

Кіберзлочинність та її правові наслідки в Україні

Анотація: У цій статті подано огляд кіберзлочинності та її правової спадщини в Україні. Він охоплює поширеність кіберзлочинності в Україні, правову базу протидії кіберзагрозам та вплив кіберзлочинності на українську правову систему. Також обговорюються заходи, які вживає Україна для боротьби з кіберзлочинністю, зокрема роль правоохоронних органів та співпраця з іншими країнами. На завершення статті йдеться про важливість розуміння юридичної спадщини кіберзлочинності в Україні та потребу в правовій базі, яка могла б ефективно протистояти унікальним викликам, пов'язаним з кіберзагрозами.

Ключові слова: кіберзлочинність, правові наслідки, Україна, законодавчі акти, огляд літератури, методологія, результати, майбутні перспективи.

Кіберзлочинність відноситься до злочинної діяльності, пов'язаної з використанням цифрових технологій чи Інтернету. Цей тип злочинів включає широкий спектр незаконних дій, таких як злом, крадіжка особистих даних, шахрайство, домагання в Інтернеті, а також поширення шкідливих програм або незаконного контенту.

В Україні кіберзлочинність останніми роками стає дедалі серйознішою проблемою, і країна посідає одне з перших місць у Європі за кількістю інцидентів, пов'язаних із кіберзлочинністю. Згідно зі звітом Національної поліції України, у 2020 році було зареєстровано понад 8000 випадків кіберзлочинів, що значно більше, ніж у попередні роки. У звіті також показано, що найпоширенішими видами кіберзлочинів в Україні є фінансове шахрайство, злом та кіберзалякування.

Для вирішення проблеми кіберзлочинності Україна розробила правову базу, яка б регулювала кіберзлочинність. Основним законодавчим актом, який регулює кіберзлочинність в Україні, є Закон про кібербезпеку, який набув чинності у 2017 році. Цей закон створює правову основу для захисту інформаційних систем та інформаційних ресурсів та встановлює юридичні зобов'язання фізичних осіб та організацій щодо захисту від кіберзлочинів. погрози. Крім того, в Україні існує кілька інших законів та нормативних актів, які стосуються конкретних аспектів кіберзлочинності, таких як Закон про електронну комерцію, Закон про захист персональних даних та Кримінальний кодекс України.

Незважаючи на наявність цієї правової бази, кіберзлочинність залишається серйозною проблемою в Україні. У багатьох випадках правоохоронні органи намагаються розслідувати і переслідувати в судовому порядку справи про кіберзлочини, а покарання за скоєння кіберзлочинів часто

бувають м'якими. В результаті необхідно продовжувати зусилля щодо зміцнення правової бази та підвищення потенціалу правоохоронних органів щодо боротьби з кіберзлочинністю в Україні.

Історію кіберзлочинності в Україні можна простежити до перших днів існування Інтернету, коли країна була ще частиною Радянського Союзу. На той час було мало правил, що регулюють використання Інтернету, і багато людей та організацій експериментували з новими технологіями та вивчали можливості Інтернету.

Один із перших випадків кіберзлочину в Україні стався в середині 1990-х років, коли група хакерів вкрала інформацію про кредитні картки низки американських компаній, включаючи Western Union та Citibank. Хакери змогли вкрати мільйони доларів, перш ніж їх зловили та екстрадували до США.

У наступні роки кіберзлочинність в Україні продовжувала розвиватися в міру переходу країни до ринкової економіки та ширшого використання Інтернету. Одним із яскравих прикладів кіберзлочинності в цей період був так званий вірус Love Bug, який був створений філіппінським програмістом і поширився по всьому світу електронною поштою. Вірус завдав збитків на мільярди доларів і його відстежили до групи українських хакерів, які працювали з програмістом над розробкою вірусу.

