Кіберзлочинність, як сучасний виклик захисту персональних даних.

1. Законодавство з питань регулювання та встановлення кримінальної відповідальності за кіберзлочини
2. Основні види кіберзлочинів в сфері захисту персональних даних.
3. Кримінальна та адміністративна відповідальність за порушення у сфері захисту персональних даних
4. Кібератаки на інформаційно-телекомунікаційну інфраструктуру держави, як один з видів кібертероризму.

Законодавство з питань регулювання та встановлення кримінальної відповідальності за кіберзлочини

Неоднорідність легального закріплення складів криміналь- них правопорушень, пов'язаних із використанням інформаційно – телекомунікаційних технологій, у законодавстві різних держав актуалізує проблему уніфікації правового регулювання таких відносин на міжнародному рівні. Відправною точкою в цьому питанні має бути теза про відсутність державних кордонів для цього виду кримінальних правопорушень. Робота щодо здійснення правового регулювання в цьому напрямку ведеться на універсальному, міждержавному та регіональному рівнях. Завдяки ратифікації державами учасницями, міжнародних договорів, встановлюються єдині правила міжнародного співробітництва в сфері протидії злочинності з використанням інформаційно – телекомунікаційних технологій.

Міжнародні договори, підписані державами, що їх підписали, встановлюють єдину основу для юрисдикції та правил міжнародного співробітництва між державами у боротьбі зі злочинністю шляхом використання комп'ютерних технологій.

Відомо, що Рада Європи докладає значних зусиль щодо уніфікації законодавства держав – учасниць у сфері правового регулювання кримінальних правопорушень у кіберпросторі.

Історично першим нормативним актом Ради Європи, з питань регулювання криміналь- ної відповідальності за кримінальні правопорушення, вчинені шляхом використання інформаційно – телекомунікаційних технологій виступала Рекомендація від 13 вересня 1989 No 89 (9) «Про кримінальні правопорушення, які пов'язані з комп'ютером».

Відповідно до зазначеного документа, держави – учасниці Ради Європи, повинні при роз- робці свого національного законодавства, прийняти о уваги Звіт Європейського комітета по проблемам злочинності, пов'язаної з комп'ютерами. В рамках цього Звіту Комітет дав оцінку, самому явищу комп'ютерної злочинності, та надав рекомендації щодо тих видів кримінальних правопорушень у кіберпросторі, які держави – учасниці повинні криміналізувати.

Зауважимо, що даний нормативний акт носив лише рекомендаційний, характер, однак саме після його прийняття почався процес фактичного створення кримінального законодавства держав – учасниць в розрізі регулювання відносин за вчинення кримінальних правопо- рушень у кіберпросторі.

Звіт дає певну класифікацію кримінальним правопорушенням, які держави учасниці повинні криміналізувати, так зокрема, виділяється список мінімально необхідних до введення в національне законодавство та додаткових (необов'язкових).

В свою чергу до мінімальних Рекомендація Ради Європи відносить:
1) Комп'ютерне шахрайство;
2) Комп'ютерну фальсифікацію;
3) Завдання шкоди комп'ютерним даним або комп'ютерними програмам;
4) Комп'ютерний саботаж;

5) Несанкціонований доступ до цифрового пристрою;
6) Несанкціонований перехват цифрової інформації;
7) Несанкціоноване відтворення цифрової інформації;
8) Несанкціоноване використання мікросхем.
Одночасно з цим Рекомендація надавала необов'язковий до криміналізації перелік складів кримінального правопорушення, зокрема:
1) Неправомірна зміна даних та програмного коду в комп'ютері;
2) Комп'ютерне шпигунство;
3) Неправомірне використання комп'ютера;
4) Несанкціоноване використання комп'ютерної програми.
Незважаючи на те, що нормативний акт носив рекомендаційний характер, низька європейський держав, поклала його в основу створення своєї національної системи по боротьбі з кримінальними правопорушеннями у кіберпросторі.

Наступним документом, який по праву можна назвати основоположним у питаннях регулювання кримінальної відповідальності за вчинення кримінальних правопорушень у кіберпросторі є Будапештська Конвенція «Про кіберзлочинність». Конвенція містить норми статей матеріального права, щодо зобов'язання держав ратифікантів імплементувати у національні законодавства зазначених норм.

Норми конвенції містять у собі спробу нормативного регулювання трьох основних блоків питань:

– уніфікація правового закріплення кримінальних правопорушень у сфері комп'ютерної інформації у національних законодавствах країн.

– зближення національних кримінально-процесуальних норм.

– регламентація міжнародного співробітництва щодо запобігання та розслідування комп'ютерних злочинів.

Текст цієї Конвенції відкритий для підписання та ратифікації для усіх держав – учасниць Ради Європи, зокрема Україна ратифікувала конвенцію 7 вересня 2005 року, а вже в 9 червня 2006 набрала чинності.

Конвенція містить перелік основних видів комп'ютерних правопорушень, що розкриває їх дефініції, та встановлює заходи відповідальності за їх вчинення, які слід включити до національного законодавства держав – ратифікантів Конвенції. Закріплені у Конвенції склади кримінальних правопорушень розділені на чотири групи відповідно до об'єкта зазіхання:

1. правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем;

2. правопорушення, пов'язані з комп'ютерами;
3. правопорушення, пов'язані зі змістом;
4. правопорушення, пов'язані з порушенням авторських та суміжних прав.
Крім того, 28 січня 2003 Додатковим протоколом до Конвенції «Про кіберзлочинність»

було визначено норму направлену на боротьбу з розповсюдженням через комп’ютерні мережі інформації расистського і ксенофобського характеру.

Кожна із закріплених у Конвенції груп містить типові ознаки кримінальних правопорушень, які необхідно закріпити у національному законодавстві держав – учасниць Конвенції.

Так, перша група правопорушень проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, включає в себе наступні види суспільно небезпечних діянь:

1) незаконний доступ
2)нелегальне перехоплення
3) втручання у дані
4) втручання у систему
5) зловживання пристроями

Зауважимо, що всі зазначені суспільно небезпечні діяння, які вчиняються у кіберпросторі, закріпленні в рамках XVI розділу Особливої частини Кримінального кодексу України в рам- ках статей 361–362. Питання виникає лише, при тлумаченні такої форми вчинення кримінального правопорушення, як нелегальне перехоплення. Зазначимо, що в Кримінальному кодексі України, діяння у формі перехоплення цифрової інформації регламентоване в частині 2 статті 362 Особливої частини Кримінального кодексу України, однак лише щодо спеціального суб’єкта такого правопорушення. Одночасно, в частині 3 статті 361 Особливої частини Кримінального кодексу України визначаються наслідки у формі порушення процесу маршрутизації цифрової інформації.

Зауважимо, що в доктринальних джерелах такі суспільно небезпечні дії прирівнюються і розглядаються, як синоніми. Однак, на нашу думку порушення процесу маршрутизації це дії спрямовані на цифровий вплив щодо інформації, яка передається, в кінцевому результаті, така інформація просто змією адресата. В свою чергу, перехоплення, це процес отримання

такої інформації без подальшого її копіювання, а результатом буде лише процес ознайомлення з нею.

