Міністерство внутрішніх справ України
ДНІПРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ

ЗАПОБІГАННЯ КІБЕРЗЛОЧИННОСТІ

Навчальний посібник

Колектив авторів

Дніпро
2026

УДК 343.85:343:53
З-33

Рекомендовано до друку
Вченою радою Дніпровського
державного університету внутрішніх справ
(протокол № 13 від 28 травня 2026 р.)

РЕЦЕНЗЕНТИ:

доктор юридичних наук, професор **Олена БАБІКОВА** – директор Науково-дослідного інституту проблем досудового розслідування;

доктор юридичних наук, доцент **Вікторія РУФАНОВА** – старший слідчий в особливо важливих справах відділу розслідування злочинів, скоєних проти життя та здоров'я особи, слідчого управління Головного управління Національної поліції в Дніпропетровській області;

кандидат технічних наук, доцент **Віктор ОБОДЯК** – доцент кафедри кібербезпеки факультету електроніки та інформаційних технологій Сумського державного університету.

З-33 **Запобігання кіберзлочинності:** навч. посіб. / кол. авт.: О. А. Моргунов, І. В. Магдаліна, О. С. Юнін та ін. Дніпро : Дніпров. держ. ун-т внутр. справ, 2026. 180 с.

ISBN 978-617-560-134-1

Видання містить аналіз поняття та ознак кіберзлочинності, її окремих кількісних та якісних показників, кримінологічну характеристику особи кіберзлочинця. Надана розгорнуту характеристику кримінально-правових заходів запобігання кіберзлочинності, зокрема, визначений стан імплементації норм міжнародного права із запобігання кіберзлочинності у кримінальному законодавстві України, проведено юридичний аналіз кримінально-правових норм, що передбачають відповідальність за кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (ст.ст. 361-363-1 КК України) та інші кіберзлочини (ст.ст. 163, 176, ч. 4 ст. 190, ч. 2 ст. 301, ст. ст. 301-1, 301-2 КК України). Розглянуті спеціально-кримінологічні та індивідуальні заходи запобігання кіберзлочинності.

Навчальний посібник розрахований на студентів (курсантів) закладів вищої освіти, у яких готують правників, працівників правоохоронних органів та суду, а також на усіх, хто цікавиться питаннями запобігання кіберзлочинності.

ISBN 978-617-560-134-1

ЗМІСТ

АВТОРСЬКИЙ КОЛЕКТИВ:

Олександр МОРГУНОВ – начальник Головного управління Національної поліції в Луганській області, доктор юридичних наук, професор;

Ігор МАГДАЛІНА –т.в.о. ректора Дніпровського державного університету внутрішніх справ, кандидат технічних наук, доцент;

Олександр ЮНІН – проректор Дніпровського державного університету внутрішніх справ, доктор юридичних наук, професор, заслужений діяч науки і техніки України;

Василь БЕРЕЗНЯК – завідувач кафедри кримінального права та кримінології факультету підготовки фахівців для органів досудового розслідування Національної поліції України Дніпровського державного університету внутрішніх справ, доктор юридичних наук, старший науковий співробітник;

Володимир ШАБЛИСТИЙ – директор Навчально-наукового інституту права та інноваційної освіти Дніпровського державного університету внутрішніх справ, доктор юридичних наук, професор;

Михайло ДУМЧИКОВ – доцент кафедри кримінально-правових дисциплін та судочинства Навчально-наукового інституту права Сумського державного університету, доктор юридичних наук, доцент;

Сергій БАБАНІН – доцент кафедри кримінального права та кримінології факультету підготовки фахівців для органів досудового розслідування Національної поліції України Дніпровського державного університету внутрішніх справ, кандидат юридичних наук, доцент;

Валентин ЛЮДВІК – доцент кафедри кримінального права та кримінології факультету підготовки фахівців для органів досудового розслідування Національної поліції України Дніпровського державного університету внутрішніх справ, кандидат юридичних наук, доцент;

Антон МАРІЄНКО – доцент кафедри кримінального права та кримінології факультету підготовки фахівців для органів досудового розслідування Національної поліції України Дніпровського державного університету внутрішніх справ, кандидат юридичних наук;

Вадим ХАШЕВ – доцент кафедри кримінального права та кримінології факультету підготовки фахівців для органів досудового

розслідування Національної поліції України Дніпровського державного університету внутрішніх справ, кандидат юридичних наук, доцент;

Юлія ХРИСТОВА – доцент кафедри кримінального права та кримінології факультету підготовки фахівців для органів досудового розслідування Національної поліції України Дніпровського державного університету внутрішніх справ, кандидат юридичних наук, доцент;

Світлана КОРОГОД – доцент кафедри кримінального права та кримінології факультету підготовки фахівців для органів досудового розслідування Національної поліції України Дніпровського державного університету внутрішніх справ, доктор філософії в галузі права, доцент;

Діана РУКІНА – фахівець відділу забезпечення якості освіти Дніпровського державного університету внутрішніх справ.

ПЕРЕДМОВА

Забезпечення інформаційної безпеки України, разом із захистом її суверенітету і територіальної цілісності, економічної безпеки, згідно ст. 17 Конституції України, є найважливішими функціями держави[1].

Кібербезпека є однією зі складових інформаційної безпеки. Стратегія кібербезпеки України, затверджена Указом Президента України від 26 серпня 2021 р. № 447/2021, визначає, що забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки України. До загроз кібербезпеці зазначена Стратегія відносить: гібридну агресію російської федерації проти України у кіберпросторі; кіберзлочинність, що завдає шкоди інформаційним ресурсам, суспільним процесам, особисто громадянам, знижує довіру суспільства до інформаційних технологій та призводить до значних матеріальних втрат; організовані та спонсоровані урядами інших держав кібератаки, що пов'язані з викраденням у політичних, економічних або військових цілях чутливої інформації (кібершпигунство) та здійсненням розвідувально-підривної діяльності; використання терористичними організаціями кіберпростору для вчинення актів кібертероризму, фінансової та іншої підтримки терористичної діяльності[2].

Інтенсивний розвиток та широке використання інформаційно-комунікаційних технологій у всіх сферах суспільного життя обумовлюють необхідність належного забезпечення безпеки функціонування кіберпростору. У цьому контексті важливу роль відіграють кримінально-правові засоби захисту відповідних суспільних відносин. У науковій та правозастосовній практиці посягання на такі суспільні відносини отримали узагальнену назву «комп'ютерні кримінальні правопорушення» або «кіберзлочини», до яких належать суспільно небезпечні винні діяння у кіберпросторі та/або з його використанням, відповідальність за які передбачена законом України про кримінальну відповідальність та/або які визнані злочинами

[1] Конституція України. URL : https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text.

[2] Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України від 26 серпня 2021 р. № 447/2021. URL : https://zakon.rada.gov.ua/laws/show/447/2021#n12.

міжнародними договорами України[3].

У кримінальному законодавстві України відповідальність за кіберзлочини передбачена у кількох розділах Особливої частини КК України: розділ XVI «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» (ст.ст. 361-363-1), розділ V «Кримінальні правопорушення проти виборчих, трудових та інших особистих прав і свобод людини і громадянина» (ст.ст. 163, 176), розділ VI «Кримінальні правопорушення проти власності» (ч. 4 ст. 190), розділ XII «Кримінальні правопорушення проти громадського порядку та моральності» (ч. 2 ст. 301, ст.ст. 301-1-301-2).

Сучасні тенденції розвитку кіберзлочинності свідчать про суттєве зростання її суспільної небезпечності. За оцінками зарубіжних дослідників, економічні збитки від одного кіберзлочину можуть становити від сотень тисяч до мільярдів доларів США, що значно перевищує втрати від традиційних форм злочинності. Загальний обсяг збитків від кіберзлочинності у світі вже перевищує прибутки від незаконного обігу наркотичних засобів. За міжнародними оцінками кіберзлочини вчиняються фактично кожні кілька секунд.

Характерною особливістю кіберзлочинності є високий рівень їх латентності. За різними даними частка невиявлених комп'ютерних кримінальних правопорушень становить від понад 80 %. Навіть у державах із розвиненими системами обліку та протидії кіберзлочинності до судового розгляду доходить незначна частина таких справ.

Рівень розвитку інформаційно-комунікаційних технологій у державі безпосередньо впливає як на поширення кіберзлочинності, так і на ефективність протидії їй. Наразі важливим є подальше вдосконалення національної системи кібербезпеки, зокрема шляхом підвищення рівня цифрової грамотності населення, розвитку спеціалізованих правоохоронних органів та імплементації міжнародних стандартів.

Запобігання кіберзлочинності передбачає застосування комплексного підходу, що включає кримінально-правові, організаційні та технічні заходи, спрямовані на своєчасне виявлення, фіксацію та розслідування відповідних правопорушень.

[3] Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 р. URL : https://zakon.rada.gov.ua/laws/show/2163-19#Text.

Розділ 1
КРИМІНОЛОГІЧНА ХАРАКТЕРИСТИКА КІБЕРЗЛОЧИННОСТІ

1.1. Поняття та ознаки кіберзлочинності

У навчальній та науковій літературі зустрічаються різні підходи до визначення поняття кіберзлочинності.

До поширених визначень слід віднести наступні.

Кіберзлочинність – це сукупність злочинів, що вчиняються у віртуальному просторі за допомогою комп'ютерних систем або шляхом використання комп'ютерних мереж та інших засобів доступу до віртуального простору в межах комп'ютерних мереж, а також проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних[4].

Кіберзлочинність – соціально-правовий феномен, що проявляється у стійких кримінальних практиках правопорушення з використанням електронно-обчислювальних машин (комп'ютерів), телекомунікаційних систем, комп'ютерних мереж і мереж електрозв'язку, форми прояву яких передбачені законом про кримінальну відповідальність[5].

Кіберзлочинність – різні види злочинів, скоєних за допомогою комп'ютерів та інтернету[6].

Поняття кіберзлочинності закріплене в Україні на законодавчому рівні у п. 9 ч. 1 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 р., згідно якого кіберзлочинність – це сукупність кіберзлочинів[7].

Для практичної діяльності правоохоронних органів, оцінки ефективності запобігання кіберзлочинності, зокрема, в частині організації ведення статистичної звітності у цій сфері основою є саме

[4] Русецький А. А., Куцолабський Д. А. Теоретико-правовий аналіз понять «кіберзлочин» і «кіберзлочинність». *Право і безпека*. 2017. № 1 (64). С. 74-78. с. 75.

[5] Галушко П. П. Кіберзлочинність: поняття та соціально-правова природа. *Вісник кримінологічної асоціації України*. 2025. № 1 (34). С. 808-815. с. 815.

[6] Лугіна Н. А., Лучук А. М. Порівняльний аналіз вітчизняного та європейського законодавства з питань запобігання кіберзлочинності. *Ірпінський юридичний часопис: науковий журнал.* 2023. Вип. 1 (10). С. 180-187. с. 183.

[7] Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 р. URL : https://zakon.rada.gov.ua/laws/show/2163-19#Text.

законодавче визначення вищевказаного поняття.