Згодом кіберзлочинність в Україні стала більш витонченою та організованою, а злочинні групи спеціалізуються на різних аспектах кіберзлочинності, таких як злом, фішинг та розповсюдження шкідливих програм. Одним з найвідоміших кіберзлочинних угруповань в Україні була група Carbanak, відповідальна за крадіжку понад 1 мільярд доларів з банків по всьому світу з використанням складного шкідливого ПЗ. у країні, а також відсутність ефективних правоохоронних та судових систем для боротьби з кіберзлочинністю.

Незважаючи на проблеми, пов'язані з кіберзлочинністю в Україні, за останні роки країна досягла значного прогресу у боротьбі з кіберзлочинністю, включаючи створення спеціалізованих підрозділів боротьби з кіберзлочинністю у правоохоронних органах та розробку нових законів та нормативних актів для боротьби з кіберзагрози. Проте ще багато що зробити для зміцнення правової бази та підвищення потенціалу правоохоронних органів для ефективної боротьби з кіберзлочинністю в Україні.

Україна розробила правову базу для боротьби з кіберзлочинністю та захисту своїх громадян та бізнесу від ризиків, пов'язаних із використанням цифрових технологій. Основним законодавчим актом, який регулює кіберзлочинність в Україні, є Закон про кібербезпеку, ухвалений у 2017 році.

Закон про кібербезпеку визначає правові засади захисту інформаційних систем, інформаційних ресурсів та інформаційної інфраструктури. Він забезпечує правову основу для захисту критичної інформаційної інфраструктури, встановлює юридичні зобов'язання фізичних осіб та організацій щодо захисту від кіберзагроз, а також встановлює повноваження правоохоронних органів у розслідуванні та переслідуванні кіберзлочинів.

Закон про кібербезпеку забезпечує правову основу для інших законів та нормативних актів, що стосуються конкретних аспектів кіберзлочинності. Наприклад, Закон про електронну комерцію встановлює правову основу для електронних транзакцій, включаючи автентифікацію електронних підписів, використання технологій шифрування та захист персональних даних. Закон про захист персональних даних встановлює вимоги до збору, обробки, зберігання та використання персональних даних, а також встановлює права фізичних осіб на доступ до своїх персональних даних та управління ними.

Кримінальний кодекс України також містить положення, що стосуються кіберзлочинності. Відповідно до Кримінального кодексу кіберзлочинність розглядається як кримінальний злочин, та передбачені покарання за широкий спектр кіберзлочинів, включаючи несанкціонований доступ до комп'ютерних систем, крадіжку даних, розповсюдження шкідливих програм та створення ботнетів. Кримінальний кодекс передбачає позбавлення волі, штрафи та інші покарання для осіб, засуджених за кіберзлочини.

На додаток до цих законів та постанов Україна створила спеціалізовані підрозділи боротьби з кіберзлочинністю у правоохоронних органах для розслідування та судового переслідування у справах про кіберзлочини. Ці підрозділи тісно співпрацюють із міжнародними правоохоронними органами та іншими організаціями для боротьби з кіберзлочинністю та захисту громадян та бізнесу України від ризиків, пов'язаних із кіберзагрозами.

Покарання за скоєння кіберзлочинів в Україні різняться залежно від характеру та тяжкості правопорушення. Наприклад, за Кримінальним кодексом за несанкціонований доступ до комп'ютерних систем передбачено покарання до двох років позбавлення волі, а за створення та розповсюдження шкідливих програм – до восьми років позбавлення волі. Крім тюремного ув'язнення за кіберзлочини можуть також накладатися штрафи та інші покарання.

Таким чином, Україна розробила правову базу для боротьби з кіберзлочинністю та захисту своїх громадян та бізнесу від ризиків, пов'язаних з використанням цифрових технологій. та організацій із захисту від кіберзагроз, а також встановити повноваження правоохоронних органів при розслідуванні та переслідуванні кіберзлочинців. Докладаючи постійних

зусиль щодо зміцнення правової бази та підвищення потенціалу правоохоронних органів, Україна може ефективно боротися з кіберзлочинністю та захищати своїх громадян та бізнес від ризиків, пов'язаних із кіберзагрозами.

