МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХЕРСОНСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ БІЗНЕСУ І ПРАВА
КАФЕДРА ГАЛУЗЕВОГО ПРАВА

КРИМІНАЛЬНО-ПРАВОВА ХАРАКТЕРИСТИКА КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ У СФЕРІ ВИКОРИСТАННЯ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНИХ МАШИН (КОМП'ЮТЕРІВ), СИСТЕМ ТА КОМП'ЮТЕРНИХ МЕРЕЖ І МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ

Кваліфікаційна робота (проєкт)
на здобуття ступеня вищої освіти «магістр»

Виконав: студент 2 курсу 13-282-Мз групи
Спеціальності 081 Право
Освітньо-професійної програми
«Право»

Дмитренко Денис Сергійович
Керівник: к.ю.н., доц. Проценко М.В.
Рецензент: к.ю.н., доц. Риженко І.М.

Херсон – 2020

ЗМІСТ

ВСТУП

Актуальність теми. Одним з головних завдань кримінального права є досконале визначення кола діянь, які є злочинами. Однією з перешкод на шляху до виконання цього завдання є стрімкий розвиток суспільних відносин, техніки (зокрема комп'ютерної), постійного накопичення людством інформації, кількість якої подвоюється кожні кілька років. Тому законодавець не завжди встигає за вказаними процесами. Особливо актуальними ці проблеми є для так званих «комп'ютерних злочинів».

Питання, пов'язані з Особливою частиною кримінального кодексу України, раніше були предметом досліджень таких вчених, як П.П. Андрушко, Ю.М. Батурін, П.Д. Біленчук, М.С. Вертузаєв, В.Г. Гончаренко, М.В. Гуцалюк, М.І. Панов, А.М. Ришелюк, Б.В. Романюк, Роботи вказаних вчених зробили значний внесок в розвиток правової науки, однак ряд проблем досліджена лише фрагментарно, деякі питання і досі залишаються дискусійними. Це проблемні питання, пов'язані з кримінально-правовим визначенням «комп'ютерних злочинів».

Мета і задачі дослідження. Метою дослідження є дослідження кримінальн-правового визначення кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Для досягнення даної мети були сформовані такі **завдання:**

– дослідити законодавче закріплення складів злочинів, що являють собою незаконне втручання в роботу комп'ютерних систем, в міжнародних правових актах;

– проаналізувати огляд зарубіжного законодавства про кримінальну відповідальність за незаконне втручання в роботу електронних систем;

– проаналізувати вітчизняне законодавство щодо кримінальної відповідальності за «комп’ютерні» злочини;

– дослідити об’єкт «комп’ютерних» злочину: проблеми кримінально-правового визначення;

– дослідити об’єктивна сторона «комп’ютерних злочинів»;

– проаналізувати суб’єкт «комп’ютерних злочинів»;

– дослідити суб’єктивна сторона «комп’ютерних злочинів».

Об’єктом дослідження є суспільні відносини, пов’язані із кримінально-правовою характеристикою кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку

Предметом дослідження є результати наукових досліджень, положення кримінального кодексу України щодо кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Методи дослідження враховують мету і завдання роботи, а також об’єкт і предмет дослідження. Основою дослідження є метод ідеалістичної діалектики, який є фундаментальним методом наукового пізнання.

При проведенні дослідження використовувались загально наукові методи: формально-юридичний, статистичний, порівняльно-правовий, системно-структурний, порівняльний, описовий, експериментальний, ряд логічних методів (аналізу, синтезу, індукції, дедукції, аналогії, версії та ін.).

Наукова новизна одержаних результатів полягає в тому, що представлена робота робить спробу комплексного дослідження кримінально-правової характеристики кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Практичне значення роботи - у виявленні основних проблемних питань щодо кримінально-правової характеристики кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Висновки, пропозиції та рекомендації, сформульовані автором у дослідженні, підлягають подальшому використаню при дослідженні вказаної теми, а окремі висновки та положення роботи – в процесі викладання навчальних дисциплін «Кримінальне право України», «Порівняльне кримінальне право та процес».

Публікації: Дмитренко Д.С. Законодавче закріплення складів злочинів, що являють собою незаконне втручання в роботу комп’ютерних систем, в міжнародних правових актах. *Актуальні дослідження правової та історичної науки (випуск 27)* : матеріали міжнародної науково-практичної інтернет-конференції / Збірник тез доповідей: випуск 27 (м. Тернопіль, 11 грудня 2020 р.). – Тернопіль, 2020. – 111 с.

Структура роботи враховує метоу та завдання дослідження і складається із вступу, двох розділів, які поділяються на чотири підрозділи, висновків, списку використаних джерел. Загальний обсяг роботи складає 57 с. Список використаних джерел налічує 45 найменувань.

РОЗДІЛ 1

Законодавство, що регламентує відповідальність за комп'ютерні злочини: порівняльно-правове дослідження

1.1. Законодавче закріплення складів злочинів, що являють собою незаконне втручання в роботу комп'ютерних систем, в міжнародних правових актах

Знання керують майже всіма компонентами західної цивілізації, майже нічого не відбувається без участі відповідної інформації. Отже, пошкодження комп'ютерних систем завдає шкоди ситуації в цілому, особливо компонентам, з якими пов'язана ця інформація.

Відповідно до ст. Стаття 10 Конвенції Ради Європи про захист фізичних осіб щодо автоматичної обробки персональних даних, підписаної у Страсбурзі 28 січня 1981 року, визначає основні принципи захисту даних, викладені у відповідному розділі.

У пункті 14 10-го звіту Комісії ООН з питань запобігання кіберзлочинності (далі 10-й Конгрес ООН), що відбувся у Відні 10-17 квітня 2000 р., Зазначено, що існують такі злочини:

Кіберзлочинність у вузькому розумінні. Будь-яка незаконна діяльність, що здійснюється за допомогою електронної діяльності, спрямованої на подолання захисту електронних систем - комп'ютерних даних.

Кіберзлочинність у її найширшому розумінні, тобто будь-яка незаконна діяльність, вчинена через комп'ютерні системи або мережі, включаючи такі злочини, як незаконне зберігання, надання або розповсюдження інформації через електронні мережі.

У висновках звіту Десятої комісії Конгресу викладені основні принципи розвитку ефективної боротьби з кіберзлочинністю.

Тому, на думку світового співтовариства, неможливо дати повну відповідь на кіберзлочинність без єдиного застосування норм та узгодження концепції, що регулює їх, ми вважаємо за доцільне посилатися на Конвенцію про кіберзлочинність, підписану 23 листопада 2001 року. Члени Ради Європи և інші країни (далі - Конвенція про кіберзлочинність). Конвенція зосереджена на усьому кіберзлочинному світі, який порушує як віртуальні об'єкти, так і традиційні злочини, яким може загрожувати незаконне втручання у функціонування комп'ютерних систем.

Частина I Конвенції про кіберзлочинність вперше описує комп'ютерні системи. Так, у пункті "a" ст. Стаття 1 Конвенції про кіберзлочинність говорить: "Комп'ютерна система означає будь-який пристрій або групу взаємопов'язаних або пов'язаних пристроїв, один або кілька з яких виконують автоматизовану обробку даних відповідно до поточної програми".

Частина II цього документа визначає заходи, які слід вжити сторонам Конвенції про кіберзлочини на національному рівні. У цьому розділі розглядається запропоноване кримінальне провадження щодо кіберзлочинності - учасників Конвенції Конвенції та держав, які бажають приєднатися до Конвенції, і включено до статті 1-4 цієї глави. Його розділи містять класифікацію кіберзлочинності. Приховані злочини, цілісність комп'ютерних даних існування систем (частина 1); комп'ютерні злочини (частина 2); Порушення вмісту даних (розділ 3); Злочини, пов'язані з порушенням авторських прав (Розділ 4).

Отже, Конвенція про кіберзлочинність II. Частина 1-2. Дії, зазначені в їх розділах, кваліфікуються як злочини. Що стосується інших діянь, то на національному рівні їх можна визначити як кримінальні чи адміністративні, цивільні чи інші злочини.

На наш погляд, Конвенція про кіберзлочинність II. Було б доцільним проаналізувати злочини, передбачені в главах 1 - 2 глави 1.

У розділі "Злочини проти конфіденційності, цілісності та доступності комп'ютерних систем даних" визначено такі злочини: "Незаконний доступ",

"незаконне вторгнення даних", "порушення цілісності даних", "втручання системи", "незаконне використання пристроїв".

Хоча Конвенція визначає правопорушення як "незаконний в'їзд" (стаття 2), в ньому зазначено, що "кожна сторона, навмисно виконавши її, вживає необхідних законодавчих та інших заходів для встановлення кримінального правопорушення згідно з її внутрішнім законодавством". користувач або будь-яка частина системи без її дозволу. Сторони мають право обходити заходи безпеки, вилучати комп'ютерні дані чи інші зловмисні наміри або вимагати криміналізації таких дій, якщо вони були скоєні у зв'язку з комп'ютерною системою, підключеною до іншої комп'ютерної системи. «

Конвенція про кіберзлочинність, яка передбачає кримінальну відповідальність за "незаконне вилучення даних" (стаття 3), стверджує, що втручання - це комп'ютерна система, яка здійснюється через або використовується цією системою, включаючи використання технічних перехоплень комп'ютерних даних. Сторони можуть вимагати криміналізації такого діяння, якщо воно було вчинене з нечесним умислом або у зв'язку з комп'ютерною системою, підключеною до іншої комп'ютерної системи. «

Пункт 4 Конвенції про кіберзлочинність пояснює злочин "порушення цілісності даних". Зміна або блокування даних комп’ютера без його дозволу.

Стаття 5 Конвенції про кіберзлочинність визначає злочин "втручання в роботу систем" таким чином:

Стаття 6 описує нещодавні правопорушення, які порушують "конфіденційність, безпеку" та доступ до електронної інформації відповідно до Конвенції про кіберзлочинність. Підкреслюється, що будь-яка Сторона вживає таких законодавчих та інших заходів, які можуть бути необхідними для оголошення кримінального правопорушення відповідно до її внутрішнього законодавства, будь то умисне чи незаконне: виробництво, продаж, придбання, імпорт, оптова торгівля. Інші види постачання.