До правопорушень, пов'язаних з комп'ютерами, Конвенція відносить:
1. шахрайство пов’язане з комп’ютером
2. підробка пов’язана з комп’ютерами
Відповідно до часини 3 статті 190 Особливої частини Кримінального кодексу України,

шахрайство вчинене шляхом незаконних операцій з використанням електронно – обчислювальної техніки. З одного боку можемо констатувати факт, імплементації норм Конвенції до Кримінального кодексу України, але з іншого, спостерігаємо проблеми правової кваліфікації такого суспільно небезпечного діяння, вчиненого шляхом використання інформаційно – телекомунікаційних технологій.

Відповідно до даних офіційного веб – ресурсу Департаменту кіберполіції Національної поліції України, фактично всі діяння, які вчиняються у кіберпросторі, шляхом використання інформаційно – телекомунікаційних технологій, систем або мереж, розглядаються Департаментом Кіберполіції, як шахрайство за частиною 3 статті 190 Особливої частини Криміналь- ного кодексу України (Офіційний веб – сайт Департаменту кіберполіції Національної по- ліції України, 2023). Однак, при розгляді, справ щодо встановлення вини особи у вчиненні кримінального правопорушення регламентованого частиною 3 статті 190 Особливої частини Кримінального кодексу України, суді перекваліфіковують зазначені суспільно небезпечні дії на 1 частину зазначеної статті, мотивуючи це тим, що обман при вчиненні цього кримінального правопорушення може виразитись у застосуванні програмних засобів, які дають змогу винному будь-яким чином (шляхом

відшукання випадкових цифр, паролів тощо) здійснити несанкціонований доступ до інформації, яка зберігається чи обробляється в автоматизованих системах, щоб ввести в оману автоматизовану систему і видати себе за того, хто має право в ній працювати і здійснювати відповідні операції.

Фактично позиція суду збігається з формулюванням комп'ютерного шахрайства передбаченого Конвенцією «Про кіберзлочинність». На нашу думку, об'єктом обману може виступати лише фізична особа, а не інформаційно – телекомунікаційна технологія, тому у випадку наприклад «фішингу», діяння варто кваліфікувати за сукупністю статей 190 та 361, 361-1 Особливої частини Кримінального кодексу України.

Щодо питання встановлення кримінальної відповідальності за підробку пов'язану з комп'ютером, то тут варто зазначити, що кримінальний закон України, не містить спеціальної норми, яка встановлювала відповідальність за таке діяння, виходячи зі змісту Конвенції. Однак, норми статті 200 Особливої частини Кримінального кодексу України встановлюють кримінальну відповідальність за відробку платіжних банківських карт, підробка яких у будь якому випадку буде пов'язана з тим чи іншим елементом інформаційно – телекомунікацій- ної техніки. Одночасно, з цим вважаємо за необхідне закріпити спеціальні норми, в кримінальному законі нашої держави (Кримінальний кодекс України, 2001).

Стаття 9 та 10 Конвенції «Про кіберзлочинність», визначає правопорушення пов'язані з дитячою порнографією та з порушенням авторських та суміжних прав. Криміналізації такі суспільно небезпечні діяння набули в статтях 177, 161, 300, 442 Особливої частини Кримінального кодексу України. Однак, самі елементи інформаційно –

телекомунікаційних технологій, систем та мереж не визначаються, які такі що підвищують суспільну небезпечність діяння при їх застосуванні.

Враховуючи, що конвенція зобов’язує не просто криміналізувати суспільно небезпечні діяння, які у ній визначені, а зробити при цьому акцент саме на використання елементів інформаційно – телекомунікаційних технологій, систем та мереж при вчиненні зазначених кримінальних правопорушень.

Крім того, норми Конвенції зобов'язують держави – учасниці. кваліфікувати як кримінально протиправні дії підбурювання до скоєння будь-якого з вищедосліджених кримінальних правопорушень, співучасть у ньому, або замах.

При цьому встановлення відповідальності за підбурювання та співучасть є обов'язком держави-підписанта Конвенції, а криміналізація замаху є правом.

Примітно закріплення у Конвенції необхідності залучення до кримінальної відповідальності юридичних. Відповідно до статті 12 Конвенції, корпоративна відповідальність реалізується за вчинення передбаченого Конвенцією кримінального правопорушення щодо юридичної особи фізичною особою чи членом органу управління юридичної особи.

Аналізуючи норми регламентовані Конвенцією «Про кіберзлочинність», можемо зробити висновок, що Конвенція, незважаючи на різноманітність закріплених в ній норм, встановлює лише загальні положення та аспекти, які регламентують відповідальність за кримінальні правопорушення, які вчиняються шляхом використання інформаційно – телекомунікаційних технологій, систем або мереж. Як результат, в рамках

імплементації зазначених норм Конвенції в рамках вітчизняного законодавства, потребується суттєві доповнення та уточнення, зокрема в частині приміток до відповідних статей Особливої частини Кримінального кодексу України. Разом з тим вважаємо, що процес імплементації норм Конвенції «Про кіберзлочинність» у вітчизняне законодавство України пройшов успішно, хоча і потребує виділення в окремих кримінальних правопорушеннях кваліфікаційних ознак, які б визначали підвищену ступінь суспільної небезпеки за вчинення кримінальних правопорушень у кіберпросторі.

Основні види кіберзлочинів в сфері захисту персональних даних.

В наш час кіберзлочинність вийшла з-під контролю правоохоронних органів однієї держави та стала значною міждержавною і транснаціональною проблемою.

Активне використання комп'ютерних технологій практично у всіх сферах суспільного життя, стало невід'ємною частиною сучасності. Можна наголосити, що 21 століття – є століттям диджиталізації, цифрових та інформаційних технологій.

Ще декілька десятиліть назад про кримінальні правопорушення в сфері комп'ютерної інформації було дуже мало згадок, однак за короткий проміжок часу, дані кримінальні правопорушення почали нести не лише окрему загрозу для осіб чи суспільства, а й для держав в цілому. Більш того проблема розвитку злочинності в сфері комп'ютерної інформації стоїть найбільш гостро, оскільки наслідки несвоєчасного реагування на таку загрозу набагато небезпечніші ніж в більшості інших кримінальних правопорушеннях.

Наразі кримінальні правопорушення в сфері комп'ютерної інформації охоплюють фактично всі сфери життя суспільства, починаючи від банківської сфери, закінчуючи національною безпекою держави.

Аналізуючи правовий аспект злочинів які вчиняються за допомогою електронно обчислювальних машин, варто зауважити, що поняття злочину в сфері комп'ютерної інформації та злочину який скоється за допомогою комп'ютерних технологій не є ідентичними поняттями. На нашу думку кримінальні правопорушення у сфері комп'ютерної інформації варто розглядати як один з підвидів злочинів з використанням комп'ютерних технологій.

Суспільна небезпека злочинів в сфері комп'ютерної інформації полягає у тому, що неправомірний доступ до комп'ютерної інформації може шкодити діяльності різноманітних систем державної оборони, банківського сектору, систем муніципальної діяльності. Так само різного типу дії щодо спотворення достовірності інформації можуть привести як до проблем загальнонаціонального характеру так і заподіяти шкоду правам та інтересам окремої особи.

В перше поняття «злочин в сфері комп'ютерної інформації» було використане в 60-х роках 20 століття, саме тоді були виявлені перші злочини з використанням електронно обчислювальних машин.