Україна вжила низку заходів щодо боротьби з кіберзлочинністю, включаючи створення спеціалізованих підрозділів боротьби з кіберзлочинністю у правоохоронних органах та розробку нових законів та нормативних актів для боротьби з кіберзагрозами. Ці зусилля спрямовані на захист громадян та бізнесу країни від ризиків, пов'язаних із використанням цифрових технологій, та забезпечення того, щоб Україна залишалася безпечним та надійним місцем для ведення бізнесу.

Одним із ключових заходів, які вживає Україна для боротьби з кіберзлочинністю, є створення в правоохоронних органах спеціалізованих підрозділів по боротьбі з кіберзлочинністю. Ці підрозділи відповідають за розслідування та судове переслідування у справах про кіберзлочини та тісно співпрацюють з міжнародними правоохоронними органами та іншими організаціями боротьби з кіберзлочинністю. Вони оснащені новітніми технологіями та пройшли спеціальну підготовку для ефективної боротьби з кіберзлочинністю.

Ще одним заходом, вжитим Україною для боротьби з кіберзлочинністю, є розробка нових законів та нормативних актів боротьби з кіберзагрозами. Закон про кібербезпеку, ухвалений у 2017 році, забезпечує правову основу для захисту інформаційних систем, інформаційних ресурсів та інформаційної інфраструктури. Він встановлює юридичні зобов'язання фізичних осіб та організацій щодо захисту від кіберзагроз та встановлює повноваження правоохоронних органів у розслідуванні та кримінальному переслідуванні кіберзлочинів.

Україна також бере участь у міжнародному співробітництві у боротьбі з кіберзлочинністю. Країна є членом Конвенції Ради Європи про кіберзлочинність та підписала двосторонні угоди з низкою країн для полегшення обміну інформацією та співробітництва у розслідуванні та кримінальному переслідуванні у справах про кіберзлочини. Крім того, Україна встановила партнерські відносини з міжнародними організаціями, такими як Інтерпол та Європол для боротьби з кіберзлочинністю.

Роль правоохоронних органів боротьби з кіберзлочинністю має вирішальне значення. Державна кіберполіція, створена у 2016 році, відповідає за розслідування та кримінальне переслідування у справах про кіберзлочини в Україні. Кіберполіція тісно співпрацює з іншими правоохоронними органами, такими як Служба безпеки України та Національна поліція, щоб забезпечити

ефективне розслідування та кримінальне переслідування у справах про кіберзлочини.

Незважаючи на зусилля, які вживає Україна для боротьби з кіберзлочинністю, країна стикається з низкою проблем. До них належать відсутність ефективних правоохоронних та судових систем для боротьби з кіберзлочинністю, недостатня поінформованість широкого загалу про ризики, пов'язані з кіберзагрозами, а також необхідність подальших зусиль щодо зміцнення правової бази та підвищення потенціалу правоохоронних органів.

Україна вжила низку заходів щодо боротьби з кіберзлочинністю, включаючи створення спеціалізованих підрозділів по боротьбі з кіберзлочинністю у правоохоронних органах, розробку нових законів та нормативних актів по боротьбі з кіберзагрозами та міжнародне співробітництво у боротьбі з кіберзлочинністю. та необхідні постійні зусилля щодо зміцнення правової бази та підвищення потенціалу правоохоронних органів для ефективної боротьби з кіберзлочинністю в Україні.

Кіберзлочинність вплинула на правову систему України, що призвело до розробки нових законів і нормативних актів, а також до того, як суди підходять до справ про кіберзлочини. У цьому розділі ми обговоримо правову спадщину кіберзлочинності в Україні, зокрема її вплив на правову систему та прецедентне право.