Виходячи з цього визначення обов'язковою ознакою кіберзлочинності є кіберзлочин. Пункт 8 ч. 1 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 р. дає таке його визначення: кіберзлочин (комп'ютерний злочин) – суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або що визнано злочином міжнародними договорами України[8].

Наведені визначення дозволяють виділити нормативно закріплені ознаки кіберзлочинності:

1) сукупність суспільно небезпечних діянь;
2) передбачення цих діянь законом України про кримінальну відповідальність та/або визнання їх злочинами міжнародними договорами України;
3) вчинення їх у кіберпросторі та/або з його використанням;
4) винність.

Сукупність суспільно небезпечних діянь. Під сукупністю слід розуміти вчинення двох або більше суспільно небезпечних діянь. До того ж, не має значення чи виявлені та обліковані ці діяння. Оскільки кіберзлочинність є за своїм змістом кримінологічним поняттям, то на нього поширюються всі ознаки, притаманні будь-якому виду злочинності. Зокрема, певну частину кіберзлочинності складають латентні комп'ютерні кримінальні правопорушення, які за тих чи інших обставин не потрапили до офіційної статистичної звітності.

Передбачення цих діянь законом України про кримінальну відповідальність та/або визнання їх злочинами міжнародними договорами України. Передбачення кіберзлочинів законом України про кримінальну відповідальність означає наявність відповідних складів кримінальних правопорушень у КК України.

Особлива частина чинного КК України не містить окремого розділу, який би містив склади всіх комп'ютерних злочинів та кримінальних проступків. Вони розміщені у різних розділах Особливої частини КК України.

До кіберзлочинів (комп'ютерних злочинів), зокрема, належать:

1) кримінальні правопорушення, передбачені розділом XVI Особливої частини «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та

[8] Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 р. URL : https://zakon.rada.gov.ua/laws/show/2163-19#Text.

комп'ютерних мереж і мереж електрозв'язку» КК України (ст. 361 «Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж», ст. 361[1] «Створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут», ст. 361-2 «Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації», ст. 362 «Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї», ст. 363 «Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється», ст. 363-1 «Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку»).

2) стаття 163 «Порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер».

3) стаття 176 «Порушення авторського права та суміжних прав».

4) частина 4 ст. 190 (шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки).

5) стаття 200 «Незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, обладнанням для їх виготовлення».

6) частина 2 ст. 301 (збут неповнолітнім чи розповсюдження серед них творів, зображень або інших предметів порнографічного характеру).

7) стаття 301-1 «Одержання доступу до дитячої порнографії, її придбання, зберігання, ввезення, перевезення чи інше переміщення, виготовлення, збут і розповсюдження».

8) стаття 301-2 «Проведення видовищного заходу сексуального характеру за участю неповнолітньої особи».

Щодо визнання суспільно небезпечних діянь кіберзлочинами міжнародними договорами України, то це положення Закону України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня

2017 р. не повністю узгоджується з ч. 3 ст. 3 КК України, згідно якої кримінальна протиправність діяння, а також його караність та інші кримінально-правові наслідки визначаються тільки цим Кодексом. До того ж, Закони України про кримінальну відповідальність мають відповідати положенням, що містяться в чинних міжнародних договорах, згоду на обов'язковість яких надано Верховною Радою України[9].

Таким чином, у разі визнання суспільно небезпечних діянь кіберзлочинами міжнародними договорами України, такі діяння повинні бути криміналізовані шляхом внесення змін до законодавства України про кримінальну відповідальність, тобто до КК України.

Вчинення їх у кіберпросторі та/або з його використанням. Поняття кіберпростору надається у п. 8 ч. 1 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 р.: кіберпростір – це середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних[10].

З наведеного визначення випливає, що ключовою ознакою кіберпростору є використання глобальних мереж передачі даних, найпоширенішою з яких на сьогоднішній день є Інтернет.

Ця ознака дозволяє стверджувати, що поняттям кіберзлочинності охоплюються не лише вищенаведені кримінальні правопорушення, а й будь-які інші, які вчиняються з використанням глобальних мереж передачі даних. Це можуть бути, наприклад, несанкціоноване поширення інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань, вчинене в умовах воєнного або надзвичайного стану (ст. 114-2 КК України), надання неправдивих відомостей до органу ведення Державного реєстру виборців або інше несанкціоноване втручання в роботу Державного реєстру виборців (ст. 158 КК України), незаконне втручання в роботу автоматизованих систем в органах та

[9] Кримінальний кодекс України: Закон України від 05 квітня 2001 р. Верховна Рада України. URL : https://zakon.rada.gov.ua/laws/show/2341-14#Text.

[10] Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 р. URL : https://zakon.rada.gov.ua/laws/show/2163-19#Text.

установах системи правосуддя (ст. 376-1 КК України), виправдовування, визнання правомірною, заперечення збройної агресії російської федерації проти України, глорифікація її учасників (ст. 436-2 КК України) тощо.

Винність. Ознака винності полягає у тому, що особа вчиняє діяння умисно або з необережності. Аналіз зазначених у цьому підрозділі складів комп'ютерних кримінальних правопорушень дозволяє стверджувати, що суб'єктивне ставлення до діяння (дії або бездіяльності) у них характеризується виною у виді прямого умислу, тобто особа усвідомлює його суспільно небезпечний характер і вчинення у кіберпросторі та/або з його використанням і бажає вчинити це діяння.

Вина у формі необережності (кримінальної протиправної самовпевненості або кримінальної протиправної недбалості) може мати місце лише у матеріальних складах комп'ютерних кримінальних правопорушень і характеризувати суб'єктивне ставлення особи до суспільно небезпечних наслідків відповідного діяння. Наприклад, необережність є однією з форм вини, яка характеризує суб'єктивне ставлення особи до заподіяння значної шкоди чи створення небезпеки тяжких технологічних аварій або екологічних катастроф, загибелі або масового захворювання населення чи інших тяжких наслідків несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (ч. 4 ст. 361 КК України).

Таким чином можна сформулювати таке визначення кіберзлочинності у широкому розумінні, яке базується на формально визначених Законом України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 р. ознаках: кіберзлочинність – це сукупність кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (ст.ст. 361-363-1 КК України) та кримінальних правопорушень, що вчиняються з використанням кіберпростору (ст. ст. 161, 176, ч. 4 ст. 190, ч. 2 ст. 301, ст.ст. 301-1, 301-2 КК України та ін.), вчинених на певній території за певний проміжок часу.

1.2. Рівень, структура та динаміка кіберзлочинності

Кіберзлочинність, як і будь-який інший вид злочинності, можна дослідити за допомогою різних кримінологічних показників. Під останніми слід розуміти сукупність основних статистичних характеристик злочинності, що дають можливість здійснити кількісно-якісне вимірювання даного явища, а саме: створити уявлення про її розміри, міру змінюваності, ймовірність та величину майбутнього прояву, а також для розроблення відповідно до цього предметних заходів щодо запобігання та протидії злочинним проявам[11]. До основних показників злочинності, що піддаються статистичному вимірюванню у першу чергу відносяться рівень, інтенсивність, динаміка, структура та географія[12].

Рівень злочинності – показник який визначає загальне число обчислених та реально здійснених кримінальних правопорушень у абсолютних величинах. У даному показнику разом із зареєстрованою злочинністю, рівнем обчисленої злочинності, включається і наявність латентних кримінальних правопорушень[13].

До рівня злочинності належать показники, що характеризують абсолютну кількість зареєстрованих кримінальних правопорушень та осіб, що їх вчинили, на певній території за конкретний проміжок часу (місяць, квартал або рік). Основними показниками, що характеризують рівень злочинності, є кількість зареєстрованих кримінальних правопорушень та кількість виявлених осіб, що вчинили кримінальні правопорушення[14].

Відзначимо, що у своєму дослідженні ми будемо відображати показники тих кіберзлочинів, відповідальність за які передбачено Розділом XVI Особливої частини КК України, оскільки ті кількісні та якісні параметри, що будуть згруповані та відображені, можливо отримати за допомогою аналізу статистичних звітів «Про зареєстровані

---

[11] Фіалка М. І. Показники злочинності. *Вісник Асоціації кримінального права України*, 2016, № 2(7). С. 361.

[12] Закалюк А. П. Курс сучасної української кримінології: теорія і практика: У 3 кн. Київ: Видавничий Дім «ІнЮре», 2007. Кн. 1: Теоретичні засади та історія української кримінологічної науки. С. 156.

[13] Кримінологія : підручник / А. М. Бабенко, О. Ю. Бусол, О. М. Костенко та ін. ; за заг. ред. Ю. В. Нікітіна, С. Ф. Денисова, Є. Л. Стрельцова. – 2-ге вид., перероб. та допов. Харків : Право, 2018. С. 83.

[14] Фіалка М. І. Там само.

кримінальні правопорушення та результати їх досудового розслідування», котрі оприлюднюються Офісом Генерального прокурора України. Характеристика інших кіберзлочинів потребує окремого, більш ґрунтовного дослідження не лише зазначених статистичних звітів, але й вибіркового аналізу кримінальних проваджень та судових вироків.

Зокрема, згідно з офіційними статистичними даними у 2013 р. в Україні було обліковано 595 кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп’ютерних мереж і мереж електрозв’язку, передбачених Розділом XVI Особливої частини КК України, у 2014 р. – 443, у 2015 р. – 598, у 2016 – 865, у 2017 р. – 2573, у 2018 р. – 2301, у 2019 – 2204, у 2020 р. – 2498, у 2021 р. – 3310, у 2022 р. – 3415, у 2023 р. – 3841, у 2024 р. – 4055 та у 2025 р. – 2987[15]. Сукупно за період 2013-2025 років обліковано 29685 фактів, що у середньому за рік складає 2283 кримінальних провадження.

За вказаний період скеровано до суду кримінальних проваджень з обвинувальним актом: у 2013 р. – 256, у 2014 р. – 201, у 2015 р. – 162, у 2016 р. – 405, у 2017 р. – 1015, у 2018 р. – 1330, у 2019 р. – 1259, у 2020 р. – 1484, у 2021 р. – 1947, у 2022 р. – 2435 , у 2023 р. – 2455, у 2024 р. – 2647, та у 2025 р. – 1648[16]. Сукупно за період 2013-2025 років скеровано до суду кримінальних проваджень з обвинувальним актом за 17244 фактами, що у середньому за рік складає 1326 кримінальних проваджень.

[15] Статистичні звіти «Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування» за 2013 – 2025 р.р., підготовлені Генеральною прокуратурою України. URL : https://new.gp.gov.ua/ua/posts/statistika.

[16] Там само.

Таблиця 1.1

Показники ефективності досудового розслідування кримінальних правопорушень,* у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку *за період 2013 – 2025 рр.