Сьогодні немає єдиного визначення, що слід розуміти під злочинами в сфері комп'ютерної інформації. Зокрема Боглов В.М. під злочинами в сфері комп'ютерної інформації розуміє передбачене кримінальним законодавством противоправне, винне порушення чужих прав та інтересів щодо автоматизованих систем обробки даних, повноцінного впливу, що підлягають правовій охороні майнових прав та інтересів, громадської та державної безпеки.

Миколенко О.М. під злочинами в сфері комп'ютерної інформації розуміє заборонені кримінальним законом суспільно – небезпечні умисні,

винні та противоправні діяння, які спрямовані на порушення недоторканості комп’ютерної інформації, яка охороняється законом та її матеріальних носіїв, що завдають шкоду правам та інтересам окремих осіб та державної та громадської безпеки.

Погорецький М.В. злочини в сфері комп’ютерної інформації визначає як навмисні суспільно небезпечні діяння, які заподіюють шкоду або створюють загрозу заподіяння шкоди суспільним відносинам, що регулює безпечне виробництво, зберігання, використання або поширення інформації або інформаційних ресурсів.

Голубєв В.О. під даними злочинами розуміє передбачені законом про кримінальну відповідальність винне, суспільно небезпечне діяння скоєне задля порушення цілісності, конфіденційності, достовірності та доступності охоронюваної законом цифрової інформації».

Амелін О. М. вважає, що в юридичному сенсі злочини в сфері комп’ютерної інформації як особлива група злочинів не існують, але при цьому підкреслює, що багато традиційних видів злочинів удосконалилися в результаті залучення коштів обчислювальної техніки, і, отже, можна говорити лише про комп'ютерні аспекти злочинів без виділення їх в окрему групу.

Юртаєва К. В. під поняттям злочин в сфері комп’ютерної інформації розуміє передбачені кримінальним законом винні суспільно небезпечні діяння, спрямовані на порушення недоторканності охоронюваної законом електронної інформації та її матеріальних носіїв, що здійснюються у процесі створення, використання та розповсюдження електронної інформації, а також спрямовані на порушення роботи ЕОМ, системи ЕОМ або їх мережі, що завдають шкоди законним інтересам власників або власників, життя здоров'ю, правам та свободам людини та громадянина, національній безпеці.

Пропонуємо під злочинами в сфері комп'ютерної інформації розуміти умисні суспільно небезпечні, протиправні, винні діяння, що посягають та заподіюють шкоду суспільним відносинам які регламентують порядок зберігання, розповсюдження, використання інформації та їх захист.

<u>Злочини у сфері використання платіжних систем.</u>

В кримінальному законодавстві України, як і в науковій літературі, немає поняття злочинів у сфері використання платіжних систем, більшість науковців розглядають такі злочини як злочини в фінансовій та банківських сферах, або злочини в сфері забезпечення фінансової та банківської інформації. Злочини в сфері комп'ютерної інформації в сфері використання платіжних систем є одним з видів кіберзлочинів. В Україні цей вид шахрайства поступово набуває масового характеру. Зокрема, одним з таких злочинів є скімінг.

Скімінг - крадіжка даних карти за допомогою спеціального пристрою – скімера.

Загалом варто розділяти скімінг на 2 види:

- Фізичний скімінг. Зловмисники копіюють всю інформацію з магнітної смуги картки (ім'я власника, номер картки, термін закінчення терміну її дії, CVV- та CVC-код), дізнатися про ПІН-код можна за допомогою міні-камери або накладок на клавіатуру, встановлених на банкоматах. Стати жертвою скіммінгу можна не лише знімаючи готівку, а й оплачуючи покупки у торгових точках. Для копіювання даних офіціанти, касири, службовці готелів використовують переносні скімери або пристрої, прикріплені до терміналу.
- Програмний скімінг. Полягає у встановленні зловмисниками на банкомат певного шкідливого програмного забезпечення яке буде здійснювати копіювання магнітної стрічки картки, ссв коду та дати дії картки, та подальше надіслання таких даних на сервери зловмисників.

Приват банк України, наголошує, що наразі використовуються так звані антискімінгові накладки, які значно знижують ризик встановлення скімерів на банкомати. Крім того спеціалісти відділу кібербезпеки приват банку рекомендують використовувати чіпові картки, які мають значно вищий рівень захисту, оскільки інформація яка міститься у чіпі має захист криптографічного характеру який унеможливлює його компрометування.

Ще одним з підвидів злочинів у сфері платіжних систем є кардинг. Кардинг це незаконні фінансові операції з використанням платіжних карток та електронних платіжних систем, які не були підтвердженні або ініційовані володільцем карти або електронного гаманця. Реквізити платіжних карток беруть як правило з різноманітних сервісів даркнету. Вартість електронного гаманця чи пластикової картки варіюється від 2 до 300 доларів, це залежить від країни володільця карти чи електронного гаманця, кількості грошових коштів на них, типу картки (бизнес, корпоративна, золота), банку який випустив картку.

Зловмисник маючи картку чи електронний гаманець може використати кошти які на них знаходяться, на товари електронної комерції в інтернеті, поповнити номер телефону з подальшим переведенням в готівкову форму, купувати техніку в онлайн магазинах з подальшим їх продажом. Найпопулярнішим способом використання таких карт є покупка товарів на різних маркетплейсах у самого себе, такий спосіб на відміну від інших дає можливість використати весь баланс картки, по – перше без посередників, а по – друге без комісії з подальшим перепродажем куплених товарів.

Схожим с кардингом виступає ще один злочин в сфері платіжних систем, Enroll можна назвати певним предикатним злочином щодо деяких направлень у кардингу, а саме Enroll це процедура за допомогою якої зловмисник отримує, або створює новий доступ до онлайн банкінгу жертви. Після отримання доступу до онлайн банкікгу жертви, зловмисник суттєво

спрощує процедуру підтвердження транзакції (навіть дуже підозрілої) оскільки підтвердження можна зробити в самому онлайн банкінгу.

Кеш – трепінг викрадення готівки з банкомату шляхом встановлення на шатер банкомату спеціальної утримуючої накладки.

Для здійснення такого злочинного дійства злочинці закривають отвір для видачі грошей в банкоматі спеціальною накладкою (планкою) з липкою стрічкою з іншої сторони. Таким чином, при проведенні громадянами операцій по зняттю готівки здійснюється захват купюр – грош прилипають до скотчу, що перешкоджає їх видачі законому власнику карти. В більшості випадків користувач банкомата, не отримавши гроші грошей, вирішує, що в його роботі виник збій чи закінчилася готівка і йде не підозрюючи про факт шахрайства. Після цього, шахраї підходять і забирають готівку.

Шахрайства сфері комп'ютерної інформації.

Фішинг є інноваційним видом шахрайства в мережі інтернет, метою якого виступає можливість заволодіти персональними даними, банківськими реквізитами, реквізитами електронних платіжних систем та крипто гаманців та дані від електронних кабінетів інтернет магазинів, з подальшим продажом таких даних або з використанням таких даних на власний розсуд.

Варто зазначити, що фішингові веб сайти дуже складно розпізнати на їх оригінальність. Фішингові веб-сайти повністю копіюють оригінальні веб-сайти, відмінність становитиме лише адресу доменного імені, який не привертає увагу непідготовленого громадянина з причини незначної відмінності у буквах чи цифрах. Як приклад можна згадати приклад крипто веб- сайту MyEtherWallet.com, кіберзлочиниці за допомогою фішингового сайту викрали близько 700000 доларів за декілька днів. Зловмисники скопіювали оригінал веб сайту та присвоїли йому доменне ім'я

myetherwaIlet.com і таким способом викрадали приватні ключі які відповідають за доступ до адресів ETH і ETC.