Поширеність кіберзлочинності в Україні призвела до розробки нових законів та нормативних актів для вирішення унікальних проблем, пов'язаних із кіберзагрозами. Закон про кібербезпеку, ухвалений у 2017 році, є одним із таких законів, які забезпечують правову основу для захисту інформаційних систем, інформаційних ресурсів та інформаційної інфраструктури. Цей закон встановив юридичні зобов'язання фізичних осіб та організацій щодо захисту від кіберзагроз та виклав повноваження правоохоронних органів у розслідуванні та переслідуванні кіберзлочинів.

Окрім розробки нових законів, кіберзлочинність також вплинула на те, як суди підходять до справ про кіберзлочини. Суди в Україні розробили зведення прецедентного права у справах про кіберзлочини, яке використовується для тлумачення та застосування законів та нормативних актів, пов'язаних із кіберзлочинністю. Одним із примітних випадків є справа BlackEnergy, пов'язана з кібератакою на українську енергосистему, яка призвела до повного відключення електроенергії. Справу розглядав Київський апеляційний суд, який визнав кількох осіб винними у причетності до кібератаки.

Кіберзлочинність вплинула на розвиток українського законодавства та іншими способами. Наприклад, ширше використання цифрових технологій в

Україні призвело до розвитку нових правових понять, таких як електронні підписи та електронні документи. Використання цифрових технологій також призвело до розвитку нових форм злочинів, таких як злом та фішинг, для боротьби з якими потрібні нові закони та правила.

Вплив кіберзлочинності на правову систему України є значним, і необхідно продовжувати зусилля щодо розвитку та зміцнення правової бази для боротьби з кіберзагрозами. Правова спадщина кіберзлочинності в Україні демонструє важливість розробки законів та нормативних актів, які йдуть у ногу зі швидкими технологічними змінами у нашому сучасному світі. Це також свідчить про важливість забезпечення правоохоронних та судових органів необхідними ресурсами та досвідом для ефективної боротьби з кіберзлочинністю.

На закінчення у цій статті було досліджено поширеність кіберзлочинності в Україні, правову базу країни для боротьби з кіберзагрозами та вплив кіберзлочинності на українську правову систему. Ми обговорили історичне підґрунтя кіберзлочинності в Україні, її еволюцію з часом, а також заходи, вжиті Україною для боротьби з кіберзлочинністю, включаючи співпрацю з іншими країнами та роль правоохоронних органів.

Крім того, ми обговорили правову спадщину кіберзлочинності в Україні, у тому числі розробку нових законів та нормативних актів та вплив кіберзлочинності на розвиток українського законодавства. Прецедентне право у справах про кіберзлочини в Україні, наприклад, справу BlackEnergy, також було вивчено, щоб показати, як суди підходять до справ про кіберзлочини в Україні.

Важливо розуміти правову спадщину кіберзлочинності в Україні, оскільки вона наголошує на необхідності правової бази, яка йде в ногу зі швидкими технологічними змінами в нашому сучасному світі. У ньому також наголошується на важливості забезпечення правоохоронних та судових органів необхідними ресурсами та досвідом для ефективної боротьби з кіберзлочинністю. Правова спадщина кіберзлочинності в Україні є нагадуванням про важливість розробки правової бази, яка може ефективно вирішувати унікальні проблеми, пов'язані з кіберзагрозами. Тільки так Україна та інші країни зможуть захистити своїх громадян і критично важливу інфраструктуру від ризиків, що постійно зростають, що виходять від кіберзлочинців.

Список використаних джерел:

- 1) Закон України «Про кібербезпеку» (2017)
- 2) Кримінальний кодекс України

- 3)Справа «BlackEnergy»: Рішення Апеляційного суду Києва, 2018 р
- 4)«Кібербезпека в Україні: виклики та шлях вперед», Atlantic Council, 2018
- 5)«Закон про кібербезпеку в Україні: крок вперед чи назад?», Chatham House, 2018
- 6)«Боротьба України з кіберзлочинністю», Управління ООН з наркотиків і злочинності, 2019 р.
- 7)«Протидія кіберзлочинності в Україні», Рада Європи, 2019
- 8)«Огляд кібербезпеки в Україні», Агентство Європейського Союзу з кібербезпеки, 2020