Рік	Обліковано фактів	Спрямовано до суду з обвинувальним актом	Частка спрямованих до суду з обвинувальним актом серед облікованих фактів	На кінець звітного періоду рішення не прийнято (про закінчення або зупинення)	Частка проваджень, по яким на кінець звітного періоду рішення не прийнято
2013	595	256	43%	331	56%
2014	443	201	45%	237	53%
2015	598	162	27%	411	69%
2016	865	405	47%	420	49%
2017	2573	1015	39%	1426	55%
2018	2301	1330	58%	771	33%
2019	2204	1259	57%	836	38%
2020	2498	1484	59%	944	38%
2021	3310	1947	59%	1291	39%
2022	3415	2435	71%	909	27%
2023	3841	2455	64%	1274	33%
2024	4055	2647	65%	1206	30%
2025	2987	1648	55%	1281	43%
Разом	**29685**	**17244**	**58%**	**11337**	**38%**

Аналіз наведених у таблиці 1.1 даних свідчить, що ефективність діяльності із кримінального провадження щодо зареєстрованих кримінальних правопорушень, у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку складає 58 %.

Для порівняння відзначимо, що серед загалом зареєстрованих за період 2013-2025 років 6326533 кримінальних проваджень до суду з обвинувальним актом скеровано 2073699 провадження, тобто 32,8 % від загальної кількості, що становить менше третини. Можна сказати, що

ефективність досудового розслідування кіберзлочинів є істотно вищою за загальні показники.

Аналіз щорічних показників свідчить, що частка кримінальних проваджень, передбачених Розділом XVI Особливої частини КК України скерованих до суду з обвинувальним актом у період 2013-2017 рр. коливалась в межах 27-45 %, однак починаючи з 2018 року істотно збільшилась до 58 % і досягла свого піку у 2022 році (71 % ефективності). Однак хоча у 2025 році ефективність дещо зменшилась до 55 %, але все одно вона істотно перевищила загальну сукупну ефективність досудових розслідувань щодо всіх зареєстрованих кримінальних правопорушень, яка склала лише 23 % (139707 з 608101).

На підвищення ефективності досудового розслідування кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку вказує і зменшення частки проваджень у яких на кінець звітних періодів рішення не було прийнято (про закінчення або зупинення). Наразі у період 2013 – 2017 рр. вона коливалась у межах 49-69 %. Тоді як у 2018 р. ця частка істотно зменшилась до 33 % і, у період 2018-2024 рр., коливалась у межах 27 – 39 % та лише у 2025 р. збільшилась до 43%. Сукупно за період 2013-2025 років частка таких проваджень становить 38%, тоді як серед всіх облікованих кримінальних правопорушень, за цей же період, вона складає 64,7 %, або 4095496 проваджень з 6326533.

Динаміка злочинності – кримінологічна категорія, що означає зміни у стані, структурі, характері, географії злочинності, які відбувалися протягом певного періоду. Основним показником динаміки є темп зростання кількості зареєстрованих кримінальних правопорушень. Він показує, скільки відсотків кількість кримінальних правопорушень чи злочинців, облікована за певний рік, складає від аналогічного показника іншого року, взятого за базу порівняння. В якості бази для порівняння може бути взятий показник першого року періоду, за який аналізується злочинність, або показник кожного попереднього року. В першому випадку темп зростання або зниження вираховується щодо постійної бази і називається базисним, а в другому – щодо змінної бази і називається ланцюговим. У практиці кримінологічного аналізу злочинності частіше використовується такий пов'язаний із попереднім показник, як темп приросту. Він показує, на скільки відсотків збільшилася або зменшилася кількість кримінальних правопорушень або злочинців, облікованих у певному році, порівняно з аналогічним

показником іншого року, взятого за базу порівняння[17].

Аналіз щорічних показників кількості зареєстрованих кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку за період 2013-2025 років за допомогою ланцюгового методу можна відобразити за допомогою табл. 1.2.

Таблиця 1.2

Динаміка зміни кількості облікованих кримінальних правопорушень,* у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку *за період 2013 – 2025 рр.

Рік	Обліковано фактів	Приріст/зменшення
2013	595	-
2014	443	-26%
2015	598	+35%
2016	865	+45%
2017	2573	+197%
2018	2301	-11%
2019	2204	-4%
2020	2498	+13%
2021	3310	+33%
2022	3415	+3%
2023	3841	+12%
2024	4055	+6%
2025	2987	-26%

Аналіз наведених статистичних даних щодо кількості облікованих кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем, комп'ютерних мереж та мереж електрозв'язку за 2013–2025 рр. дає підстави для виокремлення кількох відносно самостійних етапів розвитку криміногенної ситуації у сфері протидії кіберзлочинності:

1) перший період охоплює 2013–2016 рр. і характеризується нестабільною динамікою з поступовим переходом до зростання. Якщо у 2013 р. було обліковано 595 фактів, то у 2014 р. їх кількість зменшилася

[17] Кримінологія: підручник / О. М. Джужа, В. В. Василевич, В. В. Чернєй, С. С. Чернявський та ін. ; за заг. ред. д-ра юрид. наук, проф. В. В. Чернєя ; за наук. ред. д-ра юрид. наук, проф. О. М. Джужі. Київ : Нац. акад. внутр. справ, 2020. С. 58.

до 443 (–26 %), що може бути пов’язано із частковою окупацією території України. Водночас уже у 2015–2016 рр. спостерігається відновлення позитивної динаміки: 598 (+35 %) та 865 (+45 %) фактів відповідно. Таким чином, наприкінці цього етапу кількість правопорушень перевищила показник 2013 р. майже у півтора рази;

2) для другого періоду, що охоплює 2017–2019 рр., характерним є різке зростання у майже три рази та подальша відносна стабілізація на істотно вищому рівні. Зокрема, у 2017 р. зафіксовано збільшення кількості зареєстрованих кримінальних правопорушень на +197 %, у порівнянні з 2016 р., що можна назвати ключовим переломним моментом у всій досліджуваній динаміці. Протягом 2018–2019 рр. відбувалося незначне зниження (на 11 % та 4 % відповідно), однак показники залишалися більш ніж у два з половиною рази вищими, ніж у 2016 р. Таке зростання можна пояснити як збільшенням рівня цифровізації суспільства, так і спрямуванням більшої уваги правоохоронних органів у напрямку виявлення кіберзлочинів;

3) третій період, що охоплює 2020–2022 рр., відзначається продовженням зростання на +13 % (2498 фактів), +33 % (3310 фактів) та +3 % (3415 фактів) відповідно. Тобто навіть в умовах повномасштабної збройної агресії росії проти України тенденція щодо збільшення кількості виявлених кіберзлочинів зберіглася. Такий факт можна пояснити підвищенням ролі кіберпростору у воєнний період та активізацією загроз з боку кіберзлочинців, які діють в інтересах росії;

4) для четвертого періоду, що охоплює 2023-2025 рр., характерним є досягнення максимального рівня із подальшим різким зменшенням: у 2023 р. збільшення на +12 % (3841 факт) та у 2024 р. – на +6 % (4055 фактів), що виявилось найбільшим показником за весь аналізований період. Проте у 2025 р. відбулося суттєве зменшення на –26 % (2987 фактів). Така ситуація може вказувати як на часткову стабілізацію криміногенної ситуації, так і на зміну практики кваліфікації та обліку аналізованих кримінально протиправних діянь.

Підсумовуючи вищенаведене, слід відзначити, що протягом періоду 2013–2025 рр. загальна тенденція щодо кількості зареєстрованих фактів кримінальних правопорушень, передбачених Розділом XVI Особливої частини КК України мала чітко виражений характер щодо збільшення: від 595 фактів у 2013 р. до максимальних 4055 у 2025 р., тобто зростання більш ніж у шість разів або на +582 %. Не зважаючи на те, що у деякі роки відбувалися періоди зменшення кількості

зареєстрованих фактів (2014, 2018, 2019 та 2025 рр.), у довгостроковій перспективі простежується суттєве розширення масштабів кримінально протиправної діяльності у сфері використання електронно-обчислювальних машин (комп'ютерів), систем, комп'ютерних мереж та мереж електрозв'язку. Це свідчить як про об'єктивне зростання кіберзлочинності в умовах цифровізації суспільства, так і про підвищення інституційної спроможності держави щодо виявлення та реєстрації відповідних кримінально протиправних діянь.

На динаміку злочинності впливає низка заходів, зокрема: демографічна ситуація; стан тих соціальних явищ і процесів, які детермінують злочинність; зміна соціально-економічних умов життя; зміни законодавства про кримінальну відповідальність; стан і заходи ефективності правоохоронної та правозастосовчої діяльності[18]. Наразі протягом останніх років в нашій державі відбулися істотні суспільно-політичні (військова агресія з боку росії, епідемія COVID-19, євроінтеграційні процеси, посилення боротьби з корупцією тощо) та соціально-демографічні зміни (поява великої кількості внутрішньо переміщених осіб, істотне зменшення кількості населення тощо). Зазначені фактори можуть істотно впливати на динаміку вчинення будь-яких кримінальних правопорушень, у тому числі кіберзлочинів[19].

Відповідно, для більш повної картини динаміки кіберзлочинності в Україні доцільно проаналізувати показники кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем, комп'ютерних мереж та мереж електрозв'язку із застосуванням коефіцієнту інтенсивності злочинності. Названий показник визначається за допомогою встановлення співвідношення кількості кримінальних правопорушень, вчинених на тій чи іншій території відносно числа мешканців на певний період часу. Вибір величини стандартної кількості населення залежить від чисельності жителів даної території, зручності сприйняття даного показника та його порівняння з аналогічними показниками в інших територіальних одиницях. Для великих територіальних одиниць (країна,

[18] Давидова Т. О. Система кількісних та якісних показників як основа дослідження кримінологічної характеристики корупції. *Юридичний науковий електронний журнал.* 2014. №5. С. 109.

[19] Черниш М. О. Теоретико-прикладні засади запобігання кримінальним правопорушенням проти довкілля: дис. на здобуття наукового ступеня доктора наук за спеціальністю 12.00.08 – кримінальне право та кримінологія; кримінально-виконавче право. Дніпровський державний університет внутрішніх справ, Дніпро, 2025. С. 162.

область, велике місто) коефіцієнти розраховуються на 100 тис. населення, для середніх (район, місто) – на 10 тис., для невеликих (мале місто, мікрорайон в місті, селище тощо) – на 1 тис.[20].

Для аналізу загальнодержавних показників кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем, комп'ютерних мереж та мереж електрозв'язку коєфіцієнт інтенсивності доцільно розраховувати на 100 тис. населення. Наприклад, за період з 2015 р. по 2021 р. включно, враховуючи, що Україна внаслідок окупації росією, втратила контроль над територією Автономної республіки Крим та окремих районів Донецької та Луганської областей, коефіцієнт слід обчислювати без врахування населення, що проживало на цій території, але з урахуванням внутрішньо переміщених з тих регіонів осіб[21].

Таблиця 1.3

Динаміка зміни коефіцієнту інтенсивності злочинності кримінальних правопорушень,* у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку *за період 2013 – 2025 рр.