Суспільно небезпечний характер фішингу обумовлений передусім прямою фінансовою шкодою та породженням кризовою довіри до фінансових операцій які здійснюються в інтернеті. Через витрати обумовлені фішинговими атаками, багато з фінансових та банківських інститутів, відмовляються від оплати та покладають усю відповідальність на клієнта. У широкому сенсі фішинг підриває маркетинговий імідж компанії або фінансової установи і сильно впливають на її загальний імідж, завдає сильного удару по електронній комерції.

Пересічному інтернет-користувачу розпізнати фішинг-атаку буває досить складно через його довірливість і погану обізнаність з методами і тактиками фішингу, які постійно оновлюються (спам дедалі частіше поєднується зі зловмисним програмним забезпеченням).

На нашу думку можна виділити 3 основні види фішингу

- Масовий фішинг. Зазначений вид фішингу передбачає використання зловмисниками спам емейл листів, веб-сайтів, підроблених рекламних банерах та пуш повідомлень, які адресовані великій кількості людей. Як правило жертвами такого виду фішингу стають клієнти банків і тд. Основною ознакою такого виду фішинга є те, що він не передбачає виявлення заздалегідь конкретних жертв, оскільки адресати фішингової атаки беруться з випадкових отриманих баз даних.
- Цільовий фішинг. Найбільш небезпечним видом фішингу є саме цільовий фішинг який спрямований на цільову аудиторію, стосовно якої спеціально збирається інформація аби зробити адресоване їй послання більш переконливим. Для даного виду фішинга характерні наступні етапи: планування, підготовка, атака, збір, шахрайство, стадія завершення. На стадії планування зловмисник проводить певну розвідку щодо жертви або групи жертв, підбирає вразливі місця та робить їх аналіз. Стадія підготовки

характеризується складанням фішингового листа, або створення фішингово веб – сайту та розробка засобів атаки. На стадії атаки зловмисник відправляє фішинговий лист або шкідливе програмне забезпечення. Наступною стадією є збір інформації шкідливим програмним забезпеченням та наступний аналіз зібраної інформації. Стадія шахрайства характеризується продажом зібраної інформації, шантажем. На кінцевій стадії зловмисник ліквідує докази та замітає сліди.

- Корпоративний фішинг. Характеризується у створенні веб-сайтів, які ззовні повністю є копією оригіналу однак мають іншу адресу домену. Такі веб – сайти вузько визначають клас жертв фішерів. Основною метою фішерів є те щоб жертва сприйняла підроблений веб- сайт як легальний і надала інформацію про особисті данні.Мета шахрая полягає або в отриманні доступу до захищеного сайту, або в маскуванні його справжньої особи. При цьому шахрай може викрасти адресу жертви, фальсифікуючи інформацію про маршрутизацію повідомлення, щоб здавалося, що воно прийшло з акаунта жертви замість його власного.

Шахрайство в сфері проведення інтернет аукціонів. З поміж усіх видів інтернет шахрайств у сфері комп'ютерної інформації, інтернет аукціони стоять на перших місцях. Переважно на інтернет аукціонах виставляють міфічні лоти, коли за картинкою та описом на екрані монітора стоїть неіснуюча річ. За допомогою інтернет аукціонів довірливі покупці готові витрачати тисячі доларів за фіктивний лот. Процедура шахрайських дій полягає у тому, що товар виставляється за нижчою ціною від побібного роду товарів, але не настільки щоб жертва що – небуть запідозрила.

Використання фіктивних суб'єктів електронної комерції. Досить поширений вид шахрайства, представлений одно сторінковими веб - сайтами з унікальною ціновою пропозицією на будь-якій товар. Як правило, фіктивні Інтернет-магазини працюють за частковою або

стовідсотковою передоплаті. Відповідно, жертва, здійснивши переказ коштів, не отримує необхідного товару. Далі сайт блокується, і згодом "переїжджає" на інший хостинг або змінює доменне ім'я та продовжує свою протиправну діяльність. Такий сайт може бути наповнений великим кількістю фальшивих відгуків з метою створення образу доброчесного Інтернет-магазину та введення в оману потенційних жертв. Такий вид шахрайства є одним із самих простих методів здійснення злочинної діяльності в мережі Інтернет і завдає великої шкоди щодо фінансової спроможності слабо захищених та необізнаних громадян з урахуванням низького рівня їхньої інформаційної грамотності.

<u>Злочини у сфері інтелектуальної власності</u>

- Інтернет піратство. В законі США про авторське право надається визначення інтернет піратство, а саме - використання інтернету для незаконного копіювання і / або поширення програмного забезпечення.Основною метою інтернет піратства є одержання прибутку від такої діяльності. У мережі інтернет інтернет пірати можуть отримувати прибуток від надання платного доступу до матеріалів які знаходяться в закритому доступі або є платними за ціною значно нижчою від ціни яку пропонує автор. Також інтернет пірати можуть надавати доступ до авторських матеріалів на безкоштовній основі, а прибуток отримувати за рахунок реклами на ресурсі де розміщені піратські матеріали, або взагалі інтегрувати рекламу безпосередньо в піратські матеріали. В найгіршому випадку піратські файли можуть містити вірусні програми, як результат отримання персональних даних які зловмисник може використовувати на свій розсуд. На нашу думку інтернет піратство це використання інтернет простору для незаконного копіювання, злому та розповсюдження видеоконтенту, аудіоконтенту, літературних творів, програмного забезпечення та інших видів цифрової продукції, яка розміщена в інтернет

мережі для подальшого розповсюдження як на платній так і безоплатній основі.

Одним з видів злочинів у сфері інтелектуальної власності є кардшарінг. Кардшарінгом називають надання незаконного доступу до перегляду
супутникового та кабельного TV.

<u>Злочини у сфері інформаційної безпеки.</u>

Для злочинів в сфері інформаційної безпеки характерними є наступні ознаки: неоднорідність об’єкта посягання(на практиці маємо, що об’єктом злочинів у сфері інформаційної безпеки є не тільки комп’ютерна інформація, а й національна безпека держави, громадська безпека, економічна сфера), використання комп’ютера в якості як предмета так і способу вчинення злочину, використання комп’ютерної інформації в якості як засобу вчинення злочину так і в якості об’єкта злочину.

Створення, розповсюдження та продаж шкідливого програмного забезпечення як правило виступають у сукупності такого виду злочину в сфері комп’ютерної інформації. Йдеться перш за все свідоме створення та застосування такого програмного забезпечення за допомогою якого допускається: блокування, знищення, модифікація комп’ютерної інформації, копіювання даних які охороняються.

Прикладами подібного роду проєктів можуть виступати, віруси локери, віруси трояни, віруси кліпери, віруси стилери, віруси кейлогери. Віруси локери або як їх ще називають мальваре це віруси які при потраплянні на комп’ютер або телефон повністю блокують систему, натомість на екрані девайсу жертви вискакує повідомлення про необхідність переведення певною суми грошових коштів, як правило у криптовалюті для зняття блокування системи девайсу. Однак навіть після

оплати зловмиснику грошових коштів і отримання паролю для розблокування, система девайсу жертви повністю само знищується.

