

1. Штанько В. І. Віртуалізація і мережева реальність: проблеми і соціальні наслідки / В. І. Штанько // Вісник Національного технічного університету «ХПІ». Серія: Актуальні проблеми розвитку українського суспільства. – 2017. – № 52. – С. 94-99.

2. Palfrey John, Gasser Urs. Born Digital. Understanding the first generation of digital natives. N.Y., 2008. 375 p.

II СЕКЦІЯ: ПРАВОВІ АСПЕКТИ БЕЗПЕКИ І ЗАХИСТУ ІНФОРМАЦІЇ У ЦИФРОВОМУ ПРОСТОРІ

Бородай Анжеліка Едуардівна

студентка 4 курсу Маріупольського державного університету

КІБЕРЗЛОЧИННІСТЬ ЯК ПРОБЛЕМА ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА УКРАЇНИ

Зараз ми проживаємо у тотальній діджиталізації та розвитку інформаційних технологій, де все більш важливого значення набуває інформація. В наш час, коли життя без зв'язку здається неможливим, коли весь світ перетворився на одну глобальну мережу та коли Інтернет дає нескінченність можливостей, важливо пам'ятати про безпеку та дбати про свій захист у мережі, щоб не виникало проблем. Тому що саме через Всесвітню мережу черпаємо інформацію для навчання, шукаємо розваги, купуємо різноманітні товари, оплачуємо безліч послуг та ділимося майже всіма аспектами свого життя.

За законом України «Про основні засади забезпечення кібербезпеки України», кіберзлочин – це суспільно небезпечне винне діяння в кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про

м. Одеса, 25 березня 2022 р.

Матеріали Всеукраїнського круглого столу
«Трансформація українського суспільства в цифрову еру»

кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України. У Кримінальному кодексі України ці злочини закріплено в розд. 16 «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» [1]. У сфері інформаційних технологій можна визначити, що ситуація з кіберзлочинністю набуває все більшої загрози для суспільства.

Питання кіберзлочинності є надзвичайно важливим на державному рівні. Найчастіше під ударами кібератак опиняються об'єкти критичної інфраструктури: енергетичні об'єкти, транспорт та банківський сектор. У 2017 році в Україні відбулася масштабна атака вірусом Petya: були уражені енергетичні компанії, українські банки, аеропорт «Бориспіль», аеропорт Харкова, Чорнобильська АЕС, урядові сайти, київський метрополітен тощо. Такого безпрецедентного масштабного вторгнення в сервери вітчизняних компаній наша країна ще не зазнавала. За даними експертів Міжнародного валютного фонду, економічні втрати від атаки вірусу Petya становили майже 850 млн доларів. Водночас заяви постраждалих компаній до кіберполіції про втрату даних часто залишались без відповіді, адже знайти та притягти до відповідальності зловмисника в цьому разі виявилось неможливо [2].

Організована злочинність дедалі частіше використовує Інтернет з метою приховання своєї діяльності. Зараз нікого не здивує існуванням мережі Darknet, за допомогою якої злочинці фактично створили чорний ринок для збуту наркотиків, зброї, крадених товарів тощо. Завдяки технологіям, які забезпечують мережеву анонімність, ця частина Інтернету залишається абсолютно

м. Одеса, 25 березня 2022 р.

безконтрольною, а тому безпечною для діяльності різноманітних злочинних угруповань.

Основними види таких злочинів перш за все є: незаконний доступ, незаконне перехоплення, втручання у дані, зловживання пристроями, шахрайство, пов'язане із комп'ютерами, правопорушення, пов'язані з дитячою порнографією тощо. Кібершахраї використовують старі схеми обману довірливих громадян, яким повідомляють, що їхні знайомі потрапили до халепи й терміново необхідні гроші, щоб їм допомогти. Теж досить часто кіберзлочинці протиправно отримують доступ до особистої переписки, фото або відео, а потім за доступ чи видалення вимагають гроші. Нерідко кіберзлочиною є також цифрове піратство, тобто встановлення та користування неліцензійного програмного забезпечення, завантаження та перегляд фільмів і серіалів із піратських сайтів. Традиційно популярним методом кібершахрайських дій є створення фальшивих сайтів відомих інтернет-магазинів, брендів, фінансових установ, де користувачі через заповнення певних форм повідомляють свої персональні дані та паролі від банківських карток. Наприклад, тепер на тлі інтересу довкола криптовалютного ринку мають попит фальшиві сайти купівлі-продажу й обміну криптовалют.