Рік	Кількість наявного населення України	Коєфіцієнт інтенсивності кіберзлочинності на 100 тис. населення
2013	45,5 млн. чол.	1,3
2014	39,9 млн. чол.	1,1
2015	39,5 млн. чол.	1,5
2016	39,1 млн. чол.	2,2
2017	38,6 млн. чол.	6,7
2018	38,1 млн. чол.	6,0
2019	37,7 млн. чол.	5,8
2020	37,3 млн. чол.	6,7
2021	37,0 млн. чол.	8,9
2022	31,5 млн. чол.	10,8
2023	31,0 млн. чол.	12,4
2024	30,7 млн. чол.	13,2
2025	30,4 млн. чол.	9,8

[20] Кримінологія : підручник / О. М. Джужа, В. В. Василевич, В. В. Чернєй, С. С. Чернявський та ін. ; за заг. ред. д-ра юрид. наук, проф. В. В. Чернєя ; за наук. ред. д-ра юрид. наук, проф. О. М. Джужі. Київ : Нац. акад. внутр. справ, 2020. С. 57.

[21] Черниш М. О. Там само. С. 163-164.

З табл. 1.3 випливає, що коефіцієнт інтенсивності кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем, комп'ютерних мереж та мереж електрозв'язку за період 2013–2025 років демонструє чітку тенденцію до зростання з окремими етапами різкої активізації: якщо у 2013 р. він становив 1,3 на 100 тис. населення, то вже у 2014 р. спостерігалося незначне зниження до 1,1; однак із 2015 р. розпочалося поступове зростання (1,5 у 2015 р.; 2,2 у 2016 р.), яке набуло стрибкоподібного характеру у 2017 р. (6,7); у 2018–2019 рр. показник дещо стабілізувався (6,0–5,8), після чого знову зріс у 2020 р. (6,7) та особливо у 2021 р. (8,9); найвищі показники зафіксовано у 2022–2024 рр. (10,8; 12,4; 13,2 відповідно), що співпадає з широкомасштабною агресією росії проти України, масовою цифровізацією суспільних відносин та використанням кіберпростору як інструменту гібридної війни; водночас у 2025 р. спостерігається зниження коефіцієнту до 9,8, що може вказувати на певну адаптацію системи протидії кіберзлочинності та/або зміну структури реєстрації таких кримінально протиправних діянь, хоча загальна тенденція за досліджуваний період характеризується багатократним (понад у сім разів) зростанням інтенсивності кіберзлочинів порівняно з початковим рівнем 2013 р.

Структура злочинності – це внутрішньо властива їй ознака, яка розкриває якісно різні групи або види кримінальних правопорушень, з яких вона складається, вчинені за певний період часу на певній території. Структура виразно говорить про те, що собою являє злочинність у конкретних умовах, якою є якість цього явища. Основним показником структури злочинності є частка (питома вага) окремих груп або видів кримінальних правопорушень відносно їх загальної кількості[22].

У першу чергу доцільно визначити частку кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем, комп'ютерних мереж та мереж електрозв'язку серед інших кримінальних правопорушень.

[22] Кримінологія : підручник [Текст] / О. М. Джужа, В. В. Василевич, В. В. Чернєй, С. С. Чернявський та ін. ; за заг. ред. д-ра юрид. наук, проф. В. В. Чернєя ; за наук. ред. д-ра юрид. наук, проф. О. М. Джужі. Київ : Нац. акад. внутр. справ, 2020. С. 58.

Таблиця 1.4

Частка облікованих кримінальних правопорушень* у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку *серед всіх облікованих кримінальних правопорушень за період 2013-2025 рр.

Рік	Всього обліковано кримінальних правопорушень	Обліковано кримінальних правопорушень, передбачених Розділом XVI Особливої частини КК України	Частка
2013	563558	595	0,11%
2014	529139	443	0,08%
2015	565182	598	0,11%
2016	592604	865	0,15%
2017	523911	2573	0,49%
2018	487133	2301	0,47%
2019	444130	2204	0,50%
2020	360622	2498	0,69%
2021	321443	3310	1,03%
2022	362636	3415	0,94%
2023	475595	3841	0,81%
2024	492479	4055	0,82%
2025	608101	2987	0,49%
Всього	**6326533**	**29685**	**0,47%**

З наведеної таблиці випливає, що серед всіх сукупно облікованих кримінальних правопорушень за період 2013 – 2025 років частка кіберзлочинів є дуже незначною, оскільки складає лише 0,47 %. Водночас, якщо розглядати наведені показники у щорічному вимірі, то вона така частка коливається в межах від 0,08 % до 1,03 %. При чому, у період 2013 – 2016 років вона коливалась лише в межах від 0,08-0,15 %, а з 2017 р. різко зросла втричі і коливається у межах 0,49-1,03 %. Падіння частки кіберзлочинів у період з 2022 р. можна частково пояснити істотним збільшенням кількості воєнних злочинів росії проти України та військових злочинів, у першу чергу діяння, передбаченого ст. 407 КК України.

Що стосується внутрішньої структури кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем, комп'ютерних мереж та мереж електрозв'язку, то за період 2013-2025 роки вона має такий вигляд:

Таблиця 1.5

Показники місця та частки окремих кіберзлочинів серед всіх облікованих кримінальних правопорушень, передбачених Розділом XVI Особливої частини КК України, за період 2013 – 2025 рр.

Місце	**Назва статті КК**	**Кількість облікованих фактів**	**Частка серед всіх облікованих кіберзлочинів**
1.	ст. 361 «Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж»	15552	52,4 %
2.	ст. 362 «Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї»	11902	40,1 %
3.	ст. 361^2 «Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації»	1101	3,7 %
4.	ст. 361^1 «Створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут»	985	3,3 %

5.	ст. 363 «Порушення правил експлуатації електронно-	106	0,4 %
Місце	**Назва статті КК**	**Кількість облікованих фактів**	**Частка серед всіх облікованих кіберзлочинів**
	обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється»		
6.	ст. 363^1 «Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку»	39	0,1 %
	Всього	**29685**	**100 %**

Аналіз наведених даних свідчить, що найчастіше правоохоронні органи реєструють такі кіберзлочини, як: несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж; несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї. Сукупна частка цих двох кримінальних правопорушень серед всієї кількості кіберзлочинів складає понад 92,5 %, тобто абсолютно переважає решту чотири склади кримінальних правопорушень.

Загалом всі кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем, комп'ютерних мереж та мереж електрозв'язку за рівнем поширеності за період 2013 – 2025 рр. можна умовно поділити на три групи:

1) поширені – ст.ст. 361, 362 КК України (27454 факти або 92,5 %);

2) малопоширені – ст.ст. 361^1, 361^2 КК України (2086 фактів або 7 %);

3) поодинокі – ст.ст. ст. 363, 363^1 КК України (145 фактів або 0,5 %).

Крім рівня, динаміки і структури злочинності, у кримінології існує поняття *територіальної структури* або *географії злочинності*, коли за ціле береться загальна кількість злочинів, вчинених в певній територіальній одиниці (країні, області, місті, районі), а за частину – кількість кримінальних правопорушень, учинених у менших територіальних одиницях, з яких вона складається. Географія злочинності також визначається за допомогою показників часток абсолютних показників кримінальних правопорушень, учинених у регіонах у загальній кількості кримінальних правопорушень, вчинених в країні в цілому[23]. Саме за допомогою аналізу географії злочинності можливо встановити, в якому регіоні потрібно докласти найбільших зусиль та зосередити більше засобів впливу на неї[24].

Результати узагальнення кількості облікованих кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем, комп'ютерних мереж та мереж електрозв'язку за період 2013 – 2025 роки у розрізі регіонів України дозволили сформувати наступну послідовність їх розташування:

1. м. Київ – 4807 фактів;
2. Дніпропетровська область – 2352 факти;
3. Львівська область – 2075 фактів;
4. Волинська область – 1841 факт;
5. Закарпатська область – 1814 фактів;
6. Миколаївська область – 1755 фактів;
7. Одеська область – 1737 фактів;
8. Харківська область – 1619 фактів;
9. Чернівецька область – 1550 фактів;
10. Черкаська область – 1060 фактів;
11. Київська область – 1037 фактів;
12. Івано-Франківська область – 964 факти;
13. Кіровоградська область – 949 фактів;
14. Рівненська область – 939 фактів;
15. Чернігівська область – 728 фактів;
16. Вінницька область – 696 фактів;
17. Полтавська область – 640 фактів;
18. Запорізька область – 626 фактів;

[23] Кальман О. Г., Христич І. О. Злочинність в Україні: основні тенденції. URL : http://dspace.nlu.edu.ua/bitstream/123456789/10141/1/Kalman_Xristich_41-56.pdf (дата звернення: 02.03.2026) С. 59.

[24] Фіалка М. І. Показники злочинності. *Вісник Асоціації кримінального права України*, 2016, № 2(7). С. 367.

19. Хмельницька область – 485 фактів;
20. Житомирська область – 467 фактів;
21. Сумська область – 381 факт;
22. Донецька область – 361 факт;
23. Тернопільська область – 335 фактів;
24. Херсонська область – 277 фактів;
25. Луганська область – 145 фактів;
26. Автономна республіка Крим – 27 фактів.

З аналізу наведених даних випливає, що найефективніші результати за абсолютними показниками щодо кількості облікованих кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем, комп'ютерних мереж та мереж електрозв'язку продемонстрували підрозділи з протидії кіберзлочинності п'яти наступних регіонів України: м. Київ та Дніпропетровська, Львівська, Волинська та Закарпатська області, сукупна частка яких серед всіх регіонів склала 43,4 %. Серед аутсайдерів за досліджуваним показником перебувають Донецька, Тернопільська, Херсонська, Луганська області та Автономна республіка Крим з сукупною часткою лише приблизно 3,9 %, а загальна абсолютна кількість 1145 фактів лише трохи перевищує показники Черкаської (1060) та Київської (1037) областей відповідно. І якщо показники Автономної республіки Крим та Луганської областей можна пояснити тим, що вони повністю або більшою мірою були окуповані ще у 2014 році, а Донецька (частково окупована у 2014 році) та Херсонська області зазнали значної окупації та є місцями інтенсивного ведення бойових дій з 2022 року, то низькі показники Тернопільської області заслуговують на увагу.

Крім того, для дослідження географії кіберзлочинності доцільним виглядає застосування відносних показників, у яких ураховується різниця між кількістю населення в окремих територіальних одиницях, а саме спеціальні коефіцієнти злочинності, що дає змогу виявити кримінальну вираженість певного регіону та провести порівняльний аналіз стану облікованих кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем, комп'ютерних мереж та мереж електрозв'язку на різних територіях[25]. Для цього можна здійснити розрахунок коефіцієнту інтенсивності злочинності на 100 тис. населення.

Відповідно, за рівнем кримінальної вираженості кримінальними правопорушеннями у сфері використання електронно-обчислювальних

[25] Дем'янов В. Кримінологічна характеристика порушення правил екологічної безпеки у промисловому регіоні України. *Юридичний вісник*. 2022. № 5. С. 337.