1) Будь-який пристрій, розроблений або пристосований для злочину, зазначеного у статтях 2-5, включаючи комп'ютерне програмне забезпечення;

2) комп'ютерні паролі, коди або подібні дані, за допомогою яких можливий повний або частковий доступ до комп'ютерної системи з метою вчинення злочину, передбаченого статтями 2, 3, 4, 5.

Відповідно до другої частини конвенції наступною злочинною групою є "кіберзлочинність". До них належать: «Комп’ютерні з’єднання» (пункт 7) «Комп’ютерне шахрайство» (пункт 8).)

До категорії злочинів належать (глави 4 частини II Конвенції про кіберзлочинність), "Злочини, пов'язані з дитячою порнографією", "Злочини, пов'язані з порушенням авторських прав".

Зрозуміло, що такі правопорушення, в тому числі викладені в Конвенції про кіберзлочинність, можуть бути скоєні злочинами, зазначеними в розділі 1 "Злочини проти комп'ютерних даних, конфіденційність систем, цілісність та доступність". На наш погляд, ці соціально небезпечні види діяльності є злочинами, які перешкоджають роботі комп’ютерів, систем ьа комп’ютерних мереж (комп’ютерних систем).

Глобальні вимоги до боротьби з кіберзлочинністю включають необхідність розробки в кожній країні власних правил захисту від зазіхань на відомості, які збережені в автоматизованих системах. Цей інститут кримінального права в Україні ще недостатньо розвинений. Однак, поряд з розповсюдженням Інтернету та зростаючою загрозою комп’ютерних злочинів для суспільних інтересів України, законодавець повинен визначити коло комп’ютерних злочинів, чітко розробляючи правила, за якими можна буде притягнути до відповідальності відповідальних за їх комісія.

1.2. Огляд зарубіжного законодавства про кримінальну відповідальність за незаконне втручання в роботу електронних систем

Оскільки місцевий досвід боротьби з цими злочинами незначний, практика стосується лише немовляти, рекомендується вивчити законодавство зарубіжних країн, яке передбачає кримінальну відповідальність за дії, пов'язані з експлуатацією електронних мереж та систем.

У зарубіжній літературі питання про зв’язок того чи іншого акту з кіберзлочинністю досі є суперечливим; Для законних інтересів суспільства - прав, що захищаються державою :?

Швеція та США започаткували концепцію "кіберзлочинності" в 1970-х.

У Сполучених Штатах на федеральному рівні такими діями керує Федеральне відомство США з питань шахрайства, комп’ютерної обробки та зловживання у 1984 році. Закон, який передбачає криміналізацію несанкціонованого доступу до комп’ютерів. Комп’ютер на федеральному рівні означає будь-який комп’ютер, який використовується урядом або пов’язаними з ним фінансовими установами. Федеральний закон про конфіденційність у сфері комунікацій 1986 р. По-друге, навмисне порушення системи контролю за несанкціонованим доступом до системи та доступом до неї за допомогою інструментів, наданих агенціями електронних комунікацій Це означає. Відповідно до останнього, під умисним нападом розуміють несанкціонований доступ, при якому злочинець своїми діями отримує, змінює або блокує дозволений доступ до інформації, що зберігається в електронній системі в цій системі.

Крім того, у Сполучених Штатах комп'ютерна безпека на федеральному рівні регулюється Законом про комп'ютерне шахрайство та зловживання 1986 року (Закон про зловживання комп'ютерним шахрайством) 1986 року. І Закон про захист комп’ютера. 1987 (Закон про комп’ютерну

безпеку 1987), Закон про зловживання комп’ютером 1990 (Закон про зловживання комп’ютером 1990).

Як і в багатьох інших випадках, законодавство кожного штату США, яке передбачає криміналізацію кіберзлочинності, суттєво відрізняється.

Наприклад, у штатах Нью-Йорк, Вірджинія та Нью-Джадда злочин є офіційним, що означає, що відповідна дія вважається закінченою після завершення, а небезпечні соціальні наслідки не потрібні для характеристики дії.

Кримінальне законодавство Німеччини визначає такі складові "комп'ютерних злочинів": "Шпигунство інформації" (202a), "комп'ютерне шахрайство" (263a), "підробка речових доказів" (296), "шахрайство в юридичній діяльності, пов'язаній із процесуальними операціями" (270), «Зміна інформації» (303a)), «Комп’ютерний саботаж» (303b) (14, с. 28): Відповідальність за порушення інформації Поява комп’ютерних вірусів, регламентована ст. 202a, 303a, 303б Кримінального кодексу Німеччини [1].

Відповідно до норвезького законодавства, кіберзлочинність включає "несанкціонований доступ до комп'ютерної системи", "саботаж комп'ютерів", "шпигунство комп'ютерів", "комп'ютерне шахрайство", "незаконне копіювання програм", "злочини, злочини". про розповсюдження незаконної інформації »(порнографія, расистська література).

Новий французький кримінальний кодекс, який набув чинності 1 березня 1994 р., Радикально змінив національне законодавство про відповідальність за кіберзлочинність. Це інформаційні злочини, статті, що містять санкції за злочини, пов’язані з даними [14].

За даними Центру з вивчення комп’ютерних злочинів, рівень розкриття та розкриття злочинів, скоєних правоохоронними органами за кордоном із використанням сучасних інформаційних технологій, постійно зростає. Кількість кіберзлочинів, виявлених у Німеччині, неухильно зростає з 1991 року. У 1997 р. В цій країні було зареєстровано 39 331 комп'ютерних злочинів, а в 1998 р. - на 14,5% - до 46 022; Кількість кіберзлочинів у Франції

щороку зростає на 30-40%; (...); Тільки в 1999 році ФБР розслідувало понад 500 випадків кіберзлочинності в США, крім дитячої порнографії. [36]

На наш погляд, ефективне реагування на "кіберзлочинність" у розвинених зарубіжних країнах не принаймні обумовлене бездоганним правовим регулюванням відповідальності за комп'ютерні системи за незаконні посягання на комп'ютерну інформацію.

1.3. Аналіз вітчизняного законодавства щодо кримінальної відповідальності за «комп'ютерні» злочини

Доцільно вивчити вітчизняне законодавство про кримінальну відповідальність за "комп'ютерні" злочини.

Місцеве законодавство у галузі комп'ютерних технологій почало визначати кримінальні правопорушення набагато пізніше законодавства більш розвинених „західних" країн. І причин є кілька. На думку автора, найбільш вирішальним з них є відносно невеликий розподіл комп'ютерів у нашій країні протягом перших років незалежності. Відносно низька кількість цих злочинів, скоєних у цей період. Довготривале існування в нашому колишньому кримінальному законодавстві, яке Україна успадкувала від СРСР (це законодавство головним чином було спрямоване на боротьбу з будь-якими посяганнями на радянську систему - розкраданням державного майна) тощо.

5 липня 1994 року Верховна Рада України прийняла Закон про захист інформації в автоматичних системах, який мав на меті створити основу для регулювання відносин проти порушення інформації, що міститься в автоматизованих системах. Цей закон застосовується до будь-якої інформації, що обробляється в автоматизованих системах. Він гарантує правовий захист від навмисних або ненавмисних втрат, знищення, фальсифікації, спотворення, блокування інформації, авторських прав на

інформацію або прав автоматизованої системи чи інших незаконних дій, встановлених за контрактними відносинами (стаття 5).

Поправка до Спеціального розділу Кримінального кодексу України 1994 року включала пункт, який передбачав "відповідальність за умисне втручання в роботу автоматизованих систем, що призвело до нейтралізації або знищення комп'ютерної інформації чи носіїв інформації, або розповсюдження програмного або апаратного забезпечення". Він призначений для втручання в автоматизовані системи ն має здатність порушувати або знищувати інформацію або носій інформації. «

У другій половині 90-х років XX ст. Місцеве законодавство доповнило низку нормативно-правових актів, спрямованих на захист інформації в цілому, зокрема, на боротьбу з «кіберзлочинністю». Серед них, насамперед, Закон України "Про інформацію" від 2 жовтня 1992 р. [44]; Український акт про науково-технічну інформацію від 25 червня 1993 р. [45] та ін.

Раціональне прагнення розвитку законодавства для забезпечення взаємозв'язку юридичних знань стало реальною можливістю захистити кримінальне право швидко розвиваються комп'ютерних систем в Україні та в усьому світі.

Кримінальний кодекс України від 5 квітня 2001 року (далі - Кримінальний кодекс України) передбачає кримінальну відповідальність за "незаконне втручання в роботу комп'ютерів (комп'ютерів), систем та комп'ютерних мереж" (ст. 361 Кримінального кодексу України), наприклад, за крадіжку. зловживання. за використання, вимагання або шахрайство чи неправомірне використання комп’ютерної інформації» (ст. 362 Кримінального кодексу України). Стаття 363 Кримінального кодексу України базується на нормах Конституції України загальновизнаних принципів міжнародного права. Він передбачає відповідальність за "порушення правил, що регулюють роботу автоматизованих комп'ютерних систем".

Стаття 361 Кримінального кодексу України передбачає відповідальність за „незаконне втручання в роботу автоматизованих комп'ютерів, їх систем або комп'ютерних мереж, що призвело до спотворення або знищення комп'ютерної інформації чи носіїв інформації, а також за поширення комп'ютерних вірусів . використанням програмного та апаратного забезпечення, призначеного для незаконного проникнення на ці машини, системи або комп'ютерні мережі та здатних спричинити спотворення або знищення комп'ютерної інформації чи носіїв такої інформації.

На відміну від Кримінального кодексу України 1960 року, ця норма більше відповідає реаліям сьогодення. Роман [38] та його значним досягненням є кримінальна відповідальність, передбачена законодавцем за поширення комп'ютерного вірусу [39], який ст. 1981 Кримінального кодексу України 1960 р. Прямо не передбачав.