У зв'язку з вищесказаним, не варто забувати про власну інформаційну безпеку. Перше і головне правило – відповідально ставитися до публікації і передачі будь-яких персональних даних: ім'я та прізвище, дата та місце народження, сімейний стан, паспортні дані, професія тощо. Разом із тим, паролі та аккаунти не являються персональними даними, адже не несуть ніякої конкретної інформації про особу. Але можуть бути використані у скоєнні віртуальних злочинів. Також експерти радять видаляти геолокації з ваших

м. Одеса, 25 березня 2022 р.

Матеріали Всеукраїнського круглого столу
«Трансформація українського суспільства в цифрову еру»

особистих постів задля забезпечення власного захисту. Прикріпляти до свого персонального, а тим паче до бізнес-аккаунту, мобільний номер телефону – звичайна практика, досить зручна та розповсюджена. Проте, і тут є певні небезпеки, адже номер телефону може посприяти злому персональної сторінки для використання облікового запису. Не варто ділитися фотографіями своїх посадкових талонів в аеропорту, світлинами паспорту чи водійських прав. Нікому не передавайте ваші паролі від облікових записів. Безкоштовні мережі в кафе чи кінотеатрах є чудовою можливістю для зловмисників. Програми, які дозволяють слідкувати за вами, є у вільному доступі. Тож важливі операції краще проводити лише за перевіреного з'єднання з Інтернетом. Не варто скачувати додатки із неперевіраних джерел, якщо скачувати програми із сумнівних джерел – ми самі наражаємось на небезпеку. Завжди перевіряйте правильність адреси веб-сайтів, на яких ви виконуєте якісь фінансові операції або вводите конфіденційну інформацію. Дотримання даних правил допоможе уникнути або мінімізувати можливість бути об'єктом уваги кіберзлочинності [3].

Можна зробити висновок, що кіберзлочинність на сьогодні становить безпеку не тільки для держави, а й для суспільства. Вирішення цієї проблеми потребує більше фахівців зі спеціальних знань та сучасних методів виявлення комп'ютерних злочинів.

Список використаних джерел

1. Кримінальний кодекс України від 05.04.2001 р. URL: <http://zakon3.rada.gov.ua/laws/show/2341-14>.
2. Гуцалюк М. Інтернет: протидія кримінальним проявам та боротьба зі злочинністю. URL: <http://www.lawyer.org.ua/?w=r&i=10&d=500>.
3. Кавуненко Т. Безпека в Інтернеті: як захистити себе і не стати жертвою зловмисників? URL:

м. Одеса, 25 березня 2022 р.

Матеріали Всеукраїнського круглого столу
«Трансформація українського суспільства в цифрову еру»

<https://agentyzmin.org.ua/news/bezpeka-v-interneti-iaak-zakhystyty-sebe-i-ne-staty-zhertvoiu-zlovmysnykiv/>.

Євченко Роман Ігорович

аспірант кафедри політичних наук і права ДЗ
«Південноукраїнський національний педагогічний університет
імені К.Д.Ушинського»

ФЕНОМЕН ЛОБІЗМУ В ПРОЦЕСАХ ВРЕГУЛЮВАННЯ ПОЛІТИЧНИХ КОНФЛІКТІВ

Для розуміння функціонування розвинених демократій та шляхів врегулювання політичних конфліктів залишається вирішальним розуміння систем груп інтересів та нормативно-правового регулювання їх діяльності, але для академічних досліджень в політичній науці ця тема поки що залишається нішевою. Вивчення політики груп інтересів – тобто організації, агрегації, артикуляції та посередництва суспільних інтересів, які прагнуть формувати державну політику – є відносно невеликою галуззю політології. Тим не менш, протягом останніх п'ятнадцяти років академічний інтерес до цієї тематики зростає, на що вказує стан сучасної літератури, в Україні, зокрема – це публікації В. Нестеровича, М. Недюхи, М. Федоріна, М. Росенко, присвячені аналізу нормативно-правового регулювання лобізму в країнах розвиненої демократії [1; 2; 3]; І. Слюсаренко, який досліджує етнічні «найсистемні та найпотужніші» лобі в Україні, що здійснюється в межах «публічної дипломатії» [4]; публікації «українців за кордоном» - Т. Кузьо та О. Дейчаківського щодо дієздатності «українського лобі в США» [19]. Звичайно, що західна література з цього питання є більш предметною, містить емпіричні якісні та

м. Одеса, 25 березня 2022 р.

Матеріали Всеукраїнського круглого столу
«Трансформація українського суспільства в цифрову еру»