

Національний університет «Одеська юридична академія»

Робоча група з питань розвитку кримінального права
Комісії по правовій реформі при Президентові України

Робоча група з питань кримінального та кримінального процесуального права
Науково-консультативної ради при Голові Верховної ради України

Південний регіональний центр Національної академії правових наук України
Кафедра кримінального права НУ «ОЮА»

Одеський місцевий осередок ГО «Всеукраїнська асоціація кримінального права»

Завдання кримінального права в умовах надзвичайного стану

Матеріали Міжнародної науково-практичної конференції,

*присвяченої 25-річчю утворення
Національного університету
«Одеська юридична академія»*



**м. Одеса
9 грудня 2022 р.**

«Завдання кримінального права в умовах надзвичайного стану». Матеріали міжнародної науково-практичної конференції, присвяченої 25-річчю утворення Національного університету «Одеська юридична академія». Одеса, 9 грудня 2022 року. Укладачі: Є.Л. Стрельцов, В.П. Кедик. Відп. редактор Є.Л. Стрельцов. Одеса: ПРЦ НАПрН України, НУ «ОЮА», 09.12.2022. – 214 с.

У збірнику представлені тези доповідей та повідомлень, які були оприлюднені на міжнародній науково-практичній конференції «Завдання кримінального права в умовах надзвичайного стану», присвяченій 25-річчю утворення Національного університету «Одеська юридична академія», яка відбулась 9 грудня 2022 року на базі Південного регіонального центру Національної академії правових наук України та кафедри кримінального права Національного університету «Одеська юридична академія». Збірник розрахований на науково-педагогічних працівників, докторантів та аспірантів, магістрантів та студентів, практичних працівників, всіх, кого цікавлять сучасні проблеми кримінального права.

Відповідальний за випуск:
д.ю.н., професор Є.Л. Стрельцов

Тези друкуються в авторській редакції. Відповідальність за зміст поданого матеріалу несуть автори.

<i>Кріпак Н.Г.</i> ПОНЯТТЯ КРИМІНАЛЬНОГО ПРОСТУПКУ В ЗАРУБІЖНОМУ КРИМІНАЛЬНОМУ ПРАВІ.....	178
<i>Купенко А.І.</i> ВІДПОВІДАЛЬНІСТЬ ЗА ДОМАШНЄ НАСИЛЬСТВО: АНАЛІЗ СУДОВОЇ ПРАКТИКИ.....	180
<i>Лупу В.С.</i> ТА ФУНКЦІЇ СУЧАСНОГО КРИМІНАЛЬНОГО ПРАВА.....	183
<i>Мазур Ю.С.</i> ЗАЛУЧЕННЯ ДІТЕЙ ДО УЧАСТІ У ЗБРОЙНИХ КОНФЛІКТАХ.....	186
<i>Мархайчук Д.М.</i> ПРАВОВА КВАЛІФІКАЦІЯ КОЛАБОРАЦІЙНОЇ ДІЯЛЬНОСТІ.....	188
<i>Наливайченко В.О.</i> МАРОДЕРСТВО: ЧИ ВСІ КРИМІНАЛЬНІ ПРАВОПОРУШЕННЯ ПРОТИ ВЛАСНОСТІ, СКОЄНІ ПІД ЧАС ВІЙНИ, Є МАРОДЕРСТВОМ?	191
<i>Рачок А.І.</i> ЗАГАЛЬНА ХАРАКТЕРИСТИКА ЗЛОЧИНІВ У СЕРЕДНЬОВІЧЧІ.....	193
<i>Саїк О.Б.</i> ВОЄННИЙ СТАН ЯК ОБСТАВИНА, ЯКА ВПЛИВАЄ НА КВАЛІФІКАЦІЮ КРИМІНАЛЬНОГО ПРАВОПОРУШЕННЯ.....	195
<i>Стащук А.Ю.</i> КРИМІНАЛЬНЕ ПРАВОПОРУШЕННЯ В УМОВАХ НАДЗВИЧАЙНОГО СТАНУ: ПОНЯТТЯ, ОЗНАКИ ТА КЛАСИФІКАЦІЯ.....	197
<i>Тарасенко М.Л.</i> ОСОБЛИВОСТІ КІБЕРЗЛОЧИНІВ.....	200
<i>Філімончук М.О.</i> КРИМІНАЛЬНЕ ПРАВОПОРУШЕННЯ В УМОВАХ НАДЗВИЧАЙНОГО СТАНУ: ПОНЯТТЯ, ОЗНАКИ ТА КЛАСИФІКАЦІЯ.....	203
<i>Штанько Ю.А.</i> ШТУЧНИЙ ІНТЕЛЕКТ ЯК СУБ'ЄКТ КРИМІНАЛЬНОЇ ВІДПОВІДАЛЬНОСТІ.....	206
<i>Ядаменко О.О.</i> ВІДПОВІДАЛЬНІСТЬ ЗА МАРОДЕРСТВО ТА ІНШІ ЗЛОЧИНИ ПРОТИ ВЛАСНОСТІ В УМОВАХ ДІЇ НАДЗВИЧАЙНОГО АБО ВОЄННОГО СТАНУ: СУЧАСНИЙ ПОГЛЯД.....	208
<i>Язаджи В.С.</i> ПРОГАЛИНИ КРИМІНАЛЬНО-ПРАВОВИХ НОРМ У СФЕРІ ДОРОЖНЬО-ТРАНСПОРТНОГО РУХУ.....	210
Streltsov Yevgen. CRIMINAL LAW IN THE CONDITIONS OF THE EMERGENCY (CONFERENCE PRESENTATION)	212