Кваліфікаційні ознаки частини 2 цієї статті передбачають заподіяння значної шкоди, зазначеної в частині 1 статті (1), повторне вчинення таких дій (2), вчинення цих дій за попередньою змовою групою осіб (3) .

Стаття 362 Кримінального кодексу України передбачає відповідальність за хакерські дії, які не спрямовані на спотворення, знищення або розповсюдження вірусів за допомогою програмного та апаратного забезпечення, призначеного для проникнення в автоматизовані системи та здатного спотворювати або знищувати інформацію або її носії, який з альтернативних діянь передбаченої ним об'єктивної сторони злочину називається крадіжкою комп'ютерної інформації [40].

При викраденні, відповідно до змісту ст. 362 Кримінального кодексу України, слід розуміти як викрадення комп'ютера, пограбування або крадіжку, за умови, що вони були скоєні з метою вилучення комп'ютерної інформації, що зберігається на носіях, до яких належать системні блоки, жорсткі диски, м'які диски, компакт-диск та така інформація перебував у володінні іншої особи.

Інші альтернативні дії, передбачені статтею 362 Кримінального кодексу України, включають: привласнення, вимагання комп'ютерної інформації, заволодіння нею шляхом шахрайства, вчинення шляхом зловживання службовим становищем.

Однак отримання комп'ютерної інформації шляхом шахрайства також може бути «хакерською» дією. Поширені випадки, коли користувачі, придбавши компакт-диск, після багаторазового використання (ігри, бази даних), в меню диска знайшли примітки, що при використанні цієї програми відбувається копіювання та надсилання власної інформації про користувача.

Ознаками кваліфікованого персоналу, передбаченого частиною 2 статті 362 чинного Кримінального кодексу України, є вчинення цих дій неодноразово (1), або за попередньою домовленістю групи осіб (2); для частини 3 - заподіяння значної шкоди цими діями.

З прийняттям нового Кримінального кодексу України виділяється розділ XYI "Злочини при використанні автоматизованих комп'ютерів (комп'ютерів), систем та комп'ютерних мереж" та включення трьох досить прогресивних, на наш погляд, статей. можливість фактично переслідувати винних у скоєнні комп'ютерних злочинів.

Норми, передбачені ст. 361-362 Кримінального кодексу України належать до банкету, у зв'язку з тим, що зміст певних особливостей таких норм передбачено нормативними актами галузевого законодавства [31].

Однак Кримінальний кодекс України 2001 року прямо (прямо) не передбачає відповідальності за значну кількість актів хакерів. Так, не несе відповідальність за телефонні шахрайства, розповсюджувачі комп'ютерної порнографії, комп'ютерне піратство, комп'ютерні саботажі тощо

Експерти вносять пропозиції щодо доповнення Кримінального кодексу України нормою, яка передбачала б кримінальну відповідальність за «Порушення порядку обігу апаратних та програмних засобів, призначених для отримання несанкціонованого доступу до комп'ютерів, автоматизованих систем та комп'ютерних мереж» [17]. Це слушна пропозиція, враховуючи

необхідність законодавчого врегулювання відповідальності за навмисне розповсюдження програмного та апаратного забезпечення, призначеного для несанкціонованого доступу до комп’ютерів, їх систем та комп’ютерних мереж, включаючи комп’ютерні віруси, оскільки такі дії сприяють не лише вчиненню інших злочинів пов'язані з несанкціонованим доступом до комп'ютерів, систем або комп'ютерних мереж, але можуть також спровокувати їх вчинення.

Для правильного тлумачення існуючих трьох статей Кримінального кодексу України з метою правильного їх застосування недостатньо використовувати тлумачення ст. 1981 р. Кримінального кодексу України 1960 р. З метою вдосконалення законодавства у галузі захисту високих технологій необхідна якнайшвидша наукова та достовірна інтерпретація цих норм, а також їх складових.

Ряд питань, що стосуються належної класифікації комп’ютерних злочинів, не лише позбавляють правоохоронні органи можливості переслідувати винних, а й порушують права людини: як потерпілого, якого позбавляють компенсації, так і винного, котрий часто притягується до відповідальності за іншого злочин, а тому вимагає модернізації [22].

«Порівняльний аналіз показує, що законодавство України в галузі інформаційних відносин має ряд недоліків: по-перше, різні закони та підзаконні акти, що регулюють суспільні відносини, об’єктом яких є інформація, прийняті в різний час без належної координації понятійного апарату. Вони мають ряд термінів, які є недостатньо правильними, не викликають однозначного відображення публічної інформації або не мають чіткого визначення їх змісту. Термінологічні неточності та різні тлумачення подібних за формою та змістом понять та категорій призводять до їх неоднозначного розуміння та застосування на практиці, що спричиняє соціальну ентропію (невизначеність). Це, в свою чергу, породжує соціальні конфлікти в інформаційних відносинах та правовий хаос; у галузі боротьби зі злочинністю створені умови для можливих маніпуляцій при визначенні ознак

злочину, а це, в свою чергу, дозволяє правопорушникам уникати відповідальності; по-друге, велика кількість законодавчих та нормативних актів у галузі інформаційних відносин ускладнює їх пошук, аналіз та координацію для практичного застосування, особливо правоохоронцями у боротьбі з кіберзлочинністю, і особливо такої, що має характеристики організованості. Це призводить до зниження рівня виявлення, розкриття та передачі до суду кримінальних справ про такі злочини в Україні» [36].

На наш погляд, сьогодні в Україні практичне застосування норм, що визначають злочини, що становлять незаконне втручання в роботу електронних комп'ютерів (комп'ютерів), їх систем та комп'ютерних мереж, не ефективно з наступних причин:

1) українське законодавство недостатньо відповідає міжнародним стандартам щодо визначення комп'ютерних злочинів загалом, а також злочинів, що становлять незаконне втручання в роботу комп'ютерів, їх систем та комп'ютерних мереж зокрема;

2) обізнаність суб'єктів правовідносин у сфері використання комп'ютерної інформації низька, що є однією з причин латентності комп'ютерної злочинності в Україні;

3) у межах ст. 361 Кримінального кодексу України поєднує дві юридичні складові злочинів, які визначені як незалежні як на міжнародному рівні, так і на рівні законодавства окремих держав, а саме - "Несанкціонований доступ до комп'ютерної інформації" та "Умисне розповсюдження зловмисних комп'ютерні програми ", яку український законодавець визначає як види соціально небезпечних діянь у межах об'єктивної сторони злочину, передбаченого ст. 361 Кримінального кодексу України. У цьому випадку одна з них повинна мати соціально небезпечні наслідки, і не передбачається, що це відбудеться по відношенню до іншої. Таке визначення, звичайно, буде важким при практичному застосуванні цього правила;

4) ст. 361 Кримінального кодексу України є новинкою кримінального законодавства, однак є фактичною трансформацією свого попередника - ст. 1981 КК України 1960 р. В чинному КК України. Однак його формулювання містить логічні неточності, що може призвести до труднощів при кваліфікації соціально небезпечних актів несанкціонованого доступу до комп'ютерної інформації та навмисного розповсюдження шкідливих комп'ютерних програм на практиці;

5) у колі соціально небезпечних дій, які український законодавець пов'язує з незаконним втручанням у роботу електронних комп'ютерів (комп'ютерів), їх систем та комп'ютерних мереж, немає таких небезпечних дій, як навмисне розповсюдження шкідливих комп'ютерних програм, різних в характеристиках від комп’ютерного вірусу, за поширення якого передбачена кримінальна відповідальність;

6) як один із альтернативних наслідків несанкціонованого доступу до комп’ютерної інформації законодавець не передбачає витоку комп’ютерної інформації, тобто настання такого наслідку не кримінально карається в Україні, якщо акти не містять ознак іншого злочин, такий як шпигунство;

Цей список не є вичерпним. Очевидна наявність цих причин свідчить про необхідність детальної всебічної кримінально-правової характеристики незаконного втручання у роботу комп’ютерів.

Все частіше з розвитком високих технологій кількість незаконних посягань на комп’ютерні системи та комп’ютерну інформацію, що зберігається в них, щодня збільшується. Сьогодні особливу увагу потрібно приділити аналізу таких комп’ютерних злочинів, які можуть бути вчинені як окремо (у поєднанні), так і в поєднанні з іншими злочинами, виступаючи як спосіб вчинення останніх. Комп’ютерні злочини також можуть бути скоєні для сприяння скоєнню або приховування іншого (іншого) злочину (злочинів).

Комп’ютерна злочинність або кіберзлочинність може бути визначена як будь-яке протиправне діяння, в якому комп’ютери, комп’ютерні системи

чи комп'ютерні мережі, комп'ютерна інформація чи носії є предметом чи інструментом злочинного діяння. .

Комп'ютерна злочинність є різновидом транснаціональної злочинності, а злочини, що посягають на безпеку комп'ютерних систем, є транснаціональними.

Боротьба з кіберзлочинністю у світі ускладнюється тим, що налагодити правовий порядок у роботі Всесвітньої павутини, яка є основним засобом транснаціональної комунікації, поки не повністю можливо, оскільки мережа не має фізичних географічних кордонів, та інформація, яка передається, важко оцінюється, контролюється, а в деяких країнах, зокрема в Україні, має недоліки у щодо визначення правового статусу.

Недоліки юридичного визначення концептуальної бази та норм, що регулюють відповідальність за комп'ютерні злочини, є основною проблемою, яка ускладнює боротьбу із ними. Таким чином, для ефективного протистояння вказаним злочинним проявам відповідне законодавство має бути вдосконалене.

Для приведення вітчизняної нормативної бази та уніфікації визначення кримінальної відповідальності за кіберзлочинність міжнародними організаціями розроблено та ухвалено нормативні акти, які закріплюють не лише склади комп'ютерних злочинів, а й визначають базові поняття щодо протистояння ним. До них належать, зокрема, Рекомендації Комітету з правових питань Ради Європи, які містять мінімальний (обов'язковий) зразок (факультативний) перелік рекомендованих для закріплення у внутрішньому законодавстві європейських країн; Рекомендації Десятого конгресу ООН з питань запобігання злочинності та поводження з правопорушниками (Відень, 10-17 квітня 2000 р.); Конвенція Ради Європи про кіберзлочинність (Страсбург, 23 листопада 2001 р.). Положення цих актів містять низку відмінностей, які на практиці можна узгодити лише шляхом внесення змін до національного законодавства.

