3. Про забезпечення єдиного підходу до формування тарифів на комунальні послуги: Постанова КМУ від 1 черв. 2011 р. № 869. URL: https://ips.ligazakon.net/document/kp110869.

4. Про житлово-комунальні послуги : Закону України від 09.11.2017 № 2189-VIII. URL: https://ips.ligazakon.net/document/fn052000.

5. Як розв'язувати спори, що виникають між членами робітничих житло-будівельних кооперативних товариств і керівними органами цих товариств у зв'язку з розподілом житлової площі: Постанова Народного комісаріату юстиції УСРР від 20 березня 1930 року. ЗЗ УСРР 1930 р. відділ II, № 6, ст. 59.

Думчиков Михайло Олександрович,
асистент кафедри кримінально-правових дисциплін Навчально-наукового інституту права СумДУ, кандидат юридичних наук

КІБЕРЗЛОЧИННІСТЬ ЯК НОВА СВІТОВА КРИМІНАЛЬНА ЗАГРОЗА: РЕТРОСПЕКТИВНИЙ АНАЛІЗ

Анотація. Аналізується загрози сучасного суспільства, викликані значним поширенням інформаційних технологій та зміщенням частини злочинів в глобальну інформаційно-телекомунікаційну мережу інтернет. Висвітлюються існуючі і можливі проблеми кіберзлочинів, аналізується та аналізується їх сучасний стан.

Ключові слова: кіберзлочинність, кіберзлочин, інтерент злочин, кібербезпека, кіберзахист.

Summary. It analyzes the threats of modern society caused by the widespread spread of information technologies and the shift of some crimes to the global information and telecommunication network of the Internet. Existing and possible problems of cybercrime are covered, their current state is analyzed and analyzed.

Keywords: cybercrime, cybercrime, cybercrime, cyber security, cyber defense.

Процеси глобалізації інформаційних технологій представляють необмежені можливості для здійснення впливу на окрему особистість і суспільство в цілому. В даний час одним з найбільш пріоритетних напрямків внутрішньої політики всіх розвинених країн є реалізація ефективних заходів, покликаних забезпечити інформаційну безпеку як громадян, так і держави в цілому. В умовах все зростаючого впливу IT-індустрії на повсякденне життя, що не припиняється, розширення мережевої аудиторії і проникнення цифрових технологій у нові сфери суспільної взаємодії особливе значення набуває створення з боку

держав національних механізмів, які дозволять гарантувати інформаційний суверенітет.

На жаль, порушення інформаційної безпеки не є в наші дні чимось неординарним. Нещодавно публічного поширення отримав факт розробки центрального розвідувального управління певних технічних засобів, які можуть бути використані для отримання несанкціонованого доступу до пакету персональних даних на комп'ютерах, смартфонах та інших пристроїв які підключені до глобальної мережі. Такий доступ можливий через використання різних комп'ютерних програм, Wi-Fi мережей і навіть антивірусні рішення, які використовуються мільйонами користувачів для забезпечення власної інформаційної захисту. Наведені приклади наочно демонструють, що для забезпечення інформаційної безпеки категорично необхідна реалізація не тільки організаційних, а й відповідних технологічних заходів. Варто зазначити, що Україною було здійснено комплекс заходів які спрямовуються на забезпечення інформаційної безпеки і стабільності сегменту мережевого простору. Зокрема за рахунок використання нового обладнання яке відповідає актуальним вимогам інформаційного ринку. Відмітимо, що у національному законодавстві питання забезпечення конфіденційності персональних даних користувачів, а також питання забезпечення зв'язку та листування в тому числі у випадках, коли отримання доступу до відповідних відомостями необхідно для проведення оперативно-розшукових заходів, приділяється особлива увага [1]. Варто зазначити, що в 2017 році на національному рівні була прийнята концепція кібербезпеки де були визначений основний понятійний апарат, принципи, суб'єкти та об'єкти кібербезпеки.

На нашу думку кіберзлочинність варто визначити як злочинність в так званому кіберпросторі. Під кіберпростором варто розуміти середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних[2]. Кіберзлочини включають в себе поширення шкідливих програм, злом паролів, крадіжки номерів і паролів банківських карт, крадіжки і шахрайства з використанням електронних платіжних систем і ряд інших. Термін «кіберзлочинність» в даний час використовується поряд з терміном «комп'ютерна злочинність». Поняття «кіберзлочинність» ширше ніж «комп'ютерна злочинність» і більш точно відображає природу такого явища, як злочинність в інформаційному просторі. Проблема використання досягнень науки і техніки в злочинних цілях пов'язана зі створенням глобальної мережі

Інтернет, яка об’єднує мільйони комп’ютерів, розташованих в різних точках Землі. Більшість злочинів, які вчиняються в глобальних комп’ютерних мережах, характеризуються такими особливостями:[3]

1. підвищена скритність скоєння злочину
2. транскордонний характер мережевих злочинів, при якому злочинець, об’єкт злочинного посягання і потерпілий можуть перебувати на територіях різних держав;
3. можливість скоєння злочину в автоматизованому режимі в декількох місцях одночасно
4. необізнаність потерпілих про те, що вони піддалися злочинному впливу;
5. дистанційний характер злочинних дій в умовах відсутності фізичного контакту злочинця і потерпілого
6. неможливість запобігання і припинення злочинів даного виду традиційними засобами.

У сучасних умовах зростання кіберзлочинності загрожує безпеці всіх держав світу, підриває довіру до державних органів влади, органам місцевого самоврядування, посадових осіб. Тому необхідно підвищувати рівень міжнародної координації наукових досліджень в галузі запобігання та протидії актам кіберзлочинності за допомогою розробки нових нормативно-правових актів, спеціальних технологій для ефективного і швидкого розкриття злочинів в даній області.

Безперервне поширення цифрових сервісів в нашому повсякденному житті, так само як і посилення впливу міжнародних IT-корпорацій, породжує нові ризики і загрози для забезпечення недоторканності приватного життя громадян і національної безпеки держав. Подібні обставини вимагають пропорційного відповіді, як в сфері прийняття відповідного нормативного регулювання, так і в технологічній сфері з тим, щоб забезпечити безпеку для користувача даних і інформаційний суверенітет держави.

Список використаних джерел

1. Конституція України. URL: http://zakon5.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80.

2. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. Відомості Верховної Ради. 2017. № 45. Ст. 403.

3. Осипенко А. Л. Сетевая компьютерная преступность. Омск, 2009. С. 109–110. Oxford English Dictionary. URL: http:/ /www. askoxford.com/ (дата обращения:24.03.2020).