Віруси кліпери це вид вірусів який підмінює картковий або електронний рахунок жертви, на рахунок зловмисника і при переведенні грошових коштів жертва фактично переводить гроші зловмиснику.

Віруси стілери це такий вид вірусів які крадуть інформацію з вашого браузера і роблять на сервері зловмисника відбиток браузера жертви. З такими даними зловмисник може з легкістю використовувати весь спектр інформації яка міститься у браузері жертви, починаючи від дій у соціальних мережах закінчуючи купівлею товарів за рахунок жертви.

Підроблення комп'ютерної інформації. Створення, зміна, знищення, приховування комп'ютерних даних чи комп'ютерних програм або інше втручання в хід обробки даних різними способами, або створення таких умов, які згідно з національним законодавством будуть становити таке правопорушення, як підробка в традиційному розумінні цього значення.

Пошкодження комп'ютерних даних чи даних комп'ютерних програм. Несанкціоноване знищення, пошкодження, погіршення комп'ютерних даних чи комп'ютерних програм.

Зміна комп'ютерних даних чи даних комп'ютерних програм Несанкціонована зміна комп'ютерних даних або комп'ютерних програм.

Комп'ютерне шпигунство. Придбання з використанням протиправних засобів або шляхом несанкціонованого розкриття, передавання або використання торгівельної або комерційної таємниці з метою заподіяння економічного збитку особі, яка має право на таємницю, або отримання незаконної економічної переваги для себе або третьої особи.

Протиправне використання захищеної інформації.

Використання захищеної законом комп'ютерної програми без дозволу або її незаконне відтворення з метою отримання економічної

вигоди для себе або третьої особи, або з наміром заподіяти шкоду законному власнику програми.

Кримінальні правопорушення в сфері комп’ютерної інформації, на сьогодні виступають одним з найбільш небезпечних видів кримінальних правопорушень у кіберпросторі, як результат заподіяння фінансової шкоди як, окремим суб’єктам кіберпростору, так і державам в цілому, тим самим становлять загрозу міжнародній та національній безпеці у кіберпросторі.

Кримінальна та адміністративна відповідальність за порушення у сфері захисту персональних даних

Згідно зі статтею 182 Кримінального кодексу України, "Порушення недоторканності приватного життя", особи, які вчиняють незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу, або незаконно змінюють таку інформацію, підлягають штрафу від п'ятисот до однієї тисячі неоподатковуваних мінімумів доходів громадян, або виправним роботам на строк до двох років, або арешту на строк до шести місяців, або обмеженню волі на строк до трьох років. У випадках повторного вчинення або якщо ці дії призводять до істотної шкоди правам, свободам та інтересам особи, кара може включати арешт на строк від трьох до шести місяців, обмеження волі на строк від трьох до п'яти років, або позбавлення волі на той самий строк.

Важливо відзначити, що практика застосування цієї статті практично відсутня в Єдиному державному реєстрі судових рішень. Серед обмеженого числа рішень, які були прийняті за цією статтею, можна вказати вироки у справах, пов'язаних з незаконною передачею конфіденційної інформації

третім особам та незаконним збором і зберіганням персональних даних. Варто зауважити, що цей стан справ може бути зумовлений відсутністю відповідних рішень у реєстрі чи труднощами у пошуку. Однак, ймовірніше, що дане положення насправді рідко використовується національними органами влади, що свідчить про його фактичну неактивність.

Адміністративна відповідальність за порушення у сфері обробки та захисту персональних даних встановлена ст. 188-39 Кодексу України про адміністративні правопорушення (надалі – КупАП). Вказаним положенням передбачено відповідальність за:

1) неповідомлення або несвоєчасне повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних або про зміну відомостей, які підлягають повідомленню згідно із законом, повідомлення неповних чи недостовірних відомостей;

2) невиконання законних вимог (приписів) Уповноваженого Верховної Ради України з прав людини або визначених ним посадових осіб секретаріату Уповноваженого Верховної Ради України з прав людини щодо запобігання або усунення порушень законодавства про захист персональних даних;

3) недодержання встановленого законодавством про захист персональних даних порядку захисту персональних даних, що призвело до незаконного доступу до них або порушення прав суб’єкта персональних даних.

Також передбачено відповідальність за повторне скоєння цих порушень. Щодо санкцій, вони передбачають штраф у розмірі від ста до двох тисяч неоподатковуваних мінімумів доходів громадян. Якщо йдеться про частину першу статті 188-39 Кодексу України про адміністративні правопорушення (КУпАП), обов'язок повідомляти Уповноваженого про обробку персональних даних передбачено статтею 9 Закону. Згідно з цим положенням, володільник персональних даних повідомляє

Уповноваженого про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, протягом тридцяти робочих днів з дня початку такої обробки.

Такі види обробки були визначені Уповноваженим наказом від 8 січня 2014 року № 1/02-14, яким затверджено Порядок повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, про структурний підрозділ або відповідальну особу, що організовує роботу, пов'язану із захистом персональних даних при їх обробці, а також оприлюднення вказаної інформації.

На сьогодні випадків притягнення до адміністративної відповідальності за неповідомлення Уповноваженого не зафіксовано. Повний брак правопорушень такого характеру вкрай малоймовірний. Здається, що вказане положення КУпАП на практиці не працює.

Загалом частини 1 та 2 статті 188-39 КУпАП є досить однозначними та чіткими, не вимагаючи додаткових роз'яснень. Варто відзначити, що ці положення передбачають відповідальність за порушення лише незначних аспектів законодавства про захист персональних даних, головним чином, порушення обов'язків володільців перед Уповноваженим. Однак жодне з цих положень не передбачає відповідальності за порушення правил обробки та захисту персональних даних, які є ключовим предметом правового регулювання Закону.

У цій частині законодавець запровадив ч. 4 ст. 188-39 КУПАП. Вказаним положенням передбачено відповідальність за порушення, скоєні в ході власне обробки / захисту персональних даних. У зв’язку з цим, а також з огляду на деяку складність викладу вказаної частини ст. 188-39 КУПАП, видається необхідним детальніше її проаналізувати. З об’єктивної сторони вказане положення містить два елементи, пов’язані причиново-наслідковим зв’язком:

1) недодержання встановленого законодавством про захист персональних даних порядку захисту персональних даних;

2) незаконний доступ до них або порушення прав суб'єкта персональних даних. Щодо першого, слід наголосити, що в законодавстві нема не лише означення понять «захист персональних даних» та «порядок захисту персональних даних», а й будь-яких вимог щодо того, яким критеріям повинен відповідати такий захист. Єдине, що передбачено Законом в цій частині, – це обов'язок забезпечити «захист даних» (ст. 24 Закону).

Можна припустити, що розглядається загальний обов'язок володільця вживати організаційних та технічних заходів для запобігання випадковій втраті або знищенню, незаконній обробці, зокрема незаконному знищенню чи доступу до персональних даних. З іншого боку, може йтися про обов'язок кожного працівника не розголошувати персональні дані, які стали відомі у зв'язку з виконанням професійних, службових чи трудових обов'язків. Однак перед тим, як робити висновки про дієвість цих положень законодавства, важливо проаналізувати практику їх застосування.