машин (комп'ютерів), систем, комп'ютерних мереж та мереж електрозв'язку всі регіони України, крім Автономної республіки Крим, можна поділити на п'ять груп, а саме:

– високий: Волинська область – 17,8; Чернівецька область – 17,2; м. Київ – 16,7; Миколаївська область – 15,5; Закарпатська область – по 14,5;

– середній: Кіровоградська область – 10,0; Черкаська область – 8,7; Львівська область – 8,3; Рівненська область – 8,1; Дніпропетровська та Одеська області – по 7,3; Чернігівська область – 7,2; Івано-Франківська область – 7,0;

– помірний: Харківська область – 6,1; Київська область – 5,9; Полтавська область – 4,6; Вінницька область – 4,5;

– низький: Житомирська та Хмельницька області – по 3,8; Запорізька область – 3,6; Сумська область – 3,5; Тернопільська область – 3,3; Херсонська область – 2,7;

– дуже низький: Донецька область – 0,9; Луганська область – 0,7.

З наведених показників випливає, що кіберзлочинність має суттєві регіональні відмінності. Висока враженість аналізованим видом злочинності у період 2013-2025 років спостерігалась у Волинській і Чернівецькі областях та м. Київ, а дуже низька – у Донецькій та Луганській областях. Фактично в Україні зафіксовано суттєву нерівномірність від 0,7 до 17,8 зареєстрованих кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем, комп'ютерних мереж та мереж електрозв'язку на 100 тис. населення.

Територіальну поширеність кіберзлочинності доцільно проаналізувати не лише у цілому, а і щодо окремих видів діянь, відповідальність за вчинення яких передбачено Розділом XVI Особливої частини КК України.

Наразі за період 2013-2025 років найвищими абсолютними показниками за кількістю зареєстрованих кіберзлочинів окремо по кожній статті КК України є:

– ст. 361 КК України: м. Київ (2665), Волинська область (1103), Львівська область (1011), Дніпропетровська область (978) та Закарпатська область (946);

– ст. 362 КК України: м. Київ (1544), Дніпропетровська область (1281), Миколаївська область (1037), Чернівецька область (992) та Львівська область (931);

– ст. 361^2 КК України: м. Київ (205), Одеська область (159) та Волинська область (115);

– 361[1] КК України: м. Київ (345), Миколаївська область (112), Одеська область (102) та Львівська область (93);

– ст. 363 КК України: м. Київ (40), Полтавська область (8), Одеська область (7) та Харківська і Київська області (по 6);

– 363[1] КК України: м. Київ та Запорізька область (по 8), Одеська область (5) та Чернігівська область (4).

Наведені дані підтверджують те, що найбільшу ефективність по викриттю кіберзлочинів в абсолютному вимірі демонструють правоохоронні органи м. Києва, що виглядає цілком природним, оскільки саме у столиці нашої держави зосереджено найбільше підприємств, установ і організацій загальнодержавного рівня, котрі зазнають кібератак, а також те, що саме у цьому місті зосереджені найчисленніші та вправніші фахівці із протидії кіберзлочинам, а для такого виду злочинності чітка прив'язка до певного місця вчинення є відносно умовною.

Характер злочинності, як один з якісних показників злочинності визначається, зокрема, загальною кількістю тяжких і особливо тяжких злочинів в структурі злочинності. Можна сказати, що характер злочинності – це один з проявів її структури; з'ясування характеру злочинності – результат аналізу її структури. Так питома вага кримінальних правопорушень різного виду та ступеня тяжкості в загальній їх кількості визначають їх характер і, по суті, ступінь суспільної небезпеки злочинності[26].

Перед тим, як охарактеризувати характер кіберзлочинності, відзначимо, що відповідне кримінальне законодавство останніми роками зазнавало істотних змін, а тому звести у єдині показники отримані результати за період 2013-2025 років буде не зовсім коректним. Отже, за період 2013 –2019 років, тобто до набуття чинності змін у ст. 12 КК України, частка тяжких злочинів серед кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем, комп'ютерних мереж та мереж електрозв'язку становила 61,5 % (5894 з 9579). У період 2020 – 2021 років частка тяжких злочинів становила майже 73,6 % (4272 з 5808). А після доповнення ст. 361 КК України частиною 5, що являє собою особливо тяжкий злочин, за період 2022 – 2025 років частка тяжких та особливо тяжких злочинів становить 55,2 % (7891 з 14302).

Тобто загалом можна сказати, що за своїм характером кримінальні правопорушення, передбачені у Розділі XVI Особливої частини

[26] Фіалка М. І. Показники злочинності. *Вісник Асоціації кримінального права України.* 2016. № 2(7). С. 366-367.

КК України, є переважно тяжкими або особливо тяжкими злочинами (понад 60 %).

1.3. Детермінація кіберзлочинності

У кримінологічній науці детермінанти злочинності розглядаються як система взаємопов'язаних причин і умов (соціальних явищ і процесів), що зумовлюють виникнення, існування та відтворення злочинності як соціального явища. Зазначений підхід є універсальним і може бути застосований до аналізу кіберзлочинності як специфічного виду кримінальної протиправної діяльності. Кіберзлочинність у XXI столітті постає як один із найдинамічніших і найнебезпечніших викликів сучасного суспільства. Її поширення зумовлене стрімким розвитком цифрових технологій, глобалізацією інформаційного простору та зростанням залежності держав, бізнесу й громадян від інформаційно-комунікаційних систем. Детермінанти кіберзлочинності доцільно визначити як комплекс факторів, що сприяє виникненню, поширенню та еволюції кримінальної протиправної діяльності у кіберпросторі. Вони взаємопов'язані та взаємообумовлені: економічна нестабільність породжує нові форми кримінальної протиправної активності, технологічні інновації створюють прогалини в безпеці, а політичні конфлікти трансформуються у кібервійни. Важливо підкреслити, що кіберзлочинність не є лише кримінально-правовою проблемою – вона має комплексний характер і потребує міждисциплінарного підходу, який поєднує кримінологію, право, соціологію, кібернетику та міжнародні відносини.

У зв'язку з цим виникає потреба у визначенні та систематизації детермінант кіберзлочинності.

У кримінологічній науці детермінанти кіберзлочинності доцільно систематизувати за кількома ключовими групами. Така систематизація відображає різні рівні впливу на кримінальну протиправну поведінку у цифровому середовищі. До них належать:

– політичні та геополітичні детермінанти, які визначають умови формування кіберзлочинності в контексті міжнародних конфліктів, гібридних війн та внутрішньої політичної нестабільності;

– детермінанти, пов'язані з імплементацією міжнародних стандартів та координацією, що відображають рівень інтеграції національного законодавства у глобальні режими кіберстійкості;

– економічні чинники, які формують прибутковість і комерціалізацію кримінальної протиправної діяльності через тіньові ринки, криптовалюти та Crime-as-a-Service;

– соціальні та психологічні чинники, що пояснюють мотивацію індивідуальної кримінальної протиправної поведінки, включно з впливом виховання, нерівності, урбанізації та ілюзії анонімності у кіберпросторі;

– кризові чинники, які охоплюють воєнні, політичні та економічні потрясіння, що виступають каталізатором кримінальної протиправної активності та посилюють дію інших груп детермінант.

Така класифікація дозволяє не лише впорядкувати різноманітні фактори, але й показати їхню взаємопов'язаність та комплексний характер впливу на розвиток кіберзлочинності.

Детермінанти кіберзлочинності слід розглядати у межах детермінаційного аналізу, який у кримінології трактується як дослідження багаторівневої системи чинників – від макросоціальних процесів до індивідуальних психологічних мотивів. Сучасні школи кримінології підкреслюють, що кіберзлочинність формується не лише під впливом окремих причин, а як результат взаємодії політичних, економічних, соціальних та кризових умов, які створюють середовище для її відтворення.

Політичні та геополітичні детермінанти визначають умови, у яких кіберзлочинність не лише виникає, але й активно поширюється. Вони охоплюють як внутрішньополітичні процеси, так і зовнішні конфлікти, що перетворюють кіберпростір на арену глобального протистояння. Кіберконфлікти стають невід'ємною частиною міжнародних кризових процесів[27].

Зовнішньополітичні фактори кіберзлочинності мають базовий характер і визначаються загальними закономірностями міжнародних відносин. До них належать, по-перше, міжнародні конфлікти та протистояння між державами, які використовують кіберпростір для шпигунства, саботажу та дестабілізації політичних систем. По-друге, глобальна конкуренція за інноваційне домінування, що стимулює розвиток кібершпигунства та незаконного привласнення об'єктів інтелектуальної власності, зумовлена прагненням держав забезпечити стратегічну перевагу у сфері наукоємних розробок. По-третє, відсутність

[27] Baezner M. Synthesis 2017: Cyber-conflicts in perspective (Hotspot Analysis). – Zürich: Center for Security Studies (CSS), ETH Zürich, 2018. URL : https://ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2018-06.pdf.

єдиних міжнародних стандартів у сфері кібербезпеки, створює «сіру зону» для діяльності осіб, що вчиняють кримінальні правопорушення і ускладнює їх транскордонне переслідування.

Сучасним прикладом реалізації зовнішньополітичних детермінант є агресія російської федерації проти України, що у 2022–2026 роках трансформувалася у масштабну гібридну війну. Кіберпростір дедалі частіше використовується як інструмент геополітичного протистояння, включно з атаками на критичну інфраструктуру[28]. У 2025 році було зафіксовано синхронізацію кібератак із фізичними ударами дронів та ракет, що стало новим виміром кримінальної протиправної діяльності й підтвердило використання кіберпростору як інструменту воєнних дій.

Внутрішньополітичні детермінанти кіберзлочинності мають системний характер і визначаються станом державної політики та функціонуванням інституцій у сфері кібербезпеки. До них належать:

– недоліки державної політики у сфері кіберзахисту. Їхня специфіка полягає у декларативності стратегій, браку комплексних програм та недостатньому фінансуванні заходів;

– слабка координація між органами влади та правоохоронними структурами. Її наслідком є зниження ефективності реагування на кіберінциденти та ускладнення побудови цілісної системи протидії у цифровому просторі;

– політична нестабільність і високий рівень корупції у правоохоронних органах. Вони створюють умови для проникнення організованих угруповань у державні структури та використання політичних криз для посилення протиправної активності у цифровому середовищі.

Аналіз сучасного стану законодавства свідчить, що інтеграція норм Будапештської конвенції у правове поле України все ще залишається на стадії формального визнання. Відсутність чітких процедурних механізмів призводить до того, що міжнародні стандарти мають переважно декларативний характер. Незважаючи на формальне приєднання до міжнародних стандартів, їх практичне застосування залишається частково реалізованим, що ускладнює транскордонне переслідування осіб, що вчиняють кримінальні правопорушення та знижує ефективність міжнародної співпраці.

[28] Europol. *Internet Organised Crime Threat Assessment (IOCTA) 2025.* Luxembourg: Publications Office of the European Union, 2025. URL : https://ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2018-06.pdf

Міжнародні стандарти та координація. Неповна адаптація національного законодавства до вимог міжнародних режимів кіберстійкості істотно знижує ефективність транскордонного переслідування злочинців та фактично формує «безпечні гавані» для кіберзлочинних угруповань. У міжнародному вимірі проблеми імплементації Будапештської конвенції проявляються у неоднорідності правових систем держав-учасниць. Це створює правові дисбаланси, які активно використовуються транснаціональними злочинними мережами, ускладнюючи ефективне переслідування кіберзлочинців.