*Тарасенко М. Л.,
студентка 2 курсу факультету
прокуратура та слідства
(кримінальна юстиція),
Національного університету
«Одеська юридична академія»*

*Науковий керівник
доктор юридичних наук, доктор
теології, професор, член-
кореспондент Національної
академії правових наук України
Стрельцов Є. Л.*

ОСОБЛИВОСТІ КІБЕРЗЛОЧИНІВ³

Ми живемо сьогодні, які відомо, в епоху інформаційних технологій, де потрібно більш детально приділяти увагу безпеці у віртуальному просторі, адже з кожним днем людина все більше і більше переносе своє життя в кіберпростір. Але кримінально протиправні посягання у віртуальному світі, це явище, яке з'явилося не так давно і має досить інший характер, ніж такі ж діяння за своїм змістом, які мають більш «знайомий» характер, наприклад, крадіжки, шахрайства, вимагання. При цьому, при визначенні кіберзлочинів, незважаючи на їх певну новизну, все ж використовується більш традиційне: це кримінально протиправні діяння, які здійснюються особами, що використовують інформаційні технології для злочинних (протиправних) цілей. При цьому, варто зазначити що комп'ютер чи інший пристрій виступає як знаряддя для таких діянь, а інформаційна безпека часто виступає об'єктом.

Сучасний Кримінальний кодекс України закріпив правопорушення у даній сфері у розділі 16 «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», де систематизовані певна кількість кримінально-правових статей [1], зокрема, ст. ст. 361-361-363 КК України (далі КК). Варто зазначити, що в дану сферу також відносять статті 176, 190, 209, 363 КК, які будуть проаналізовані нижче.

Стаття 361 КК «Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку» встановлює кримінальну відповідальність за одне з найбільш актуальних та поширених видів кримінальних правопорушень в нашій державі. Сутність таких діянь проявляється в тому, що отримання незаконним способом доступу до певних даних та подальше їх використання для задоволення своїх потреб, найчастіше пов'язане з подальшим заволодінням майном жертв. Таким прикладом виступає випадок, де правопорушник за допомогою «шкідливого» програмного засобу для підбору паролів, здійснила несанкціоновану авторизацію (вхід) до облікового запису (електронно-поштового ресурсу) «hotmail», який належав іншій особі та заволоділа персональними даними облікового запису останньої, для подальшого отримання майна жертви завдяки її даних[2].

Наступна стаття 361-1 КК має пряме значення до розробки програмних кодів або ж створення певних «шкідливих» програм, які можуть бути створення для різни цілей.

³ В чинному Кримінальному кодексі України «злочин» є одним з видів кримінальних правопорушень, яке, поруч з «кримінальний проступок», складає загальну категорію «кримінальне правопорушення». Але у більш звичному вигляді, при характеристиці певних груп кримінально протиправних посягнень, ще використовується поняття «злочин». Тому і в цих тезах буде використовуватися і в цих тезах, при характеристиці кримінально протиправних діянь у віртуальному просторі.

Найбільш популярними таких діянь є «збій» комп'ютерної програми, яке виконується особою, котра діє з прямим умислом з подальшою метою отримання незаконних грошей, для «особистого» налагодження системи, зарядження вірусом певних файлів, отримання персональних даних тощо. Особа, яка вчинила такі дії буде нести кримінальну відповідальність за ст. 361-1 КК України.

