Право і суспільство. 2016. № 4. С. 221–224. URL: http://nbuv.gov.ua/UJRN/Pis_2016_4_39.

2. Комарницька О., Прядко В. Установлення місцезнаходження засобу радіоелектронного зв'язку: підготовка та проведення негласної слідчої (розшукової) дії. Вісник Національної академії прокуратури України. 2014. № 2. С. 71–78. URL: http://nbuv.gov.ua/UJRN/Vnapu_2014_2_14

3. Кримінальний процесуальний кодекс України: Науково-практичний коментар. У 2 т. Том 1. О. М. Бандурка, Є. М. Блажівський, Є. П. Бурдоль та ін. ; за заг. ред. В. Я. Тація, В. П. Пшонки, А. В. Портнова. Харків. Право, 2012. 768 с.

4. Бобрицький Л. В. Практичні аспекти застосування кримінального процесуального законодавства України щодо установлення місцезнаходження радіоелектронного засобу. Боротьба з організованою злочинністю і корупцією (теорія і практика). 2013. № 3(спец. вип.). С. 155–160. URL: http://nbuv.gov.ua/UJRN/boz_2013_3(spets.

5. Луцик В. В. Установлення місцезнаходження радіоелектронного засобу. Юридичний науковий електронний журнал. № 4. 2014. С. 199– 202.

УДК 004.05

ВІТАЛІЙ АНАТОЛІЙОВИЧ СВІТЛИЧНИЙ
кандидат технічних наук, доцент, доцент кафедри інформаційних технологій та кібербезпеки Харківського національного університету внутрішніх справ

КІБЕРБЕЗПЕКА УКРАЇНИ ТА ОСОБЛИВОСТІ КІБЕРЗЛОЧИНІВ

Відповідно до законодавства України, кібербезпека – це захищеність життєво важливих інтересів людини й громадянина, суспільства та держави у процесі використання кіберпростору, яка забезпечує сталий розвиток інформаційного суспільства і цифрового комунікативного середовища, своєчасне виявлення, запобігання та нейтралізацію реальних і потенційних загроз національній безпеці України у кіберпросторі (ст. п. 5 ч. 1 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України»). У глобальному розумінні, кібербезпекою є реалізація заходів із захисту мереж, програмних продуктів та систем від цифрових атак.

В державі на законодавчому рівні приймаються відповідні закони та нормативні акти, які регулюють відносини в цій сфері. Станом на 2019 р. до правової основи кібербезпеки України входять такі нормативно-правові акти: Конституція України, Кримінальний кодекс України, закони України «Про основні засади забезпечення кібербезпеки України», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основи національної безпеки» та інші закони, Доктрина інформаційної безпеки України, Конвенція Ради Європи про кіберзлочинність та інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України.

Аналіз першопричин кіберзлочинів призводить до цілої низки системних проблем у галузі, ігнорувати які з кожним наступним інцидентом стає дедалі важче. Одна з головних – неефективна нормативна база та система управління.

Так, наприклад закон України "Про захист інформації в інформаційно-телекомунікаційних системах" та серія нормативних документів про технічний захист інформації на теперішній час є безнадійно застарілі. Більше того, вони зобов'язують органи державної влади, об'єкти критичної інфраструктури та приватні компанії, які хочуть надавати послуги державним органам (наприклад, Інтернет-провайдери), впроваджувати Комплексну систему захисту інформації, яка окрім того, що морально застаріла, впродовж багатьох років довела свою неефективність.

Відповідно до Конвенції про кіберзлочинність, яка є частиною українського законодавства з 11.10.2005 р., кіберзлочини умовно поділяються на чотири види.

До першого виду належать правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем. До цього виду кіберзлочинів можна віднести всі злочини, спрямовані проти комп’ютерних систем і даних (наприклад, навмисний доступ до комп'ютерної системи або її частини; навмисне пошкодження, знищення, погіршення, зміна або приховування комп'ютерної інформації; навмисне вчинення, не маючи на це права, виготовлення, продажу, придбання для використання, розповсюдження або надання для використання іншим чином пристроїв, включаючи комп'ютерні програми).

До другого виду кіберзлочинів належать правопорушення, пов'язані з комп'ютерами. Такі злочини характеризуються умисним діянням, що призводить до втрати майна іншої особи шляхом будь-якого введення, зміни, знищення чи приховування комп'ютерних даних або будь-якого втручання у функціонування комп'ютерної системи, з шахрайською або нечесною метою набуття, не маючи на це права, економічних переваг для себе чи іншої особи.

Третій вид кіберзлочинів охоплює правопорушення, пов'язані зі змістом (контентом), що полягає у здійсненні умисних незаконних дій щодо вироблення, пропонування або надання доступу, розповсюдження дитячої порнографії, а також володіння такими файлами у своїй системі.

Четвертим видом є умисні дії, пов'язані з порушенням авторських та суміжних прав, відповідно до вимог Бернської Конвенції про захист літературних і художніх творів, Угоди про торговельні аспекти прав інтелектуальної власності та Угоди ВОІВ про авторське право, а також національного законодавства України.

Існують також інші класифікації кіберзлочинів, проте запропонована конвенцією є найбільш популярною. В Україні політика щодо кібербезпеки покладається на низку державних органів, а саме на Державну службу спеціального зв'язку та захисту інформації України, Національну поліцію України, Службу безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи,

Національний банк України. В кожному із зазначених органів діють відповідні підрозділи. Але при цьому кожна людина що використовує кіберпростір грає певну роль в забезпеченні своєї кібербезпеки кіберпростору, включаючи пристрої та мережі, які вона використовує.

УДК 351.741:343.45:342.721
ПЕТРО СЕРГІЙОВИЧ КЛІМУШИН
кандидат технічних наук, доцент, доцент кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ
ЄЛИЗАВЕТА ГЕОРГІЇВНА БЄЛЯЄВА
курсант 4 курсу факультету № 4 Харківського національного університету внутрішніх справ

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Одним із напрямків розвитку України є підвищення захисту персональних даних та забезпечення прав осіб на недоторканність приватного життя. Захист основоположних прав і свобод людини щодо обробки персональних даних безпосередньо впливає на авторитет держави, зокрема, її здатність реалізовувати ефективну внутрішню і зовнішню політику в галузі прав людини. Як показує практика, процес гармонізації національного законодавства у сфері захисту персональних даних є складним, тому повинен бути безперервним і слідувати постійним змінам, які відбуваються в цій області. В даний час кожен володілець та розпорядник персональних даних визначає власну політику безпеки щодо обробки даних, яка має відповідати вимогам законодавства [2].

У 2015 році був прийнятий Закон України «Про Національну поліцію», який передбачає повноваження поліції в безпрецедентному масштабі формувати і використовувати інформаційні ресурси (бази даних). Сучасні інформаційні технології та законодавство відкривають можливості для правоохоронних органів обробляти величезний обсяг персональних даних. Проте, з огляду на численні переваги цих технологій, слід визнати, що при несанкціонованому їх використанні (без дотримання вимог закону), це може призвести до серйозних наслідків [3].

Серед поширених порушень можна виділити [1]:

– Доступ до персональних даних за відсутності повноважень, законної підстави і обґрунтованої мети такого доступу.

– На практиці поширеними є випадки, коли працівники підрозділів з протидії наркозлочинності масово витребовують з медичних закладів дані щодо осіб, які стоять на обліку як такі для формування баз даних про цих осіб. Суспільство так і не отримало відповідь, яка мета і законна підстава збирати інформацію про здоров‘я людини, яка не вичинила правопорушення.