З врахуванням практики, яка сформувалася в результаті розгляду судами протоколів про адміністративні порушення, можна стверджувати, що поняття «встановленого законодавством про захист персональних даних порядку захисту персональних даних» тлумачиться досить широко та охоплює будь-які дії, що становлять порушення Закону (див. детальніше нижче). Загалом тлумаченню цього поняття судовими рішеннями не приділяється особливої уваги, зазвичай вони автоматично приймають таку позицію. Тому варто розглянути можливість введення в Кодекс адміністративних правопорушень та Закон про захист персональних даних певних базових вимог щодо якості та рівня такого захисту (достатність, адекватність, пропорційність тощо), обов'язку вживати заходів для

визначення необхідного рівня захисту (проводити діагностику систем захисту, визначення ризиків, пов’язаних з обробкою тощо) і т.д.

Отже, попри широкий, на перший погляд, характер вказаного положення, сфера його дії доволі вузька. Натомість, самі по собі порушення окремих найвагоміших положень Закону можуть (і повинні) кваліфікуватись як окремі правопорушення у сфері законодавства про захист персональних даних. Як приклад, можна навести:

- неповідомлення суб’єкта про збір персональних даних,
- незаконну обробку (і зокрема поширення) персональних даних, яка не пов’язана з порушенням порядку захисту,
- обробку персональних даних на підставі згоди з порушенням основних вимог, що ставляться до неї (поінформованість, добровільність, наявність документів, що підтверджують її надання),
- відмову в наданні доступу суб’єктові до його персональних даних, надання неповних відомостей чи надання відповіді з порушенням визначених Законом строків,
- ненадання відомостей щодо порядку обробки персональних даних,
- ненадання відомостей про порядок доступу до персональних даних,
- брак обліку операцій, пов’язаних з обробкою персональних даних,
- відмову змінити/видалити персональні дані, що не відповідають дійсності, непризначення відповідальної особи,
- нечітке визначення її обов’язків, порушення умов щодо призначення розпорядника тощо.

Можна припустити, що розглядається загальний обов’язок володільця вживати організаційних та технічних заходів для запобігання

випадковій втраті або знищенню, незаконній обробці, зокрема незаконному знищенню чи доступу до персональних даних. З іншого боку, може йтися про обов'язок кожного працівника не розголошувати персональні дані, які стали відомі у зв'язку з виконанням професійних, службових чи трудових обов'язків. Однак перед тим, як робити висновки про дієвість цих положень законодавства, важливо проаналізувати практику їх застосування.

З врахуванням практики, яка сформувалася в результаті розгляду судами протоколів про адміністративні порушення, можна стверджувати, що поняття «встановленого законодавством про захист персональних даних порядку захисту персональних даних» тлумачиться досить широко та охоплює будь-які дії, що становлять порушення Закону (див. детальніше нижче). Загалом тлумаченню цього поняття судовими рішеннями не приділяється особливої уваги, зазвичай вони автоматично приймають таку позицію. Тому варто розглянути можливість введення в Кодекс адміністративних правопорушень та Закон про захист персональних даних певних базових вимог щодо якості та рівня такого захисту (достатність, адекватність, пропорційність тощо), обов'язку вживати заходів для визначення необхідного рівня захисту (проводити діагностику систем захисту, визначення ризиків, пов'язаних з обробкою тощо) і т.д.

Підсумовуючи, можна констатувати, що протягом усього шляху розвитку українського законодавства про захист персональних даних його орієнтирами були саме європейські стандарти, які містяться в документах і міжнародних договорах Ради Європи та ЄС. Водночас у чинному законодавстві України про захист персональних даних міститься ціла низка прогалин і розбіжностей. Особливо показова, у цьому контексті ситуація з положеннями законодавства України, які регламентують питання відповідальності за порушення стандартів захисту персональних даних. До основних проблем, які існують у зв'язку з цим, можна віднести: 1) брак у законодавстві України повноцінного означення поняття «захист

персональних даних» / критеріїв, яким повинен відповідати такий захист / вимог щодо визначення володільцем і розпорядником рівня такого захисту; 2) розмитість фактичних підстав відповідальності за порушення в ході обробки персональних даних; 3) недостатність винятково адміністративного стягнення як засобу покарання за порушення стандартів захисту персональних даних; 4) значні недоліки в процедурі накладення стягнення за скоєння адміністративного правопорушення, передбаченого ч. 4 ст. 188-39 КУпАП; 5) неефективність інституційної системи притягнення до відповідальності за порушення положень законодавства щодо захисту персональних даних, що наразі виконує Секретаріат Уповноваженого.

Кібератаки на інформаційно-телекомунікаційну інфраструктуру держави, як один з видів кібертероризму.

Сьогодні однією з найважливіших завдань нашої держави виступає протидія злочинності у сфері інформаційно-телекомунікаційних технологій. Цифровізація, діджиталізація та стрімкий розвиток інформаційно-телекомунікаційних технологій, систем та мереж загалом , призводить до того, що злочинність у кіберпросторі породжує все нові методи та простори для здійснення протиправних суспільно небезпечних дій. Варто зауважити, що феномен злочинності у кіберпросторі для нашої держави є доволі новим, однак при цьому має значний ступінь суспільної небезпечності є може бути об’єктом посягання багатьох суспільних відносин. Збройна агресія Російської Федерації, стала певним каталізатором вироблення нової якісної системи охорони кіберпростору України. Це перш за все стосується вдосконалення існуючої стратегії кібербезпеки України, а також внесення змін в існуючий Кримінальний кодекс України, щодо питання кримінальної відповідальності за суспільно небезпечні діяння, які вчиняються у кіберпросторі.

Інновації у сфері інформаційно-телекомунікаційних технологій сприяють не лише прогресивному економічному розвитку, а й призводять до появи нових форм кримінально-протиправних посягань на інформаційні інфраструктури критично важливих об'єктів. В нинішніх умовах інформаційно-телекомунікаційні технології можуть бути використані як засоби терору, війни та зброї.

Підвищення рівня суспільної небезпечності діянь, що вчиняються в інформаційній сфері, обумовлює необхідність підвищення захищеності критично важливих об'єктів інформаційної інфраструктури та одночасного посилення протидії загрозі розповсюдження злочинності у кіберпросторі. Здається, що руйнація інформаційної інфраструктури критично важливих і потенційно небезпечних об'єктів України шляхом неправомірного або несанкціонованого доступу до цифрової інформації з подальшим зараженням їх шкідливим програмним забезпеченням може завдати значної шкоди національній безпеці, а також призвести до екологічної катастрофи, людських жертв та інших тяжких і особливо тяжких наслідків.

Сьогодні спостерігається широка робота різних держав щодо створення кіберзброї, зокрема вірусів, шкідливого програмного забезпечення та поштових бомб. Перелічену кіберзброю можна завчасно інсталювати на цифрові пристрої, або закласти в інформаційно-телекомунікаційні технології з наступним приведенням їх в дію через інформаційно-телекомунікаційні мережі або системи. Звичайно в теорії це виглядає доволі скептично, адже на практиці такі дії не призведуть до знищення критичної інфраструктурі у загальному розумінні, однак, нанести пошкодження інформаційно-телекомунікаційним технологіям інших держав, проникнути в їх критичну інформаційно-телекомунікаційну систему цілком реально. Результатом таких дій може буди паралізування військової комунікаційної інфраструктури держави.