Недоліки у нормативно-правовому визначенні основних видів злочинів, що посягають на безпеку комп’ютерних систем у країнах колишніх радянських республік, зумовили необхідність прийняття загальних заходів, які б дозволили гармонізувати такі формулювання. 1 червня 2001 р. Було підписано Угоду про співробітництво держав-членів Співдружності Незалежних Держав у боротьбі зі злочинами в галузі комп'ютерної інформації, в якій сторони визнають наступні дії кримінально караними за національним законодавством, якщо вони вчинені навмисне: незаконний доступ до захищеної законом комп’ютерної інформації, якщо він завдав шкоду роботі комп’ютера, комп’ютерної системи або їх мережі особою, яка має доступ до комп’ютера, комп’ютерної системи або їх мережі, що спричинило знищення, блокування або модифікацію охоронюваної законом інформації, якщо цей вчинок спричинив значне пошкодження або серйозні наслідки; незаконне використання комп’ютерних програм та баз даних, які є об’єктами авторського права, а також присвоєння авторства, якщо це спричинило значну шкоду.

Застосуванню в Україні законодавства щодо протидії комп’ютерним злочинам заважає низка наступних факторів:

1. Невідповідність вітчизняного законодавства міжнароднм стандартам щодо регламентації комп'ютерних злочинів взагалі та злочинів, являють собою незаконне втручання в роботу комп'ютерів, їх систем та комп'ютерних мереж зокрема.

2. Відносно низький рівень обізнаності суб’єктів правовідносин у сфері користування комп’ютерною інформацією, що з одного боку «полегшує роботу» злочинцям у вказаній сфері, а з іншого – призводить до латентності комп’ютерної злочинності в Україні;

3. Стаття 361 Кримінального кодексу України об’єднує різні юридичні складові злочинів, які визнані самостійними як на міжнародному рівні, так і на рівні законодавства окремих держав, а саме – «Несанкціонований доступ до комп'ютерної інформації» та «Навмисне розповсюдження шкідливих

комп'ютерних програм», які визначаються як види соціально небезпечних діянь у межах об’єктивної сторони злочину, передбаченого ст. 361 Кримінального кодексу України. У цьому випадку для одного з них передбачено обов’язкове настання соціально небезпечних наслідків, а для іншого - відсутність. Таке визначення, звичайно, створить труднощі при практичному застосуванні цього правила;

4. Ст. 361 Кримінального кодексу України є новинкою кримінального законодавства, однак є фактичною трансформацією відповідної статті, яка існувала в Кримінальному кодексі України 1960 р. В чинному КК України. Зазначене визначення містить у собі недоліки які заважають правильно кваліфікувати соціально небезпечні акти несанкціонованого доступу до комп'ютерної інформації та навмисного розповсюдження шкідливих комп'ютерних програм на практиці;

5. У колі соціально небезпечних дій, які український законодавець пов'язує з незаконним втручанням у роботу електронних комп'ютерів (комп'ютерів), їх систем та комп'ютерних мереж, немає таких небезпечних дій, як навмисне розповсюдження шкідливих комп'ютерних програм, які по своїй суті не є комп’ютерними вірусами, за поширення яких вітчизняним законодавцем передбачене настання кримінальної відповідальності.

6. Вітчизняним законодавцем не передбачено витоку інформації з комп’ютерних мереж та систем, тобто вчинення актів незаконного втручання в роботу комп’ютерів, систем та комп’ютерних мереж, що спричиняє «витік» інформації з комп’ютерів інформації про їх користувачів. Останні кримінальні правопорушення набувають усе більшої суспільної небезпечності, оскільки все більше інформації про громадян України потрапляє в суспільні мережі, усе більше сервісів «переходить» від «паперової» форми в «електронну» з відповідним збереженням в електронному вигляді інформації про громадян, підприємства, установи та організації.

7. Вітчизняне законодавство не містить визначення комп’ютерної інформації.

РОЗДІЛ 2
ОБ’ЄКТИВНІ ОЗНАКИ «КОМП’ЮТЕРНИХ» ЗЛОЧИНІВ

2.1. Об’єкт «комп’ютерних» злочину: проблеми кримінально-правового визначення

Правове забезпечення захисту будь-яких товарів, цінностей або суспільних відносин, як їх елемент, є основою механізму правового регулювання, завдяки якому правовий порядок підтримується в державі.

Правильне визначення об’єкта злочину має своє практичне значення, оскільки помилка в ньому унеможливлює правильну кримінально-правову кваліфікацію вчиненого діяння.

Дослідження об'єкта злочину у вітчизняній теорії кримінального права проводиться спільно з предметом злочину.

Найбільш розповсюдженою є класифікація об’єктів злочину на загальні, загальні та прямі.

Теорія кримінального права має суперечливі погляди на загальне визначення об'єкта злочину. Прямими, а також загальними та родовими об'єктами можуть бути лише соціальні відносини, а не товари та цінності, спроба замінити соціальні відносини, які є об'єктом злочину, будь-якими іншими соціальними явищами є помилковими.

Також до об’єкту злочину можна віднести цінності, що охороняються законодавством, на які посягає злочинне діяння.

Родовим об'єктом злочинів глави XVI Кримінального кодексу України "Злочини при використанні електронних комп'ютерів (комп'ютерів), систем та комп'ютерних мереж" деякі вчені визнають зв'язки з громадськістю у сфері комп'ютерної інформаційної безпеки та належне функціонування електронні комп’ютери (комп’ютери), їх системи та комп’ютерні мережі.

Водночас, конкретизуючи родовий об’єкт злочинів при використанні комп’ютерів, їх систем та комп’ютерних мереж, ми вважаємо за необхідне

включити у визначення загального об’єкта розділу XVI Кримінального кодексу України вказівку на комп’ютерні носії інформації концентрація комп’ютерної інформації.

Таким чином, родовий об’єкт злочинів, відповідальність за які передбачена ст. 361-363 Кримінального кодексу України доцільно враховувати зв’язки з громадськістю у сфері безперебійної та стабільної роботи електронних комп’ютерів (комп’ютерів), їх систем та комп’ютерних мереж та забезпечувати безпеку та цілісність комп’ютерної інформації та засобів масової інформації .

Що стосується визначення безпосереднього об’єкта, то вони визнають у теорії кримінального права, зокрема, ті соціальні цінності, на які посягає конкретне злочинне діяння або бездіяльність [29]. Однак, ґрунтуючись на чітко визначеному раніше визначенні об’єкта злочинного посягання як відносин у суспільстві, що охороняється кримінальним законодавством, ми не погоджуємося з цим тлумаченням і вважаємо за доцільне розуміти об’єкт, на який посягає злочинець, для розуміння громадськості відносини, постраждалі від певного злочину.

Законодавцем та науковцями не конкретизовано безпосередній об’єкт злочину, передбаченого ст. 361 Кримінального кодексу України. Важкість визначення безпосереднього об’єкту вказаного злочину пов’язана у першу чергу із ти, що у відповідній статті Особливої частини КК України передбачено настання кримінальної відповідальності фактично два окремих діяння, а саме за незаконний доступ до інформації, яка міститься у комп’ютерах, та умисне розповсюдження (можливе різними способами) програмного забезпечення, яке шкодить комп’ютерам та інформації, яка міститься у них.

Різниця між вказаними двома окремими групами діянь логічно викликає необхідність виділити два різні безпосередні об’єкти злочинного посягання, а саме:

1. Щодо кримінального правопорушення першої групи, то безпосереднім об’єктом виступає право власника або володільця (особи, яка користується) на виключних доступ комп’ютерів та/або їх систем, завдяки існуванню та захисту якого забезпечується захист комп’ютерного устаткування та наявної у ньому інформації, які перебувають у його власності та/або користуванні.

2. Щодо умисного розповсюдження шкідливих комп’ютерних програм, то тут ситуація з безпосереднім об’єктом дещо інша. Безпосереднім об’єкту вказаних кримінальних правопорушень виступає право особи, у володінні та/або користуванні перебувають комп’ютери та інформація, яка міститься у них, на забезпечення цілісності та збереження інформації та/або її носія.

Системний аналіз змісту норм ст. 41 Конституції України, Закону України «Про інформацію» дозволяє зробити висновок про те, що інформація в нашій країні може бути предметом майнових прав громадян, юридичних осіб та держави, може бути предметом повного володіння, а також предметом володіння, користування чи розпорядження як складових речових прав.

Таким чином, право володіти та розпоряджатися комп'ютерною інформацією є безпосереднім предметом юридичного складу злочину «Несанкціонований доступ до комп'ютерної інформації».

Право власника (володільця) на використання комп'ютерної інформації є безпосереднім предметом злочину «Навмисне розповсюдження шкідливих комп'ютерних програм».

Майнові права, ексклюзивний доступ та авторське право на комп'ютерну інформацію та/або комп'ютерні системи ставляться під загрозу у результаті втручання в інформаційну безпеку людей, суспільства та держави [23].

Нажаль, вітчизняне законодавство не містить прямих вказівок на існування і, відповідно, захист права власності на комп’ютерну інформацію

на відміну від існування законодавчого закріплення права власності на комп’ютерну систему як об’єкт матеріального світу, яке чітко визначає Конституція.