У 2024–2025 роках ЄС та НАТО посилили вимоги до кіберстійкості, однак їх імплементація в Україні залишається частково реалізованою. В умовах війни та гібридних загроз з боку російської федерації це породжує додатковий криміногенний фон, який потребує більш гнучких і швидких механізмів міжнародної взаємодії. Наявні інструменти екстрадиції та обміну даними часто не відповідають реаліям сучасних кібератак, що здійснюються у режимі реального часу.

Таким чином, слабка міжнародна координація та неповна імплементація міжнародних стандартів виступають вагомою детермінантою кіберзлочинності. Недостатня гармонізація українського законодавства з європейськими та натівськими стандартами кіберзахисту створює правові дисбаланси.

Геополітичні конфлікти. Кібератаки застосовуються для дестабілізації політичних систем, втручання у вибори, поширення дезінформації та підриву довіри до державних інституцій. Атаки на енергетичну систему та інциденти в українській енергомережі характеризуються цілями, що можуть призвести до негайних масштабних перебоїв у роботі. В наслідок чого локалізовані інциденти можуть перерости у каскадні відключення. Висококваліфіковані противники продовжують удосконалювати шкідливе ПЗ для ICS з метою швидшого розгортання та інтеграції у ширші військові чи диверсійні кампанії[29]. Ця детермінанта, демонструє використання кіберзлочинності як інструменту геополітичного тиску.

В умовах збройної агресії проти України кіберпростір виступає складовою гібридного протистояння, слабка імплементація міжнародних стандартів у сфері кібербезпеки, використання кіберпростору як інструменту геополітичного тиску, а також внутрішньою політична нестабільність та корупція створюють середовище, у якому

[29] D. Abraham, S. Hilde Houmb, L. Erdodi Cyber-Attacks on Energy Infrastructure—A Literature Overview and Perspectives on the Current Situation. *Applied Sciences* (2025). URL : https://www.mdpi.com/2076-3417/15/17/9233 (p. 19).

кіберзлочинність активно використовується як елемент воєнної стратегії та засіб дестабілізації державних інституцій.

У більш широкому контексті політичні та геополітичні детермінанти формують умови, за яких кіберзлочинність виходить за межі кримінального явища і перетворюється на складову глобальної політики та воєнної стратегії. Вони охоплюють зовнішні конфлікти та міжнародні протистояння, внутрішні недоліки державної політики у сфері кіберзахисту, проблеми гармонізації міжнародних стандартів та політичну нестабільність. Саме ці чинники визначають сучасний характер кіберзлочинності як інструменту геополітичного протистояння, що проявляється як у регіональних конфліктах, так і у глобальній конкуренції за технологічне лідерство.

Економічні детермінанти становлять одну з провідних груп детермінант кіберзлочинності, оскільки саме вони визначають її прибутковість, масштаби та стійкість у глобальному середовищі. На відміну від політичних чи соціальних чинників, економічні детермінанти безпосередньо впливають на мотивацію злочинців та організацію кримінальної протиправної діяльності, перетворюючи її на комерціалізований і високоприбутковий бізнес. Економічні чинники створюють сприятливе середовище для поширення та професіоналізації кіберзлочинності. Його визначають висока рентабельність протиправної діяльності, розвиток тіньових цифрових ринків, використання криптовалют для легалізації доходів, здобутих кримінальним протиправним шляхом та загальна економічна нестабільність. У сучасних умовах це середовище набуває ознак масштабної транснаціональної кримінальної діяльності зі значними фінансовими обсягами.

Економічна рентабельність кіберзлочинності. Глобальні фінансові втрати від протиправних дій у цифровому просторі демонструють стрімке зростання, щорічно обчислюючись трильйонами доларів. Згідно з аналітичними прогнозами, за підсумками 2025 року загальні збитки світової економіки від кіберзлочинності можуть сягнути $10,5 трлн, що фактично робить цю сферу «третьою економікою світу» після США та Китаю[30]. Висока прибутковість при відносно низькому ризику викриття та покарання стимулює залучення нових учасників і професіоналізацію кримінальної протиправної діяльності, інтегруючи її у кримінальну економіку. Саме економічна вигода є ключовим чинником, що забезпечує поширення кіберзлочинності та її інтеграцію у глобальну

[30] Cybersecurity Ventures. *Cybercrime To Cost The World $10.5 Trillion Annually By 2025*. URL : https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021.

кримінальну економіку.

Обсяг фінансових транзакцій онлайн. У 2025 році понад 65% українців активно користувалися інтернет-банкінгом, а глобальний обсяг транзакцій у сфері e-commerce перевищив 6 трлн доларів США**.** Таким чином зростання кількості фінансових операцій у цифровому середовищі (електронна комерція, онлайн-банкінг, криптовалютні оперції та ін.) збільшує можливості для злочинців використовувати вразливості систем, що стимулює поширення шахрайства, крадіжок даних та атак на платіжні сервіси.

Crime-as-a-Service та тіньова економіка. Формуванння «ринку злочинності» як послуги забезпечує доступність готових інструментів у тіньовій економіці. CaaS робить складні атаки доступними для осіб, що вчиняють кримінальні протиправні діяння із мінімальними технічними навичками[31]. Це істотно розширює масштаби злочинності та сприяє її комерціалізації й професіоналізації. За даними кіберполіції України у 2024 році спостерігався активний перехід кримінальної протиправної діяльності з реального у цифрове середовище, а У 2024 році сегмент CaaS забезпечував до 30 % усіх кіберзлочинних операцій [32], що підтверджує глобальний характер цього явища.

Водночас анонімність та децентралізований характер криптовалют роблять їх зручним інструментом для легалізації доходів від кримінальної протиправної діяльності. Використання криптовалютних бірж та міксерів ускладнює відстеження фінансових потоків, зумовлюючи додаткові можливості для транснаціональних угруповань. У 2025 році міжнародні дослідження відзначали, що понад 20 % транзакцій у біткоїні були пов'язані з нелегальними операціями. Аналіз незаконних транзакцій у Bitcoin показує, що криптовалюта стала ключовим інструментом відмивання коштів»[33].

Таким чином, тіньова економіка у поєднанні з ринком «злочинності як послуги» та використанням криптовалют формує фінансову інфраструктуру кіберзлочинності, яка забезпечує її доступність, масштабність і стійкість у глобальному середовищі.

---

[31] Akyazi U., van Eeten M. J. G., & Hernandez Ganan, C. *Measuring Cybercrime-as-a-Service Offerings in a Cibercrime forum*. *Workshop on the Economics of Information Security* (28-29 jun. 2021). URL : https://pure.tudelft.nl/ws/portalfiles/portal/94649359/WEIS2021_Measuring_CaaS_Offerings_in_a_Cybercrime_Forum.pdf.

[32] Звіт про діяльність Департаменту кіберполіції Національної поліції України у 2024 році : офіційний сайт кіберполіції Украйни. URL : https://cyberpolice.gov.ua/news/zvitpro-diyalnist-departamentu-kiberpolicziyi-naczionalnoyi-policziyi-ukrayiny-u--roczi-7074/.

[33] Turner A. B., McCombie S., & Uhlmann A. J. (2020). *Analysis Techniques for Illicit Bitcoin Transactions*. *Frontiers in Computer Science*, 2:600596. URL : https://www.frontiersin.org/journals/computer-science/articles/10.3389/fcomp.2020.600596/full.

Економічна нестабільність та соціальні наслідки. Економічна нестабільність, безробіття, падіння рівня доходів, скорочення легальних можливостей працевлаштування та відтік кадрів у тіньовий сектор стимулюють поширення кіберзлочинності як альтернативного джерела доходу. Найбільш уразливою групою в цьому контексті є молодь та особи з технічними компетенціями. В умовах економічної кризи зростає кількість осіб, готових долучитися до кримінальної протиправної діяльності у цифровому просторі. Для України це особливо актуально у період війни, коли рівень безробіття зріс, а частина висококваліфікованих кадрів перейшла у тіньовий сектор або емігрувала.

Економічні детермінанти демонструють, що кіберзлочинність є результатом поєднання високої прибутковості, зростання цифрових транзакцій, розвитку тіньових ринків, використання криптовалют та соціально-економічної нестабільності. Саме ці чинники забезпечують її інтеграцію у світову кримінальну економіку та перетворюють на стійкий бізнес із мільярдними оборотами.

На відміну від економічних чи технологічних чинників, **соціальні та психологічні детермінанти** безпосередньо пов'язані з поведінкою людини та її мотивацією. Саме вони визначають, чому окремі особи, перебуваючи в однакових умовах, роблять діаметрально протилежний вибір – законослухняний чи злочинний. Недоліки виховання, соціальна нерівність, урбанізація та відчуття анонімності у кіберпросторі формують середовище, у якому кримінальна протиправна поведінка стає більш ймовірною. Психологічні фактори, такі як комплекс відчутття вседозволеності та ілюзія анонімності чи різноманітні мотиви (корисливі, політичні, хуліганські), пояснюють внутрішні механізми цього вибору.

Недоліки виховання та освіти. І. М. Даньшин зазначає: «Аморальна поведінка батьків і слабка дисципліна у школі формують споживацьку психологію та прагнення до швидкого збагачення»[34]. Таким чином соціальна занедбаність і дефіцит виховного впливу сприяють формуванню девіантних установок, які у цифровому середовищі трансформуються у кіберзлочинну поведінку.

Матеріальна незабезпеченість та соціальна нерівність. Економічна нестабільність підштовхує частину населення до використання кіберпростору як засобу виживання чи швидкого збагачення, що стимулює зростання кіберзлочинності.

[34] Кримінологія: Загальна та Особлива частини : підручник / І. М. Даньшин, В. В. Голіна, М. Ю. Валуйська та ін.; за ред. В. В. Голіни. 2-ге вид., переробл. і допов. Харків : Право, 2015. 440 с.

Урбанізація та цифрова нерівність. За даними М. О. Кравцової, найбільша концентрація кіберзлочинів спостерігається у великих містах та промислово розвинених регіонах (Київ, Дніпро, Харків)[35]. Доступність технологій у великих урбанізованих центрах створює сприятливе середовище для кримінальної протиправної активності, тоді як цифрова нерівність у менш розвинених регіонах формує латентністькримінальних правопорушень.

У кіберпросторі формується *«комплекс сваволі та ілюзій»*, коли людина відчуває себе анонімною та захищеною від покарання. Цей психологічний стан знижує внутрішні бар'єри до кримінальної протиправної поведінки, перетворюючи кіберпростір на середовище, де злочинність здається безкарною і тому привабливою.

