361^{-1}. Зокрема, стаття 361 Кримінального кодексу України викладається в новій редакції, згідно з якою розмежовується ступінь відповідальності за несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж залежно від спричинених наслідків, а також посилюються санкції за вчинення відповідного кримінального правопорушення [10].

Водночас вказана стаття передбачає, що втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, не вважається несанкціонованим, якщо таке втручання вчинено відповідно до Порядку пошуку та виявлення потенційних вразливостей таких систем чи мереж.

Окрім того, посилюються санкції за вчинення кримінального правопорушення, передбаченого статтею 361^{-1} Кримінального кодексу України.

Отже, 24 січня 2022 року голова Держспецзв’язку Юрій Щиголь на брифінгу повідомив, що до Кримінального Кодексу України будуть внесені зміни у сфері кібербезпеки, а також про плани створення посади офіцера кібербезпеки. Проте план, який був висвітлений 24 січня 2022 року Юрієм Щиголем на брифінзі, виконано лише

наполовину. І поки що неможливо сказати, коли буде запроваджено таку посаду як офіцер з кіберпезпеки.

ЛІТЕРАТУРА:

1. Ліпкан В. А., Ліпкан О. С. Національна і міжнародна безпека у визначеннях та поняттях. навч.посіб. Вид 2-ге, перероб. і допов. Київ. 2018. 400 с.

2. Калюжний Р.А. Інформаційне забезпечення управлінської діяльності в умовах інформатизації: організаційно-правові питання теорії і практики: підручник для студ. вищ. навч. закл. Київ: Академія державно-податкової служби України, 2002. 296 с.

3. Калюжний Р.В. Питання концепції реформування інформаційного законодавства України. Збірник «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні». Київ: НТУУ «КПІ», Міносвіти і науки України, СБУ. Київ, 2000. С. 17–21.

4. Проект Національної стратегії у сфері прав людини станом на 25 березня 2015 року. URL: http://old.minjust. gov.ua/file/44709 (дата звернення: 03 квітня 2022 року)

5. Косогов О. М. Пріоритетні напрямки державної політики щодо забезпечення безпеки національного кіберпростору. Збірник наукових праць Харківського університету Повітряних Сил. 2014. Вип. 3. С. 127–130.

6. На офіційний сайт України здійснили кібератаку. 26 січня 2022 року. URL: https://www.ukrinform.ua/rubric-technology/3392214-na-oficijnij-sajt-ukraini-zdijsnili-kiberataku-mzs.html (дата звернення: 03 квітня 2022 року).

7. У ніч вторгнення росіяни хотіли знищити весь кіберзахист України. 02 квітня 2022 року. URL: https://www.ukrinform.ua/rubric-technology/3446588-u-nic-vtorgnenna-rosiani-hotili-znisiti-ves-kiberzahist-ukraini-sbu.html (дата звернення: 03 квітня 2022 року).

8. Атака на держсайти: до всіх відомств хочуть приставити офіцера з кіберзахисту. 24 січня 2022 року. URL: https://www.pravda.com.ua/news/2022/01/24/7321548/ (дата звернення: 05 квітня 2022 року).

9. В Україні з'явиться нова посада "офіцера кіберзахисту" – для цього змінюватимуть закон. 24 січня 2022 року. URL: https://24tv.ua/ukrayini-zyavitsya-nova-posada-ofitsera-kiberzahistu-ukrayina-novini_n1850247 (дата звернення: 05 квітня 2022 року).

10. Рада посилила спроможності національної системи кібербезпеки. 24 березня 2022 року. URL: https://www.ukrinform.ua/rubric-technology/3438840-rada-posilila-spromoznosti-nacionalnoi-sistemi-kiberbezpeki.html (дата звернення: 05 квітня 2022 року).