Після чисельних внесених змін до «статті 1 Закону України «Про авторське право та суміжні права» частково внесені визначення наступних предметів посягання у ході несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку: 1. База даних (компіляція даних) - сукупність творів, даних або будь-якої іншої незалежної інформації у довільній формі, в тому числі - електронній, підбір і розташування складових частин якої та її упорядкування є результатом творчої праці, і складові частини якої є доступними індивідуально і можуть бути знайдені за допомогою спеціальної пошукової системи на основі електронних засобів (комп’ютера) чи інших засобів. 2. Веб-сайт - сукупність даних, електронної (цифрової) інформації, інших об’єктів авторського права і (або) суміжних прав тощо, пов’язаних між собою і структурованих у межах адреси веб-сайту і (або) облікового запису власника цього веб-сайту, доступ до яких здійснюється через адресу мережі Інтернет, що може складатися з доменного імені, записів про каталоги або виклики і (або) числової адреси за Інтернет-протоколом. 3. Веб-сторінка - складова частина веб-сайту, що може містити дані, електронну (цифрову) інформацію, інші об’єкти авторського права і (або) суміжних прав тощо. 4. Електронна (цифрова) інформація - аудіовізуальні твори, музичні твори (з текстом або без тексту), комп’ютерні програми, фонограми, відеограми, програми (передачі) організацій мовлення, що знаходяться в електронній (цифровій) формі, придатній для зчитування і відтворення комп’ютером, які можуть існувати і (або) зберігатися у вигляді одного або декількох файлів (частин файлів), записів у базі даних на зберігаючих пристроях комп’ютерів, серверів тощо у мережі Інтернет, а також програми (передачі) організацій мовлення, що ретранслюються з використанням мережі Інтернет. 5. Комп’ютерна програма - набір інструкцій

у вигляді слів, цифр, кодів, схем, символів чи у будь-якому іншому вигляді, виражених у формі, придатній для зчитування комп'ютером, які приводять його у дію для досягнення певної мети або результату (це поняття охоплює як операційну систему, так і прикладну програму, виражені у вихідному або об'єктному кодах). 6. Обліковий запис – формалізований згідно зі стандартами мережі Інтернет запис на комп'ютерному обладнанні (комп'ютерах, серверах), підключеному до мережі Інтернет, що ідентифікує користувача (наприклад, власника веб-сайту) на такому обладнанні, включає в себе дані про доступ до частини каталогів і програмного забезпечення комп'ютерного обладнання, а також визначає права такого доступу, що надають можливість володільцю облікового запису додавати, видаляти, змінювати електронну (цифрову) інформацію і дані веб-сайту, надавати доступ до веб-сайту або його частин, окремих даних іншим особам, припиняти функціонування такого веб-сайту або його частини в межах облікового запису» [42].

Однак дотепер у вітчизняному законодавстві відсутнє визначення власника комп'ютерної інформації.

Слушним удається системний аналіз законодавства про інформацію на предмет визначення власника зазначеної інформації.

Так, згідно ст. 4 Закону України «Про інформацію», суб'єктами інформаційних відносин є:

1. Фізичні особи.

2. Юридичні особи.

3. Об'єднання громадян.

4. Суб'єкти владних повноважень.

Отже, системний аналіз законодавства України про власність та про інформацію дозволяє надати наступне визначення власника комп'ютерної інформації: громадяни, юридичні особи та держава, які володіють, користуються та розпоряджається комп'ютерами, комп'ютерними мережами та системами.

Поняття «користувач комп'ютерної інформації» не визначено у вітчизняному законодавстві, хоча, на наш погляд, таке визначення є суттєвим для практичного застосування норм кримінальної відповідальності за незаконне втручання в комп'ютерні системи. Перш за все, це важливо при визначенні розміру шкоди, спричиненої втручанням у роботу комп'ютерних систем, як матеріальною, так і моральною. Таким чином, користувачі, які набувають право на використання певної інформації на платній основі, втрачаючи таке право через пошкодження цієї інформації, зазнають матеріальної шкоди.

Щодо ідентифікації осіб, які зазнали шкоди від скоєння злочинних дій, слід зазначити, що такими можуть бути особи, які згідно чинного законодавства набули майнові права або права на використання комп'ютерних систем чи комп'ютерної інформації, які соціально небезпечні дії, передбачені ст. 361 Кримінального кодексу України, заподіяно шкоду. Такі особи, відповідно до ст. 49 Кримінально-процесуального кодексу України повинні бути визнані жертвами злочину,

На наш погляд, слід зазначити, що жертви несанкціонованого доступу до комп'ютерної інформації можуть бути визнані лише власниками та користувачами такої інформації, тоді як жертви навмисного розповсюдження шкідливих комп'ютерних програм можуть бути власниками та користувачами як комп'ютер. комп'ютерна інформація та комп'ютерні системи, включаючи Інтернет, якщо такі системи або їх програмне забезпечення були пошкоджені негативним впливом шкідливих програм.

2.2. Об'єктивна сторона «комп'ютерних злочинів»

З об'єктивної точки зору, як зазначалося раніше, злочин, передбачений статтею 361 Кримінального кодексу України, виражається у двох альтернативних активних діях:

1. Незаконне втручання в роботу АЕОМ, їхніх систем або комп'ютерних мереж, що призвело до спотворення або знищення комп'ютерної інформації чи носіїв такої інформації, яку ми попередньо визначили як «Несанкціонований доступ до комп'ютерної інформації»;

2. Поширення комп'ютерного вірусу [32].

Що стосується актів втручання в роботу комп'ютерних систем, то зауважимо, що в якості своїх обов'язкових ознак законодавець передбачає:

1) дії, які полягають у незаконному втручанні в роботу електронних комп'ютерів, їх систем та комп'ютерних мереж;

2) настання альтернативних соціально небезпечних наслідків у вигляді:

- спотворення комп'ютерної інформації;

- знищення комп'ютерної інформації або її носіїв;

3) причинний зв'язок між діянням та наслідками.

Як вже зазначалося вище, юридичний зміст та форма вказані діянь є різними. З огляду на зазначене, слушним удається виділення самовільного, незаконного доступу до інформації, яка міститься у комп'ютерних мережах і системах, а також умисного розповсюдження комп'ютерних програм, які спричиняють їм шкоду, як два самостійні склади злочинів. Кожне з цих з цих діянь по суті утворює окремий склад злочину і має бути представлене в окремих статтях Особливої частини Кримінального кодексу України.

Характерним є те, що вказана норма залишилась сучасній Україні «у спадщину» від Кримінального Кодексу України 1960 р. Таке «запозичення» удається тим більше помилковим, що з моменту введення відповідної статті до Кримінальної Кодексу України 1960 р. комп'ютерні технології і, відповідно «комп'ютерні злочини» зазнали істотних та принципових змін.

Разом із визначенням зазначеного складу злочину, до КК України 2001 р. перейшов і головний недолік вказаної статті: невдала спроба поєднання в один склад злочину два окремих види посягання із різним об'єктом та об'єктивною стороною.

Отже необхідність виділення цих двох зазначених види посягань в різні склади злочинів назріло давно – зокрема, для максимального спрощення формулювань, які містяться у кримінальному законі, його максимальне уточнення, чіткість та лаконічність.

Крім зазначених вище причин необхідність виділення зазначених діянь у різні склади злочинів обумовлені також наступними причинами:

1. Уникнення зайвої змістовної «перезавантаженості» окремої статті Особливої частини Кримінального кодексу України.

2. Персоналізація покарання відповідно до рівня суспільної небезпеки кожного конкретного виду кримінального правопорушення (не в останню чергу через різницю в об’єкті посягання та об’єктивній стороні).

Закон України «Про інформацію» [43] розмежовує конфіденційну та конфіденційну інформацію як типи інформації з обмеженим доступом, надаючи їм особливий статус та особливий захист.

Таким чином, конфіденційна інформація, відповідно до ст. 30 Закону України «Про інформацію» - це «інформація, яка перебуває у володінні, користуванні або розпорядженні фізичних або юридичних осіб та поширюється на їх запит відповідно до передбачених ними умов» [43].

Щодо конфіденційної інформації, цей Закон у абз. 3 вул. 30 передбачає, що громадяни, юридичні особи, які мають інформацію професійного, ділового, виробничого, банківського, комерційного та іншого характеру, отриману за власні кошти, або таку, що є предметом їх професійних, господарських, виробничих, банківських, комерційних та інших інтересів і не порушує передбачену законом таємницю, самостійно визначає режим доступу до нього, включаючи належність до категорії конфіденційних, та встановлює систему (методи) захисту для нього.

До секретної інформації, відповідно до абз. 3 вул. 30 цього Закону є такою, що "містить інформацію, що становить державну та іншу таємницю, передбачену законом, розголошення якої завдає шкоди людині, суспільству та державі". Порядок обігу секретної інформації та її захист, відповідно до

Закону "Про інформацію", визначається відповідними державними органами за умови дотримання вимог, встановлених Законом України "Про інформацію" [43].

Відповідно до позиції законодавця, ми вважаємо, що концепція доступу, як певні правила отримання можливості безпосереднього контакту з певним об’єктом, повинна застосовуватися до будь-якого об’єкта права власності, включаючи комп’ютерну інформацію та комп’ютерні системи.

Відповідно до ст. 41 Конституції України кожен має право володіти, користуватися та розпоряджатися своїм майном, результатами своєї інтелектуальної, творчої діяльності [31]. Тобто кожен власник комп’ютерної інформації вільний встановлювати спеціальний режим доступу до неї, крім випадків, передбачених чинним законодавством України.

Однак відповідно до умов встановлення доступу до конфіденційної інформації, передбачених ст. 30 Закону України "Про інформацію", «такий режим може встановлюватись власником такої інформації (фізичною чи юридичною особою) на свій розсуд, а не регулюватися конкретними правовими нормами щодо такого захисту» [43].

Отже, під режимом доступу до інформації розуміється сукупність конкретних правил, встановлених власником комп’ютерної інформації, які регламентують порядок отримання, використання, розповсюдження та зберігання комп’ютерної інформації, що не суперечить чинному законодавству.

У цьому розділі вони розглянуть особливості об’єктивної сторони однієї з правових структур, які описані законодавцем у диспозиції ч. 1 ст. 361 Кримінального кодексу України, а саме незаконне втручання у роботу комп’ютерів, їх систем та комп’ютерних мереж, що призвело до спотворення або знищення комп’ютерної інформації чи носіїв такої інформації, яку ми умовно називаємо „Несанкціонований доступ до комп’ютерної інформації” [32].