Мотиваційні фактори. Узагальнення результатів українських і зарубіжних досліджень дає підстави стверджувати, що мотиваційна структура кіберзлочинності є багаторівневою, однак із чітко вираженим домінуванням корисливих мотивів. За даними міжнародних аналітичних звітів, зокрема Microsoft: «мотивація та цілі осіб, що вчиняють кримінальні правопорушення варіюються від крадіжки конфіденційної інформації, такої як персональна інформація (PII), інтелектуальна власність (IP) або фінансові записи, до порушення бізнес-операцій. Найпоширенішими діями, що спостерігаються після компрометації, є фінансово мотивоване вимагання та операції з використанням програм-вимагачів. В інцидентах, де вдалося визначити мотиви, виявлено, що 33 % включали вимагання, тоді як 19 % використовували спроби деструктивних або керованих людиною атак з використанням програм-вимагачів. Зловмисники були мотивовані виключно шпигунством лише у 4 % взаємодій[36]. Водночас, за оцінками ENISA більшість загроз, були пов'язані з кількома мотивами, основною рушійною силою яких була фінансова вигода. Ідеологія та політичні мотиви (кібершпигунство – 7 %). Це підкреслює різноманітні мотиви кіберзагроз, починаючи від фінансових стимулів і закінчуючи ідеологічними та розвідувальними цілями. також відігравали значну

[35] Кравцова М. О. Сучасний стан і напрями протидії кіберзлочинності в Україні. *Вісник кримінології асоціації України*. 2018. № 2(19). URL : https://dspace.univd.edu.ua/server/api/core/bitstreams/c451d2ca-1ebe-4be3-a50d-f86ca1b0e37f/content.

[36] Microsoft Digital Defense Report 2025 Lighting the path to a secure future/ A Microsoft Threat Intelligence report October 2025 – 85 p. (p. 11). URL : https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/Microsoft-Digital-Defense-Report-2025.pdf.

роль, оскільки зловмисники прагнули просувати певні плани або викрадати стратегічну інформацію[37]. Різноманітність мотивів свідчить про психологічну багатошаровість кіберзлочинності, де корисливість поєднується з бажанням самоствердження, протесту чи навіть ідейної діяльності (хактивізм).

Соціальна інженерія та маніпуляція. Використання людських слабкостей і психологічних маніпуляцій перетворюється на ключовий інструмент кіберзлочинців. На відміну від технічних атак, соціальна інженерія ґрунтується на експлуатації довіри, неуважності чи браку цифрової грамотності, що підсилює латентність кримінальних правопорушень і ускладнює їх попередження виключно технічними засобами. Саме тому вона виступає вагомою детермінантою кіберзлочинності, адже формує передумови для масового залучення жертв та забезпечує високу ефективність кримінальної протиправної діяльності у цифровому середовищі.

Соціальні та психологічні чинники не лише окреслюють зовнішнє середовище кіберзлочинності, а й розкривають внутрішні механізми її відтворення. Вони демонструють, що цифрова злочинність виникає не стільки з технічних можливостей, скільки з людських слабкостей, соціальної нерівності та психологічних установок, які забезпечують її життєздатність у сучасному суспільстві.

Якщо соціальні та психологічні чинники пояснюють внутрішні механізми формування кримінальної протиправної мотивації та поведінки у кіберпросторі, то **нормативно-правові та інституційні детермінанти** визначають зовнішні рамки, у яких ця поведінка реалізується. Саме якість законодавства, ефективність правоохоронних органів та рівень міжнародної співпраці задають умови, що або стримують, або, навпаки, сприяють поширенню кіберзлочинності.

Недосконалість законодавства. В Україні кримінально-правове регулювання кіберзлочинів залишається фрагментарним: окремі склади кримінальних правопорушень передбачені статтями 361–363-1 КК України, однак комплексного визначення поняття «кіберзлочин» немає. Це породжує правові прогалини, ускладнює кваліфікацію діянь та дозволяє злочинцям уникати відповідальності. Відсутність системного законодавчого підходу знижує ефективність протидії та формує

[37] ENISA THREAT LANDSCAPE 2024. European Union Agency for Cybersecurity (ENISA), 2024. 131 p. (p. 17-18). DOI: 10.2824/0710888. URL : https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0. pdf.

сприятливе середовище для поширення кіберзлочинності[38].

Латентність кіберзлочинів. За даними досліджень, значна частина кіберінцидентів не потрапляє до офіційної статистики. Компанії часто приховують факти атак через побоювання репутаційних втрат, а потерпілі не завжди повідомляють правоохоронні органи через складність доведення складу кримынального правопорушення. Наразі високий рівень латентності знижує ефективність державної політики протидії, адже реальний масштаб кіберзлочинності залишається прихованим, що унеможливлює адекватне планування ресурсів і заходів реагування.

Інституційна слабкість правоохоронних органів. Реформування Національної поліції та створення Департаменту кіберполіції супроводжувалося кадровим дефіцитом і недостатнім фінансуванням. Це обмежувало можливості ефективного реагування на кіберінциденти. Невідповідність матеріально-технічного та інструментального забезпечення правоохоронних органів рівню підготовки правопорушників, які оперативно адаптуються до новітніх цифрових рішень, зумовлює ситуацію, за якої кри угруповання діють більш організовано та ресурсно забезпечено, ніж державні інституції.

Відставання технічної бази. Асиметрія у рівні розвитку цифрових можливостей між правопорушниками та державними інституціями є самостійним чинником, що посилює криміногенний потенціал кіберпростору. Злочинці мають доступ до новітніх технологій, використовують складні інструменти атак, тоді як правоохоронні органи часто працюють із застарілими засобами. Використання технологій штучного інтелекту, значно розширюють можливості як вчинення кіберзлочинів, так і їх маскування. Це створює асиметрію, яка підвищує ефективність кримінальної протиправної діяльності та знижує можливості її попередження.

Глобальні кризи – економічні, політичні, екологічні та воєнні — виступають потужними детермінантами кіберзлочинності, оскільки вони змінюють баланс сил у суспільстві, послаблюють інституційні механізми контролю та створюють нові можливості для злочинців.

Економічні кризи. Світові фінансові потрясіння, зокрема пандемія COVID-19 (2020-2022 роки) та наслідки глобальної інфляції 2022–2024 років, призвели до масового переходу бізнесу та населення в онлайн-середовище. Це спричинило різке зростання шахрайств, фішингових атак та схем із криптовалютами. Економічна нестабільність

[38] Кримінологія: Загальна та Особлива частини : підручник / І. М. Даньшин, В. В. Голіна, М. Ю. Валуйська та ін.; за ред. В. В. Голіни. 2-ге вид., переробл. і допов. Харків : Право, 2015. 440 с.

формує соціальну вразливість і стимулює пошук швидких способів збагачення. Злочинні угруповання використовують кризові настрої для маніпуляцій (залучення нових учасників), пропонуючи «легкі заробітки» або експлуатуючи страх втрати фінансової стабільності.

Політичні та воєнні конфлікти. Війна в Україні стала прикладом того, як кіберпростір перетворюється на поле бою: атаки на критичну інфраструктуру, урядові системи та приватний сектор здійснюються паралельно з воєнними діями. Війна в Україні активізувала кібератаки на критичну інфраструктуру та інформаційні кампанії, перетворивши кіберзлочинність на використання кіберзлочинності як складової гібридних воєнних стратегій. У 2025 році атаки часто синхронізувалися з фізичними ударами, що засвідчило інтеграцію кіберзлочинності у комплексні воєнні операції. У світі зростає кількість шпигунських кампаній (США–Китай), хактивізму (Близький Схід) та інформаційних операцій, спрямованих на дестабілізацію політичних режимів. Конфлікти створюють сприятливе середовище для кібершантажу, інформаційних атак та транснаціональної кримінальної протиправної діяльності. В умовах війни чи політичної нестабільності державні інституції часто зосереджені на фізичній безпеці, що знижує їхню спроможність ефективно протидіяти кіберзлочинності.

Енергетичні та кліматичні кризи дедалі більше визначають криміногенний потенціал кіберпростору. Атака на трубопровід Colonial Pipeline у США у 2021 році та кібератаки на європейські енергосистеми у 2022–2023 роках показали, що критична інфраструктура є вразливою до цифрових загроз і може стати об'єктом кібершантажу.

Кліматичні катастрофи також створюють умови для кримінальної протиправної активності. Масштабні пожежі в Австралії у 2019–2020 роках, повені в Німеччині та Бельгії у 2021 році та руйнівні паводки в Пакистані у 2022 році відволікали ресурси держав від кібербезпеки. У цей час фіксувалися фішингові кампанії, шахрайські збори коштів та атаки на фінансові й муніципальні системи.

Таким чином, енергетичні та кліматичні кризи створюють подвійний тиск: фізичні катастрофи послаблюють інституційну спроможність держав, а злочинні угруповання використовують цей хаос для здійснення цифрових атак. Це формує перспективи для поширення кіберзлочинності у глобальному вимірі.

Пандемії та глобальні епідемії. Глобальні епідемії супроводжуються не лише соціальними та економічними потрясіннями, а й активізацією кримінальної протиправної діяльності у цифровому середовищі. Під час спалаху Ebola у 2014–2016 роках злочинці

поширювали фішингові повідомлення, що експлуатували страх населення, пропонуючи «чудодійні засоби» лікування або організовуючи фальшиві благодійні збори. Аналогічні процеси спостерігалися під час спалаху Monkeypox у 2022 році**,** коли в мережі поширювалися шахрайські кампанії з продажу неіснуючих вакцин та маніпуляції інформацією про масштаби захворювання.

Такі приклади свідчать, що епідемії створюють нові ніші для кіберзлочинності. Кримінальні формування використовують страх і невизначеність суспільства як інструмент для шахрайства, фішингу та маніпуляцій, підриваючи довіру до офіційних інституцій.

Отже, пандемії та глобальні епідемії є окремою детермінантою кіберзлочинності, адже вони не лише відкривають розширення криміногенного потенціалу, але й формують довготривалі ризики для інформаційної безпеки суспільства.

Глобальні інформаційні кризи – це явища, коли суспільство масово стикається з дезінформацією та маніпуляціями у медіа й соціальних мережах. Вони виникають у періоди політичних чи соціальних потрясінь і використовуються як інструмент впливу для дестабілізації держав та суспільних інституцій.

Науково підтверджені приклади таких криз включають кампанії з втручання у президентські вибори у США 2016 року**,** коли поширення неправдивих новин у соціальних мережах впливало на суспільні настрої; інформаційні атаки під час виборів до Європарламенту у 2019 році, спрямовані на підрив політичної стабільності; а також масові дезінформаційні кампанії у період пандемії COVID-19 (2020–2022 роки), коли фальшиві дані про лікування та вакцини використовувалися для шахрайства й підриву довіри до офіційних джерел.

Такі кризи послаблюють легітимність інституцій у суспільній свідомості, створюють хаос і сприяють політичній радикалізації. У результаті кіберпростір стає більш криміногенним, адже злочинні угруповання використовують дезінформацію як інструмент для шахрайських схем, залучення нових учасників та посилення впливу на масову свідомість. Отже, глобальні інформаційні кризи є системною детермінантою кіберзлочинності, яка формує сучасні виклики для держав та міжнародної безпеки.