Стаття 176 КК «Порушення авторського права і суміжних прав», незважаючи на те, що знаходиться в іншому розділі Особливої частини КК, теж достатньо часто відноситься до групи кримінальних правопорушень, які посягають на кібербезпеку. На сьогоднішній день в Україні існує великий показник «піратства», коли особа офіційно не купує комп'ютерну програму, а завантажує її безкоштовно, використовуючи для цього певну «зламану» версію, або ж коли робить інсталяцію програми та обхід активації за допомогою «злому», думаючи, що за це немає відповідальності та легковажно розраховуючи на наслідки, але у КК такі діяння заборонені та в разі їх виявлення, особу притягнуть до кримінальної відповідальності згідно з ст. 176 КК України.

Статті 190 КК «Шахрайство» та 209 КК «Легалізація (відмивання) майна, одержаного злочинним шляхом», мають вагоме значення в кіберпросторі, тому осіб, які вчиняють подібні діяння, часто притягують до відповідальності саме за шахрайство. Так, наприклад, з початком проблеми захворювання коронавірусом COVID-19 та введенням спеціальних карантинних заходів, кількість випадків шахрайства у віртуальному світі значно зросла. Шахраї розсилали СМС-повідомлення або телефонували й повідомляли обманну інформацію про певні державні компенсації для громадян, такі як: виплата коштів на лікування, придбання тестів для визначення коронавірусу, компенсація за втрату місця роботи тощо. Це робилось для того, що б отримати доступ до банківських рахунків, інших фінансових відомостей потенційно потерпілих осіб, з метою протиправного отримання їх грошей.

Випадки розкриття таких кримінальних правопорушень є доволі не частими, адже особи-шахраї користуються одноразовими сім-картами, змінюють телефонні термінали, використовують банківські картки, оформлені на підставних осіб для подальшого зняття готівки. Але, потрібно відмітити, що сьогоднішній день правоохоронці роблять значні успіхи в розкритті такої категорії кримінальних правопорушень та викриття шахраїв.

В цілому, однієї, загальної класифікації кримінальних правопорушень у цій сфері немає, але при спробах її створення, за основу береться класифікація відповідно до Конвенції про кіберзлочинність 2001 року, яка була ратифікована Україною у 2005 році:

1) правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний доступ до систем; нелегальне перехоплення інформації; втручання у дані та системи; виготовлення, розповсюдження та збут шкідливого програмного забезпечення та спеціальних пристроїв): ст. 361, 361-1 КК України

2) правопорушення, пов'язані з комп'ютерами (комп'ютерне підроблення та комп'ютерне шахрайство): ст. 190, 363 КК України

3) правопорушення, пов'язані зі змістом (вироблення, володіння, розповсюдження або передача дитячої порнографії за допомогою комп'ютерних систем): ст. 361-2, 362 КК України

4) правопорушення, пов'язані з порушенням авторських та суміжних прав [3] - ст. 179 КК України

Невизначеність та недостатність досвіду у визначення змісту та ознак протиправних дій призводить до того, що слідчими органами ще недостатньо активно, на нашу думку, проводиться розслідування таких кримінальних справ. Про багатогранність проблеми розслідування кіберзлочинів (кримінальних правопорушень) та широкі можливості для їх дослідження та розроблення шляхів їх вирішення можна багато говорити. З огляду входження України у світовий інформаційний простір потрібно більше уваги приділити побудові національній моделі забезпечення кібербезпеки держави, громадян, а також підприємств, адже як кримінально-протиправні посягання в цієї сфери набирають обертів

та характеризуються ретельною підготовкою, маскуванню доказів та латентністю, що ускладнює роботу правоохоронних органів. Науковий аналіз таких проблем, в зв'язку з наведеними аргументами, має необхідний характер.

Список використаних джерел:

1. Кримінальний кодекс України : Кодекс України від 05.04.2001 р. № 2341-III : станом на 6 листоп. 2022 р. URL: <https://zakon.rada.gov.ua/laws/show/2341-14#Texti>
2. Костянтин Кривенко. Кіберзлочинність: актуальна судова практика | Think brave. Think brave | Останні новини бізнесу України.
3. Конвенція про кіберзлочинність : Конвенція Ради Європи від 23.11.2001 р. : станом на 7 верес. 2005 р. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text