М. С. Вертузаєв, В. О. Голубєв, О. І. Котляревський, О. М. Юрченко зазначають: «Втручаючись у роботу АС, законодавець пропонує зрозуміти будь-які дії винного, що впливають на обробку інформації в АС. зберігаються, або вводяться або передаються для обробки в АС, тобто дії, що впливають на весь набір операцій (збір, введення, запис, перетворення, зчитування, зберігання, знищення, реєстрація), що здійснюються за допомогою апаратного та програмного забезпечення, включаючи обмін на канали передачі даних. При втручанні в роботу АС відбувається порушення її роботи, що спричиняє спотворення процесу обробки інформації, що призводить до спотворення або знищення самої інформації або її носіїв інформації» [15].

Що стосується цього визначення, не можна не згадати два моменти.

По-перше, недоцільно вказувати на обов'язковий негативний вплив на всю сукупність операцій, оскільки вплив може бути спрямований на будь-який з видів обробки інформації або будь-який набір цих типів. У той же час, вищезазначене тлумачення позбавляє можливості притягнення до відповідальності особу, дії якої мали негативно вплинути не на всі процеси обробки інформації, а на деякі з них.

По-друге, на наш погляд, не слід зазначати, що наслідком втручання в роботу комп’ютерних систем є обов’язкове спотворення процесу обробки даних, що руйнує саму інформацію або її носії. Настання таких наслідків законодавцем визначено як обов'язкову ознаку об'єктивної сторони композиції, а не будь-яке втручання в роботу комп'ютерних систем тягне за собою їх виникнення. Освічений програміст може виконувати такі дії, не завдаючи шкоди роботі комп’ютера, наприклад, проникати через нього через комп’ютерну мережу, видаляти або копіювати необхідну інформацію, виходити, і комп’ютерна система не змінюватиметься, оскільки при копіюванні комп’ютерної інформації або її носій інформації не зазнає жодних змін, а у разі видалення інформації про комп’ютер, яка не входить до

складу програмного забезпечення, програмне забезпечення безпосередньо не змінюється.

Д. С. Азаров визначає «втручання в роботу комп'ютерної системи - як будь-який вплив на обробку інформації, що здійснюється за допомогою програмного та (або) апаратного забезпечення під час безпосередньої роботи з цими системами за допомогою автоматизованих робочих станцій» [2].

З цього визначення випливає, що лише особа, яка впливає на конкретні комп’ютерні системи лише під час роботи з ними, може нести кримінальну відповідальність за негативний вплив на процес обробки інформації. Це твердження є неточним, враховуючи сучасні реалії комп’ютерних злочинів загалом та злочину, який розслідується, зокрема, оскільки основна частина комп’ютерних злочинів вчиняється віддалено, тобто за допомогою використання засобів зв’язку, зокрема, комп’ютерних мереж. У таких випадках пошкодження віддаленої комп’ютерної системи завдається віддалено. Однак мережа, яка виступає як засіб чи інструмент (залежно від виду діяння) вчинення злочину, не може бути визначена як комп’ютерна система, на яку спрямований злочин. Тому ми вважаємо, що нелогічно стверджувати, що перешкоди в роботі комп’ютерних систем повинні виникати під час безпосередньої роботи з цими системами.

РОЗДІЛ 3
СУБ'ЄКТИВНІ ОЗНАКИ «КОМП'ЮТЕРНИХ ЗЛОЧИНІВ»

2.1. Суб'єкт «комп'ютерних злочинів»

Відповідно до ч. 1 ст. 18, ч. 1 ст. 19, ч. 1.2 ст. 22 КК України, суб'єктом злочину, передбаченого ст. 361 Кримінального кодексу України, є загальним. Тобто кримінальна відповідальність за вчинення злочину, передбаченого ст. 361 Кримінального кодексу України, підлягає осудна фізична особа, яка до моменту вчинення злочину досягла шістнадцяти років.

На думку В. А. Володимирова та Г. А. Левицького, «ознаки, що характеризують суб'єкта, нерозривно пов'язані з усіма іншими ознаками та ознаками злочину. Саме своїми соціально небезпечними діями (об'єктивна сторона) суб'єкт завдає шкоди об'єкту посягання, діючи винувато - навмисно чи необережно (суб'єктивна сторона)» [16].

Таким чином, висновок про те, що суб'єктом злочину, передбаченого ст. 361 Кримінального кодексу України, є загальним, вимагає ретельного вивчення, з метою визначення обумовленості його визначення як такого.

Суб'єктом злочину, передбаченого ст. 361 Кримінального кодексу України, є особа, яка має достатні навички вчинення комп'ютерних злочинів. Однак вчені не пропонують визнавати цю людину особливим предметом, тобто наділеним такими властивостями, які відрізняють її від кола загальних предметів.

Так, одна група експертів прямо вказує, що суб'єктом злочину, передбаченого ст. 361 Кримінального кодексу України, є загальним, інша група звертає увагу на наявність у суб'єкта злочину певних додаткових ознак, не ідентифікуючи його як особливий.

П. П. Андрушко, вважаючи, що «предметом ст. 361 Кримінального кодексу України злочином є особа, яка досягла шістнадцяти років, вказує, що це можуть бути особи з персоналу "АЕОМ, їх систем та комп'ютерних

мереж", а також "суб'єкти злочину у формі комп'ютерний вірус за допомогою програмного забезпечення та технічних засобів, призначених для незаконного проникнення в АЕОМ, їх системи та комп'ютерні мережі та здатних спричинити спотворення або знищення комп'ютерної інформації або її носіїв, можуть бути розробниками таких програм та технічних засобів, зокрема їх виробниками, виробники (розробники) програм з комп'ютерними вірусами, так звані «техно-щури», «хакери» та інші»» [3].

Відповідно до ч. 2 ст. 18 Кримінального кодексу України особливим суб'єктом злочину є фізична осудна особа, яка вчинила злочин у віці кримінальної відповідальності, суб'єктом якого може бути лише певна особа. Тобто спеціальний суб'єкт - це особа, яка, крім розсудливості та досягнення віку кримінальної відповідальності, має ще й певні особливі ознаки, які зазначені у нормі права (особливі ознаки).

У ст. 361 Кримінального кодексу України відсутні інструкції щодо особливих ознак предмета комп'ютерних злочинів. Таким чином, із змісту статті очевидно, що кіберзлочинець наділений такими ознаками:

- має доступ до комп'ютерної системи, до якої або з якої можна зробити несанкціонований доступ або навмисно поширювати шкідливі комп'ютерні програми;

- має певні знання та навички, що дозволяють йому виконувати певні операції з комп'ютерними системами (маніпулювати даними, реалізовувати шкідливі програми, підробляти паролі та коди тощо) [32].

Якщо підхід до визначення комп'ютерного злочинця як особливого міг мати місце ще десять років тому, то сьогодні, враховуючи особливості сучасного інформаційного суспільства, ми вважаємо, що визначення суб'єкта злочину за ч. 1 ст. 361 Кримінального кодексу України, як спеціальний, не є доцільним, оскільки знання та навички роботи з комп'ютерними системами, зокрема, як користувач, сьогодні, по суті, не можуть вважатися особливими. Вміння працювати за комп'ютером є обов'язковою умовою розвитку

сучасної людини, забезпечення її віртуального спілкування, збору інформації, навіть знайомств.

«Це пов’язано насамперед із факторами розвитку суспільства та переходом його до інформаційної фази розвитку, в якій процеси інформатизації активніше проникають у всі сфери людської діяльності, стають ефективним елементом економіки» [23].

Подібну думку висловлює Ю. М. Батурин, який зазначає: «велика кількість злочинів, пов’язаних із використанням комп’ютерів, вчиняються простими людьми, робота чи інтереси яких пов’язані з комп’ютерними технологіями» [10].

Таким чином, особи, які вчинили комп’ютерні злочини, не мають конкретних характеристик, які б відрізняли їх від загальних суб’єктів злочинів, тому, на наш погляд, їх не можна віднести до спеціальних суб’єктів. Визначаючи предмет злочину, передбаченого ст. 361 Кримінального кодексу України, як особливий суб’єкт на практиці призведе до неможливості притягнення до відповідальності винних у несанкціонованому доступі до комп’ютерної інформації та розповсюдженні шкідливих комп’ютерних програм.

Слушним є визначення суб’єкту злочину, передбаченого ст. 361 Кримінального кодексу України, як загальний, але за умови обов’язкової перевірки спеціальних навичок особи та реальної можливості вчинити злочин цієї категорії. Таким чином, суб’єктом злочину, передбаченого ст. 361 Кримінального кодексу України, слід визнати спільного суб'єкта: особу, яка осудна і досягла шістнадцяти років до злочину.

Це пов’язано в першу чергу з тим, що сьогодні використання комп’ютерів та комп’ютерних мереж є побутовим явищем. Завдяки Інтернету існує як ділова, так і приватна кореспонденція, аудіо- та відеозв’язок, пошук інформації тощо. Завдяки великій кількості комп’ютерних та Інтернет-клубів кожен, хто потребує роботи за комп’ютером чи комп’ютерною мережею, може задовольнити цю потребу. Доступ до комп’ютерів у таких клубах не

обмежений, а час користування платним. Тому кожен, навіть не маючи власного комп'ютера, може скористатися послугами клубу та перебувати в Інтернеті необхідну кількість часу. До речі, навчитися працювати на комп'ютері на рівні користувача теж не проблема.

Таким чином, при розслідуванні справ про вчинення злочину, передбаченого ст. 361 Кримінального кодексу України, необхідно встановити фактичну здатність підозрюваних (обвинувачених, підсудних) виконувати певні операції з комп'ютерними системами, оскільки відсутність навичок роботи з комп'ютером буде свідчити про те, що особа не могла вчинити певні злочинні дії [32].

Необхідно також встановити, чи має особа доступ до комп'ютерної мережі з персонального комп'ютера, та (або) наявність електронного комп'ютера (терміналу), з якого були скоєні злочинні дії, включаючи розробку, копіювання на шкідливих носіях інформації. комп'ютерні програми [15].