Загалом, коли ми говоримо про кібертероризм, варто розуміти, що руйнівний характер вчинених дій безпосередньо пов'язаний саме з застосуванням інформаційно-телекомунікаційних технологій, систем та мереж. При цьому неважливо, чи спрямований він на порушення функціонування інформаційних об'єктів чи інших систем, що впливають на життєдіяльність суспільства.

Так, Ю. І. Когут, зазначсає, що сьогодні кібертероризм є одним із найнебезпечніших видів тероризму в цілому, а його наслідки можуть бути катастрофічними. Терористичні акти в Сполучених Штатах Америки 11 вересня 2001 року та аварія в енергетичній системі в серпні 2003 року – наочні приклади.

Сьогодні особи, які спеціалізуються на скоєнні кримінальних правопорушень з використанням інформаційно-телекомунікаційних технологій, дедалі частіше атакують державні, комерційні та інші інформаційно-телекомунікаційні мережі. Як приклад, можна навести ситуацію, яка склалася в сфері енергозабезпечення держави, зокрема, 23 грудня 2015 року за допомогою шкідливого програмного забезпечення «BlackEnergy», яке мало ознаки троянської програми було відключено близько 30 підстанцій Прикарпаття-обленерго, в зв’язку з чим більш 200 тисяч жителів Івано-Франківської області залишалися без електроенергії на термін від одного до п’яти годин.

Але напевно наймасштабнішою кібератакою яка була здійсненна на критичну державну інфраструктуру можна вважати 6 грудня 2016 року коли була здійсненна кібератака на системи та мережі Міністерства фінансів України, Державну казначейську службу України та Пенсійний фонд України. Особливістю цієї атаки було не просто було не просто блокування інформаційно-телекомунікаційних технологій, систем та мереж зазначених органів, алей й часткове видалення цифрової інформації, яка містилася у них.

Ще одним прикладом неправомірного впливу на критичну інфраструктуру України є випадок, коли внаслідок поширення шкідливого програмного забезпечення типу «Petya» була фактично заблокована діяльність таких державних компаній, як Укрпошта, Укртелеком та аеропорт Бориспіль. В даному конкретному випадку кібератака була спрямована на блокування комп'ютерів зазначених секторів інфраструктурних об'єктів держави.

За даними Департаменту кібербезпеки Служби безпеки України за 2022 рік було нейтралізовано понад 4.5 тисячі кібератак, а на перший квартал 2023 року 550. Також було зазначено, що здебільшого Російська Федерація атакує об'єкти логістики, енергетики, транспорту, військові об'єкти.

Варто зауважити, що на відміну від традиційних кримінальних правопорушень у кіберпросторі таких, як кіберхашрайство, кардинг, скімінг та фішинг, які займають 90% серед усіх вчинених суспільно небезпечних діянь у кіберпросторі і виконавцями яких виступають звичайні користувачі віртуального простору, кримінальні правопорушення, які націлені на об'єкти критичної інформаційної інфраструктури України вчиняються з кадрових співробітників розвідних управлінь, які здійснюють всі найсерйозніші атаки і мають необмежене фінансування.

Варто зауважити, що до вразливих місць інформаційно-телекомунікаційних технологій, систем та мереж кожного інформаційного об'єкта можна віднести: 1) протоколи передачі цифрової інформації; 2) закордонне комунікаційне обладнання; 3) програмне забезпечення в інформаційно - телекомунікаційному обладнанні; 4) сховища та бази даних з віддаленим доступом.

Варто наголосити на тому, що лише декілька країн у світі займаються підготовкою спеціалістів для здійснення кібератак, зокрема це Сполучені Штати Америки, Російська Федерація та Китайська Демократична Народна

Республіка. Відповідно до даних голови компанії McAfee Дейва Ді Велта, всі перелічені країни активно займаються кібершпигунством та здійснюють інформаційні атаки щодо потенційних супротивників.

Звичайно, що сучасні загрози та виклики в рамках охорони кіберпростору нагально потребують підготовки спеціалістів з зазначеної сфери. Для прикладу в Китайській Народній Республіці військові відомства часто влаштовують олімпіади для майбутніх «хакерів». Так, Тан Дейлін, який був переможцем подібної олімпіади, потім здійснював кібератаки проти американських урядових відомств, результатом яких був витік більше тисячі секретних документів.

Слід зазначити, що в Європейському Союзі вже давно організовуються та проводяться великомасштабні національні, міжнародні та транснаціональні навчання з кібербезпеки. Такі навчання сприяють підвищенню рівня спеціальної підготовки керівного складу та підлеглих органів управління, сил та засобів кібербезпеки для належного забезпечення стійкого функціонування критично важливих об'єктів національної інфраструктури в умовах інформаційно-технічних впливів ймовірного супротивника.

Сьогодні в нашій державі питанням підготовки спеціалістів в рамках кібербезпеки відводиться багато часу. Відповідно до Стратегії кібербезпеки України від 26 серпня 2021 року утворено центри (підрозділи) забезпечення кібербезпеки або кіберзахисту в Державній службі спеціального зв'язку та захисту інформації України, Службі безпеки України, Національному банку України, Міністерстві інфраструктури України, Міністерстві оборони України, Збройних Силах України. Викладено, що інформаційно-телекомунікаційні технології можуть бути використані і як різновид зброї.

У багатьох країнах розробляються стратегії ведення віртуальної війни, між ними йде гонка кіберозброєнь, які створюються з метою

виведення з ладу державних комп'ютерних мереж та об'єктів життєзабезпечення.

Питаннями протидії таким кримінальним правопорушенням стурбована вся світова спільнота, адже атаки проти об'єктів життєзабезпечення та оборони країни можуть призвести до глобальних жертв та руйнувань.

Одним із негативних наслідків бурхливого розвитку інформаційно-комунікаційних технологій та мережі Інтернет є поява нових форм міжнародних конфліктів, включаючи інформаційні та мережеві війни.

Виходячи з того факту, що кіберпростір все частіше становиться ареною протистояння, критично важливим є міжнародно-правове регулювання правовідносин, які виникають у ньому. На наше переконання, з метою удосконалення міжнародно-правового регулювання протидії тероризму, нагальним є потреба у розробці спеціальних міжнародних договорів, які повинні бути направлені на протидію новим терористичним викликам. Зокрема, потребує окремої міжнародної регламентації протидії кібертероризму, тобто тероризму з використанням можливостей кіберпростору, де інформаційно-телекомунікаційні технології, системи та мережі можуть виступати, як об’єкти посягання або засоби вчинення суспільно небезпечного діяння.

Зауважимо, що на нашу думку забезпечення міжнародної безпеки в рамках кіберпростору повинно базуватися на розширенні зав’язків між країнами з метою вироблення спільних зусиль по боротьбі з суспільно небезпечними діяннями у кіберпросторі.

Варто відзначити, що міжнародне законодавство в сфері боротьби з кримінальними правопорушеннями у кіберпросторі має не досконалий стан. Фактично єдиним міжнародним актом, який наразі вважається еталонним, щодо питань встановлення кримінальної відповідальності за суспільно небезпечні діяння вчинені у кіберпросторі є Конвенція «Про

кіберзлочинність». Однак, конвенція надає перелік обмеженій кількості правопорушень, які вчиняються шляхом використання інформаційно-телекомунікаційних технологій, систем та мереж, залишаючи при цьому кібертероризм поза увагою.