2.2. Суб'єктивна сторона «комп'ютерних злочинів»

Другим суб'єктивним елементом злочину є суб'єктивна сторона злочину. Суб'єктивна сторона злочину виявляє внутрішнє психічне ставлення суб'єкта до вчиненого ним суспільно небезпечного діяння та його шкідливі наслідки. Як зазначив В.Я. Тацій зазначає, «такий, що соціально небезпечний вчинок, вчинений людиною, отримує адекватне відображення в її психіці. Таке внутрішнє, психічне ставлення людини до суспільно небезпечного діяння чи бездіяльності, вчиненого нею, а також його наслідки називається в кримінальному праві суб'єктивною стороною злочину» [49].

Встановлення ознак суб'єктивної сторони визначається не тільки необхідністю дотримання презумпції невинуватості. Риси суб'єктивної сторони злочину характеризуються та взаємодоповнюються об'єктивними ознаками складу, їх суть розкривається через об'єктивні ознаки.

Суб'єктивна сторона злочину, крім вини в тій чи іншій формі, включає необов'язкові ознаки: мотив і мету злочину. Якщо останні чітко передбачені у розпорядженні, їх обов’язково встановлюють, оскільки вони визначають кваліфікацію злочину. В інших випадках вони є факультативними, тобто не впливають на кваліфікацію, але їх встановлення є необхідним, оскільки їх наявність, ознаки, інші ознаки визначають визначення інших елементів злочину.

Диспозиція ст. 361 Кримінального кодексу України, як зазначено вище, передбачено дві альтернативні активні дії, визначені нами як "Несанкціонований доступ до комп'ютерної інформації" та "Умисне розповсюдження шкідливих комп'ютерних програм". Обидва вони мають логічно незалежний склад, а також спрямовані на досягнення різних, але певних результатів [32].

Таким чином, обидва ці злочини, передбачені ст. 361 КК України як альтернативні дії, спрямовані на досягнення кінцевого результату. Це свідчить про наявність вольових та інтелектуальних моментів злочину. Тобто, обидва ці злочини є умисними.

Форму вини слід визначати на основі ретельного аналізу інтелектуально-вольових ознак психічного ставлення суб'єкта до вчиненого ним соціально небезпечного діяння.

Відповідно до ч. 2 ст. 24 Кримінального кодексу України прямий умисел полягає у тому, якщо особа усвідомлювала соціально небезпечний характер своєї дії (дії чи бездіяльності), передбачала її соціально небезпечні наслідки та бажала їх здійснення. Непрямий умисел полягає у тому, якщо особа усвідомлювала соціально небезпечний характер своєї дії (дії чи бездіяльності), передбачала її соціально небезпечні наслідки і хоча вона цього не хотіла, але свідомо припускала їх виникнення »(ч. 3 ст. 24 Кримінальної Кодекс України).

У ч. 2 ст. 25 Кримінального кодексу України зазначається: "Халатність – це кримінальна зарозумілість, якщо особа передбачала

можливість соціально небезпечних наслідків своєї дії (дії чи бездіяльності), але необдумано сподівалася їх запобігти".

Халатність – це злочинна необережність, якщо особа не передбачала можливості соціально небезпечних наслідків своєї дії (дії чи бездіяльності), хоча вона мала і могла передбачити їх »(ч. 3 ст. 25 Кримінального кодексу України).

Форми вини характеризуються вольовими та інтелектуальними особливостями психічного ставлення суб'єкта, а також відокремлюються одна від одної групуванням таких ознак [13].

Щодо характеристик форм вини злочину, передбачених ст. 361 Кримінального кодексу України, слід звернути увагу, насамперед, на об’єктивні особливості їх вчинення.

Водночас очевидно, що, вчиняючи будь-яке з цих дій, слід враховувати конкретну форму вини стосовно певних складових їх об'єктивної сторони.

Ми вважаємо за доцільне при проведенні дослідження форм вини щодо діянь, передбачених ст. 361 Кримінального кодексу України, також виділити їх як самостійний склад злочину злочинів "Несанкціонований доступ до комп'ютерної інформації" та "Умисне розповсюдження шкідливих комп'ютерних програм", які вже пропонувались раніше, і таким чином розслідувати їх окремо [32].

Отже, стосовно злочину "Несанкціонований доступ до комп'ютерної інформації", слід зазначити, що, як обговорювалося в розділі 1 цього дослідження, цей акт логічно визначається як самостійний склад, насамперед тому, що він, на відміну від навмисного розповсюдження шкідливих комп’ютерних програм ”має матеріальний склад [32].

Тобто, психічне ставлення людини до злочину «Несанкціонований доступ до комп’ютерної інформації» повинно складатися з усвідомлення особою соціальної небезпеки своїх дій та можливості кримінальних наслідків таких дій, а також бажання чи свідомого визнання їх виникнення.

"Несанкціонований доступ до комп'ютерної інформації", як уже зазначалося, може передбачати несанкціонований доступ або навмисне порушення правил доступу до комп'ютерної системи.

М.С.Вертузаєв, В.О. навмисне. Для комп'ютерних злочинів ознака інтелекту завжди присутня, але воля злочинця може бути різною, що може зробити намір прямим або опосередкованим. "ці автори зазначають, що знищення інформації здійснюється навмисними або необережними діями осіб, які мають можливість впливати на цю інформацію. Кримінальна відповідальність за несанкціонований доступ до комп'ютерної інформації, зазначається, що суб'єктивна сторона злочину характеризується виною у формі прямого умислу, а непрямий умисел та необережність вини можуть мати місце у згубних наслідках несанкціонований доступ» [15].

Ці заяви експертів свідчать про необхідність встановлення моменту волі щодо безпосередніх наслідків, тобто про те, що злочин може бути вчинений як з прямим, так і з непрямим (можливим) умислом.

Однак виникає питання, чи може діяння, спрямоване на доступ до комп'ютерної інформації, бути вчинене з непрямими намірами, коли вольовим знаком психічного ставлення людини є не пряме бажання безпосередньо виточити, спотворити чи знищити комп'ютерну інформацію, а людина лікує такі наслідки байдуже, свідомо допускає їх настання.

Таким чином, вольовий знак у вигляді прямого бажання наступити або байдуже ставлення людини до настання будь-якого з альтернативних наслідків не виключає наявності вольового моменту у будь-якій формі стосовно настання іншого наслідку . Так, людину, яка безпосередньо хоче, щоб комп'ютерна інформація просочилася, може байдуже сприймати інші наслідки: спотворення або знищення комп'ютерної інформації.

ВИСНОВКИ

Розгляд проблемних питань, які були предметами нашого дослідження, дає можливість зробити наступні висновки:

1. Глобальні вимоги до боротьби з кіберзлочинністю включають необхідність розробки в кожній країні власних правил захисту від посягань на дані, що зберігаються в автоматизованих системах. Цей інститут кримінального права в Україні ще недостатньо розвинений. Однак, поряд з розповсюдженням Інтернету та зростаючою загрозою комп'ютерних злочинів для суспільних інтересів України, законодавець повинен визначити коло комп'ютерних злочинів, чітко розробляючи правила, за якими можна буде притягнути до відповідальності відповідальних за їх комісія.

2. Ефективна протидія «комп'ютерним злочинам» у розвинутих зарубіжних країнах зумовлений не в останню чергу досконалим правовим регулюванням відповідальності за незаконні посягання на роботу комп'ютерних систем та комп'ютерної інформації.

3. Вітчизняне законодавство не відповідає міжнароднм стандартам щодо регламентації комп'ютерних злочинів взагалі та злочинів, являють собою незаконне втручання в роботу комп'ютерів, їх систем та комп'ютерних мереж зокрема.

4. Рівень обізнаності суб'єктів правовідносин у сфері користування комп'ютерною інформацією є відносно низьким, що, у свою чергу, з одного боку «полегшує роботу» злочинцям у вказаній сфері, а з іншого – призводить до латентності комп'ютерної злочинності в Україні.

5. Стаття 361 Кримінального кодексу України об'єднує різні юридичні складові злочинів, які визнані самостійними як на міжнародному рівні, так і на рівні законодавства окремих держав, а саме – «Несанкціонований доступ до комп'ютерної інформації» та «Навмисне розповсюдження шкідливих комп'ютерних програм», які визначаються як

види соціально небезпечних діянь у межах об’єктивної сторони злочину, передбаченого ст. 361 Кримінального кодексу України. У цьому випадку для одного з них передбачено обов’язкове настання соціально небезпечних наслідків, а для іншого – відсутність. Таке визначення, звичайно, створить труднощі при практичному застосуванні цього правила.

6. Ст. 361 Кримінального кодексу України є новинкою кримінального законодавства, однак є фактичною трансформацією відповідної статті, яка існувала в Кримінальному кодексі України 1960 р. В чинному КК України. Зазначене визначення містить у собі логічні неточності, що може призвести до труднощів при кваліфікації соціально небезпечних актів несанкціонованого доступу до комп'ютерної інформації та навмисного розповсюдження шкідливих комп'ютерних програм на практиці.

7. У колі соціально небезпечних дій, які український законодавець пов'язує з незаконним втручанням у роботу електронних комп'ютерів (комп'ютерів), їх систем та комп'ютерних мереж, немає таких небезпечних дій, як навмисне розповсюдження шкідливих комп'ютерних програм, які по своїй суті не є комп’ютерними вірусами, за поширення яких вітчизняним законодавцем передбачене настання кримінальної відповідальності.

8. Вітчизняним законодавцем не передбачено витоку інформації з комп’ютерних мереж та систем, тобто вчинення актів незаконного втручання в роботу комп’ютерів, систем та комп’ютерних мереж, що спричиняє «витік інформації з комп’ютерів інформації про їх користувачів. Останні криминальні правопорушення набувають усе більшої суспільної небезпечності, оскільки все більше інформації про громадян України потрапляє в суспільні мережі, усе більше сервісів «переходе» від «паперової» форми в «електронну» з відпоідним збереженням в електронному вигляді інформації про громадян, підприємства, установи та організації.

9. Вітчизняне законодавство не містить визначення комп’ютерної інформації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Title 18. Crimes and Criminal Procedure. Text contains those laws in effect on May 16, 2020 // Office of the Law Revision Counsel (OLRC). The United States Code. URL: https://uscode.house.gov/ view.xhtml?path=/prelim@title18/part1/chapter105& edition=prelim. (дата звернення: 14.06.2020).

2. Азаров Д.С. Кримінальна відповідальність за злочини у сфері комп'ютерної інформації: Автореф. канд. юрид. наук. – К., 2002. – 18 с.

3. Андрушко П.П. Законодавча техніка Кримінального кодексу України 2001 року та її вплив на тлумачення його норм // Новий Кримінальний кодекс України: Питання застосування і вивчення: Матер. міжнар. наук. конф. [Харків] 25-26 жовт. 2001 р. /Редкол.: Сташис В.В. (голов. ред.) та ін. - К.-Х.: "Юрінком Інтер", 2002. - С. 24-30.

4. Антонов С. Компьютерные преступления в банковской сфере //Юридическая практика. – 1997. – № 8. – С. 7 – 9.

5. Архів Дарницького районного суду м. Києва: Кримінальна справа № 1-503, вирок від 16.01.2001 р.

6. Ахтирська Н. Про удосконалення кримінального законодавства України в сфері боротьби з кіберзлочинністю //htth://www.crime-research.org

7. Баранов О. Кримінологічні проблеми комп'ютерної злочинності //Інформаційні технології та захист інформації: Зб. наук. праць. – Запоріжжя: Юридичний інститут МВС України, 1998. – Вип. 2. – С.64 – 69.

8. Баранов О. Уголовная ответственность за компьютерные преступления //Безопасность информации. – 1996. – № 2. – С.4 – 9.

9. Баранов О. Цифрове законодавство //Дзеркало тижня. – 2002. – № 20. – 7 черв.

10. Батурин Ю.М. Проблемы компьютерного права. – М.: Юрид. лит., 1991. – 271 с.

11. Бачило И.Л., Семилетов С.И. Основные направления организационно-правового регулирования использования глобальных сетей, включая Интернет /Информационное право: информационная культура и информационная безопасность. Материалы Всероссийской научно-практической конференции Санкт-Петербургского гуманитарного университета профсоюзов, 17 – 19 октября 2002 г. – С.90 – 100.

12. Беляков К.И. Управление и право в период информатизации: Монографія. – Киев: КВЩ, 2001. – 308 с.

13. Біленчук П.Д., Зубань М.А. Комп'ютерні злочини: соціально-правові та кримінолого-криміналістичні аспекти: Навч. посіб. – К.: Українська академія внутрішніх справ, 1994. – 72 с.

14. Бурчак Ф.Г. Квалификация преступлений. Изд. 2-е, доп. – Киев.: Изд-во полит. лит-ры Украины, 1985. – 119 с.

15. Вертузаєв М., Попов А. Запобігання комп'ютерним злочинам та їх розслідування // Право України . – 1998. - № 1. – С. 101 – 103.

16. Владимиров В.А., Левицкий Г.А. Субъект преступления. - М.: Высшая школа МООП РСФСР, Научно-исследовательский и редакционно-издательский отдел, 1964. - 57 с.

17. Гавловський В.Д., Романюк В.С. Проблеми організації боротьби з правопорушеннями, що вчиняються з використанням сучасних інформаційних технологій //Публікації Центру

дослідження проблем комп'ютерної злочинності. – www/crime-recearch.org/library/Gav-Rom-Cim.htm

18. Гавловський В.Д., Цимбалюк В.С. Кіберзлочинність як чинник державної інформаційної політики України //Боротьба з організованою злочинністю і корупцією (теорія і практика). Координаційний комітет по боротьбі з корупцією і організованою злочинністю при Президентові України. Міжвід. наук.-дослід. центр. – 2002. – № 5. – С. 106 – 116.

19. Глушков В.О., Бєляков К.І., Орлов С.О. Інформаційні відносини: кримінально-правовий аспект. Про Проект Концепції стратегії реалізації державної політики щодо боротьби з кіберзлочинністю в Україні. /http://mndc. naiau. kiev. ua /KONC/ ceber. httm.

20. Голубєв В. Кібертероризм – загроза національній безпеці та інтересам України //Юридичний журнал. – 2004. – № 1 (19). – С. 132 – 134.

21. Голубєв В. Комп'ютерна злочинність //Юридичний вісник України. – 2002. – № 6 (9). – С. 1 – 4.

22. Гуцалюк М. Координація боротьби з комп'ютерною злочинністю //Право України. – 2002. – № 5. – С. 121 – 126.

23. Гуцалюк М. Протидія комп'ютерній злочинності //Право України. – 2003. – № 6. – С.114 – 117.

24. Гуцалюк М. Протидія міжнародній комп'ютерній злочинності //Вісник прокуратури. – 2003. – № 9 (27). – С.60 – 64.

25. Гуцалюк М. Хроніка вірусної атаки на Укртелеком //htth://www.ukrtel.net

26. Духов В.Е. Экономическая разведка и безопасность бизнеса. – Киев: ИМСО МО Украины, НВФ “Студцентр” , 1997.

27. Жарова А.К. Правовые проблемы обращения информации в Интернете. Опыт Республики Узбекистан: Автореф. дисс. канд. юрид. наук. – М., 2002. – С. 23.

28. Калюжный Р.А. Теоретические и практические проблемы использования вычислительной техники в системе органов внутренних дел (организационно-правовой аспект): Автореф. дисс. д-ра юрид. наук, – Институт государства и права им. В.М.Корецкого. – Киев, 1992. – 23 с.

29. Карпов Н., Вертузаев М. К вопросу о борьбе с компьютерными преступлениями в Украине //Международный научно-практический правовой журнал “Закон и жизнь”. – 2004. – № 7 (152). – С.29 – 32.

30. Колесник В.А. Розслідування комп’ютерних злочинів. Наук.-метод. посіб. – К.: Вид-во НА СБУ, 2003. – 124 с.

31.Конституція України : офіц. текст. Київ : КМ, 2013. 96 с.

32. Кримінальний кодекс України. *Відомості Верховної Ради України (ВВР)*, 2001, № 25-26, ст.131. URL: https://zakon.rada.gov.ua/laws/show/2341-14/conv#n2491 (дата звернення: 1.12.2020 р.).

33. Кудрявцев В.Н. Общая теория квалификации преступлений. – 2-е изд., перераб. и дополн. – М.: Юристъ, 2001. – 304 с.

34. Курс уголовного права. Общая часть. Т. 1: Учение о преступлении: Учеб. для вузов / Под ред. Н.Ф.Кузнецовой, И.М.Тяжковой. – М.: Зерцало, 1999. – 592 с.

35. Левиашвили М.Ш. Объект уголовно-правовой охраны и его значение для классификации преступлений //Уголовно-правовые

исследования: Сб., посвящ. 80-летию со дня рожд. Т.В.Церетели. – Тбилиси: Мецниереба, 1987. – С.94 – 103.

36. Мінченко А.В. Правова інформатика. Інформатика в історичному аспекті: Навч. посіб. – К.: Арістей, 2003. – 296 с.

37. Мотлях О.І. Захист інформації у комп'ютерних системах: актуальність та новизна підходів //Вісник Академії праці і соціальних відносин Федерації профспілок України. – 2001. – № 1(10). – С. 57 – 62.

38. Мотлях О.І. Інформаційна безпека: пріоритетні напрями, шляхи розвитку та вдосконалення //Вісник Академії праці і соціальних відносин Федерації профспілок України. – 2000. – № 1 (5). – С. 40 – 45.

39. Науково-практичний коментар Кримінального кодексу України від 5 квітня 2001р. / За ред. М.І.Мельника, М.І.Хавронюка. – К., 2001. – 1104 с.

40. Овчинский В.С. Интерпол в вопросах и ответах. – М.: ИНФРА – М., 2001. – С. 135 – 136.

41. Полевой Н.С., Крылов В.В. Компьютерные технологии в юридической деятельности. – М.: Изд-во «БЭК», 1994. – 304 с.

42. Про авторське право і суміжні права : Закон України від 23.12.1993 р. *Відомості Верховної Ради України (ВВР)*. 1994. № 13. Ст.64.

43. Про інформацію : Закон україни від 2.10.1992 р. *Відомості Верховної Ради України (ВВР)*. 1992. № 48. ст.650.

44. Проект Концепції стратегії реалізації державної політики щодо боротьби з кіберзлочинністю в Україні / http:// mndc. naian. kiev. ua

45. Розенфельд Н.А. Кримінально-правова характеристика незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж. Дисс. канд. юрид. наук. – К., 2003. – 200 с.

46. Руководство для следователей / Под общ. ред. В.В.Мозякова. – М.: Изд-во «Экзамен», 2005. – 912 с.

47. Советский энциклопедический словарь. – М.: Советская энциклопедия, 1982. – 1600 с.

48. Старченко Ю.О. Окремі аспекти протидії "хакерській" діяльності в Україні //Інформаційний бюлетень. – 2000. – № 2. – С. 40 – 41.

49. Таций В.Я. Объект и предмет преступления в советском уголовном праве. – Харьков: Вища школа, 1998. – 196 с.

50. Тищенко Є.Ф., Селюк А.В. Розслідування комп'ютерних злочинів. Наук.-метод. посіб. – К.: Вид-во НА СБУ, 2003. – 124 с.

51. Уголовное право. Общая часть /Отв. ред. И.Я.Козаченко, З.А.Незнамова. – М.: Издательская группа ИНФРА-НОРМА, 1997. – 516 с.

52. Янішевський Д.О. Встановлення відповідальності за "комп'ютерні злочини" //Боротьба з організованою злочинністю і корупцією (теорія і практика). Координаційний комітет по боротьбі з корупцією і організованою злочинністю при Президентові України. Міжвідомчий науково-дослідний центр. – 2002. – № 5. – С.117 – 123.