Також, варто відмітити, що на дванадцятому зібранні Конгресу Організації Об'єднаних Націй по попередженню злочинності та кримінального правосуддя було поставлено питання протидії кіберзлочинності, і як результат була прийнята резолюцію в пункті 31 якої визначено, що законодавство щодо встановлення кримінальної відповідальності за кримінальні правопорушення у кіберпросторі в нинішній час формується в рамках національних та регіональних умов. Провідним способом боротьби з цією формою злочинності слід вважати використання норм національного кримінального права, яке найбільшою мірою відповідає поточному стану злочинності у цій сфері, а також інтересам держави та суспільства.

На відміну від більшості країн де законодавчо не визначений перелік об'єктів критичної інформаційної інфраструктури, Законом України від 16.11.2021 «Про критичну інфраструктуру» статтею 9 визначені основні сектори критичної інфраструктури.

Нажаль, сьогодні в кримінальному законодавстві України немає спеціалізованої статті яка б передбачала кримінальну відповідальність за неправомірний або несанкціонований вплив на об'єкти критичної інформаційної інфраструктури держави. Загалом всі такі дії будуть кваліфікуватися за відповідними статтями XVI Особливої частини Кримінального кодексу України, залежно від наслідків, які були спричинені. На нашу думку виходячи із специфічного об'єкта аналізованих суспільно небезпечних діянь, немає нагальної потреби введення нових статей до Особливої частини Кримінального кодексу України, які б регулювали зазначені суспільно небезпечні діяння, однак при цьому

вважаємо за необхідне ввести в рамках кваліфікуючих ознак, до відповідних статей XVI розділу Особливої частини Кримінального кодексу України наступне: 1) несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж критичної інфраструктури держави; 2) створення з метою протиправного використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних засобів, щодо інформаційно-телекомунікаційних технологій, систем або мереж, що мають ознаки об’єктів критичної інфраструктури держави.

Особлива увага з боку держави має бути зосереджена на запобіганні діям, спрямованим на розв'язання проти неї інформаційних воєн, націлених на дестабілізацію системи національної безпеки.

Як інформаційна зброя можуть виступати абсолютно різні засоби: високоточна зброя для ураження органів управління або окремих радіоелектронних засобів, засоби радіоелектронної боротьби, джерела потужного електромагнітного імпульсу, програмні віруси та ін. Як критерій віднесення до розряду інформаційної зброї може розглядатися тільки ефективність того чи іншого пристрою під час вирішення завдань інформаційної війни.

Загалом ми вважаємо, що основними причинами, що породжують таку кримінальну ситуацію та сприяють зростанню кримінальних правопорушень, що посягають на інформаційні інфраструктури критично важливих та потенційно небезпечних об'єктів України, є: 1) поширення в засобах масової інформації матеріалів, які пропагують безкарність кібертерористів; 2) слабка готовність правоохоронних органів та спеціальних служб протистояти зазначеним суспільно небезпечним діянням; 3) відсутність необхідної профілактики у сфері боротьби з

кримінальними правопорушеннями, які посягають на інформаційні інфраструктури критично важливих та потенційно небезпечних об'єктів.

Підсумовуючи вище зазначене хочемо акцентувати увагу та тому, що світовий кіберпростір є метою добре організованих кібератак. Методи та засоби, які використовуються для їх підготовки, постійно вдосконалюються. Такі кібератаки можуть бути спрямовані проти різних об'єктів критичної інформаційної інфраструктури не лише своєї, а й зарубіжних держав. Ефективна протидія кібератакам можлива лише в рамках спільних зусиль усіх заінтересованих країн, насамперед національних уповноважених органів у галузі виявлення та попередження комп'ютерних атак, та уніфікації міжнародного законодавства у сфері забезпечення безпеки критичної інформаційної інфраструктури.

Література.

1. Болгов В. М. Організаційно-правове забезпечення протидії кримінальним правопорушенням, що вчиняються з використанням інформаційних технологій : наук.-практ. посіб. / В. М. Болгов, Н. М. Гадіон, О. З. Гладун та ін. – К. : Національна академія прокуратури України, 2015. – 202 с.

2. Миколенко О.М. Деякі особливості розслідування злочинів у сфері використання електроннообчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку. Кібербезпека в Україні: правові та організаційні питання : матеріали Всеукр. наук.-практ. конф. (м. Одеса, 21 жовтня 2016 р.)., 2016. – 233 с.

3. Погорецький М. Кіберзлочини: до визначення поняття. Вісник прокуратури. – 2012. – № 8. – С. 89–96.

4. Голубєв В.О. Розслідування комп'ютерних злочинів / Монографія. - Запоріжжя: Гуманітарний університет "ЗІДМУ", 2003. - 296 с.

5. Амелін О. Визначення кіберзлочинів у національному законодавстві. Науковий часопис Національної академії прокуратури України. 2016. № 3. С. 1–10

6. Юртаєва К. В. Визначення місця вчинення злочинів з використанням комп'ютерних технологій. Форум права. 2009. № 2. С. 434–441. URL: http://nbuv.gov.ua/j-pdf/FP_index.htm_2009_2_69.pdf (дата звернення: 24.07.2022).

7. Vakulyk, O.O., Andriichenko, N.S., Reznik, O.M., Volik, V.V., Yanishevska, K.D. International aspect of a legal regulation in the field of financial crime counteraction by the example of special services of Ukraine and the CIS countries Journal of Legal, Ethical and Regulatory Issues, 2019, 22(1). URL: http://repository.mdu.in.ua/jspui/handle/123456789/1013

8. Словник банківських термінів. URL: https://www.banki.ru/wikibank/skimming/

9. Офіційний сайт Приват Банку. URL: https://privatbank.ua/strahovaniye/zakhyst-vid-shakhraystva#:~:text=3.,4.

10.Юрчук А.М. VII регіональна міжвузівська студентська науково-практична конференція Проблеми українського суспільства: кіберзлочинність. Види кіберзлочинності. URL: http://prog-rdak.16mb.com/wp-content/uploads/2017/04/kiberzlochunu.pdf

11.Klochko, A.N., Kulish, A.N., Reznik, O.N. The social basis of criminal law protection of banking in Ukraine Russian journal of criminology, 10(4), pp. 790–800

12.Rusch, J. The compleat cyber-angler: A guide to phishing. Computer Fraud & Security, (1):4-6. doi: 10.1016/S1361-3723(05)00145-4.

13.Lyubimenko O.O. Fraud on the Internet as a threat to the economic security of the state. URL: https://cyberleninka.ru/article/n/moshennichestvo-v-seti-internet-kak-ugroza-ekonomicheskoy-bezopasnosti-gosudarstva/viewer

14.Copyright Law of the United States. (Title 17). URL: https://www.copyright.gov/title17/

15.Болгов В.М., Гадіон О.З. Організаційно-правовий захист від кримінальних правоохоронців, які відповідають за інформаційні технології: наука і практика. Київ. Національна академія прокуратури України. URL: http://ir.nusta.edu.ua/jspui/handle/123456789/2337

16. М. Бем, І. Городський. Захист персональних даних: правове регулювання та практичні аспекти: науково-практичний посібник. – «К.І.С.»., 2021. С. 161.