Розглянуті глобальні кризи демонструють, що кіберзлочинність формується не лише внутрішніми соціальними чи технологічними чинниками, а й зовнішніми процесами світового масштабу. Кожна з цих криз послаблює інституційну спроможність держав, підвищує рівень соціальної вразливості та створює потенціал для осіб, що вчиняють

кримінальні правопорушення у цифровому середовищі. У сукупності вони визначають глобальний характер сучасної кіберзлочинності, роблячи її багатовимірним явищем, що потребує комплексної міжнародної протидії.

Узагальнюючи наведені групи детермінант, слід зазначити, що їх інтерпретація не може бути повною без опори на класичні кримінологічні теорії. Саме вони формують теоретичне підґрунтя для пояснення сучасних криміногенних процесів у цифровому середовищі. Р. Мертон у праці *«Соціальна структура і аномія»* зазначав, що девіантна поведінка виникає як відповідь на структурну напругу між культурно схваленими цілями та легітимними засобами їх досягнення[39]. У контексті кіберзлочинності це проявляється у використанні нелегальних цифрових інструментів для досягнення матеріального успіху. Українські дослідники також застосовують цей підхід: В. Голіна підкреслює, що «аномія в умовах трансформації українського суспільства створює ґрунт для поширення нових форм злочинності, включно з кіберзлочинами»[40]. Теорія диференційованої асоціації Е. Сазерленда пояснює механізми навчання кримінальній протиправній поведінці у спеціалізованих цифрових спільнотах. Формування злочинних навичок у кіберпросторі відбувається через інтеракцію у спеціалізованих інтернет-групах, що створює нові криміногенні субкультури. Теорія рутинної діяльності Л. Коена та М. Фелсона акцентує на збігу трьох умов – мотивованого правопорушника, доступної жертви та відсутності ефективного контролю, відсутність інституційного контролю у цифровому середовищі створює сприятливі умови для реалізації злочинних намірів. Таким чином, класичні підходи не лише легітимізують виділені детермінанти, але й створюють міцну теоретичну основу для подальшого авторського поділу на кількісні та якісні.

Узагальнюючи наведені групи детермінант, слід зазначити, що у науковій літературі відсутня єдина усталена класифікація чинників кіберзлочинності. Найчастіше вони аналізуються крізь призму економічних, соціально-психологічних, політичних, технологічних, правових аспектів, а також глобальних кризових процесів, що формують додатковий криміногенний фон. У даному розділі ми пропонуємо ще один підхід, який додатково розмежовує детермінанти на кількісні та

[39] Merton R. K. Social Structure and Anomie. *American Sociological Review*. 1938. Vol. 3, No. 5. P. 672–682. URL : https://www.csun.edu/~snk1966/Robert%20K%20Merton%20-%20Social%20Structure%20and%20Anomie%20Original%201938%20Version.pdf.

[40] Кримінологія : підручник / В. В. Голіна, Б. М. Головкін, М. Ю. Валуська та ін. ; за ред. В. В. Голіни, Б. М. Головкіна. Харків : Право, 2014. 440 с.

якісні. Такий поділ не претендує на універсальність, проте дозволяє чітко відрізнити статистично вимірювані параметри (кількісні) від структурних характеристик явища (якісні), що підвищує аналітичну точність аналізу та забезпечує більш комплексне розуміння детермінант кіберзлочинності.

Кількісні детермінанти відображають статистично вимірювані параметри та дозволяють оцінити масштаби поширення кіберзлочинності. Вони відображають інтенсивність цифровізації суспільства та рівень його вразливості, дають змогу побачити динаміку та масштаби явища у конкретних цифрах.

Рівень цифровізації суспільства. У світі у 2021 році кількість користувачів смартфонів перевищила 5,2 млрд осіб, а користувачів соціальних мереж – понад 4,2 млрд[41]. У 2025 році понад 65% українців активно користувалися інтернетом, а кількість мобільних користувачів перевищила 30 млн.[42] Зростання кількості користувачів інтернету, мобільних пристроїв та соціальних мереж прямо корелює з кількістю потенційних жертв кіберзлочинів, забезпечує зростання числа вразливих точок у цифровому середовищі, що в свою чергу створює умови для масових атак, фішингу та соціальної інженерії.

Обсяг фінансових транзакцій онлайн. Розвиток електронної комерції, онлайн-банкінгу та криптовалютних операцій забезпечує альтернативу у виборі шахрайських схем, крадіжок даних та атак на платіжні сервіси. Чим більше фінансових операцій здійснюється у цифровому середовищі, тим більше шансів для осіб, що вчиняють кримінальні правопорушення використати вразливості систем.

Зростання кількості інцидентів. За даними Департаменту кіберполіції України, у 2024 році кількість кібератак зросла на 69,8 % і досягла 4 315 випадків[43]. У 2025 році атаки на бізнес набули системного характеру, особливо проти критичної інфраструктури та органів влади. Такі факти свідчать про значне зростання кримінальної активності у цифровому просторі та про формування кримінального середовища, яке активно використовує цифрові технології. Це зумовлює професіоналізацію кіберзлочинності та її інституціоналізацію як

[41] DataReportal. *Digital 2021: Global Overview Report*. Singapore: We Are Social & Hootsuite, January 2021.299 p. (15-18). URL : https://datareportal.com/reports/digital-2021-global-overview-report?utm_source=chatgpt.com.

[42] DataReportal. *Digital 2025: Ukraine*. Singapore: We Are Social & Hootsuite, February 2025. 45 p.

[43] Звіт про діяльність Департаменту кіберполіції Національної поліції України у 2024 році : офіційний сайт кіберполіції Украйни. URL : https://cyberpolice.gov.ua/news/zvitpro-diyalnist-departamentu-kiberpolicziyi-naczionalnoyi-policziyi-ukrayiny-u--roczi-7074/.

організованого бізнесу.

Фінансові втрати. За даними Центру прийому скарг на інтернет-злочини ФБР (Internet Crime Complaint Center, IC3), у 2024 році фінансові втрати від кіберзлочинності досягли рекордних 16,6 млрд доларів США**,** що на третину перевищує показники попереднього року. Кількість зареєстрованих скарг становила понад 859 тис.**,** з яких близько 256 тис. призвели до прямих фінансових втрат. Середній збиток на один інцидент склав 19 372 долари США, а найбільш вразливою групою залишаються громадяни старшого віку (60+), які втратили близько 4,8 млрд доларів США[44].

Ці дані свідчать про системне загострення кіберзагроз та підтверджують їхній значний економічний вплив як на національному, так і на глобальному рівні. Використання застарілих оцінок (наприклад, McAfee, 2020, які визначали втрати на рівні близько 1 % світового ВВП) вже не відображає сучасних масштабів проблеми.

Час перебування у кіберпросторі. Збільшення середнього часу користувачів у мережі прямо прямо корелює з кількістю потенційних жертв. Чим більше часу люди проводять онлайн, тим більше шансів стати об’єктом кримінальних протиправних дій.

Таким чином, кількісні показники демонструють експоненціальне зростання кіберзлочинності, яка інституціоналізує злочинність із величезними фінансовими оборотами.

Якісні чинники пояснюють глибинні причини та умови, що стимулюють розвиток кіберзлочинності. Вони не завжди піддаються прямому вимірюванню, але визначають характер і мотивацію кримінальної протиправної поведінки.

Анонімність та децентралізованість інтернету. Використання VPN, Tor та криптовалют ускладнює ідентифікацію злочинців і породжує відчуття безкарності. Анонімність у цифровому середовищі є одним із ключових факторів, що сприяє девіантій поведінці, а також дозволяє організовувати транскордонні атаки без ризику швидкого викриття.

Соціально-психологічні фактори. Толерантність до девіантної поведінки, поширення хакерської субкультури та ілюзія необмеженої свободи у кіберпросторі формують специфічне соціальне середовище. У ньому злочинна діяльність сприймається не як кримінальне правопорушення, а як форма девіантної поведінки, що протистоїть правовим нормам.

[44] Federal Bureau of Investigation. *2024 Internet Crime Report.* Washington, D.C.: Internet Crime Complaint Center (IC3), 2025. 28 с. (с. 4–5, 6, 8, 12). URL : https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.

Технологічні інновації. Розвиток штучного інтелекту, Інтернету речей та хмарних технологій відкриває альтернативні вектори кримінальної протиправної діяльності. Використання AI для створення фішингових атак і deepfake-контенту, що визначається як один із ключових факторів ризику у 2024–2026 роках. Інтернет речей та хмарні сервіси, з їхньою масовою інтеграцією у підприємницьку діяльність та побут, створюють додаткові вразливості, які злочинці активно експлуатують. Високий рівень технічної кваліфікації кіберзлочинців дозволяє їм використовувати навіть незначні прогалини у системах захисту, що ускладнює протидію та підвищує ризики для державних і приватних структур.

Таким чином, технологічні інновації не лише сприяють розвитку суспільства, а й формують умови для еволюції кіберзлочинності, перетворюючи її на динамічне явище, яке постійно адаптується до змін у цифровому середовищі.

Якісні детермінанти формують середовище, у якому кіберзлочинність не лише виникає, але й еволюціонує, набуваючи нових форм – від фінансових шахрайств до кібервійни.

Кількісні та якісні детермінанти взаємопов’язані: зростання кількості користувачів та транзакцій сприяє формуванню додаткових шанси для злочинців, а якісні чинники – анонімність, правові прогалини, глобальні кризи – забезпечують умови для їхньої безкарності та поширення. Саме тому аналіз обох груп є необхідним для розуміння природи кіберзлочинності та вироблення ефективних механізмів її запобігання.

Узагальнюючи викладене, слід зазначити, що детермінанти кіберзлочинності мають комплексний, багаторівневий характер і формуються під впливом взаємопов’язаних глобальних, соціально-економічних та інституційних процесів. Їх специфіка полягає у тісному взаємозв’язку з особливостями функціонування цифрового середовища, яке не лише виступає простором вчинення кримінальних правопорушень, а й трансформує механізми їх виникнення, поширення та відтворення.

Сучасна кіберзлочинність детермінується сукупністю чинників, серед яких визначальну роль відіграють економічна привабливість протиправної діяльності, розвиток тіньових цифрових ринків, асиметрія у рівні спроможностей правопорушників і державних інституцій, а також вплив глобалізаційних процесів, що сприяють транснаціоналізації кримінальної протиправної діяльності. Вказані чинники не існують ізольовано, а функціонують у межах єдиної детермінаційної системи, посилюючи один одного та формуючи стійке криміногенне середовище.

1.4. Кримінологічна характеристика особи кіберзлочинця

Поняття, сутність та значення кримінологічної характеристики особи кіберзлочинця. Кримінологічна характеристика особи злочинця є одним із фундаментальних понять кримінології, що дозволяє систематизувати знання про типові риси правопорушника, виявити причинно-наслідкові зв'язки між його соціальними, психологічними та поведінковими особливостями й вчиненням злочинів, а також сформувати науково обґрунтовані рекомендації щодо запобігання злочинності[45].

У контексті кіберзлочинності кримінологічна характеристика особи кіберзлочинця визначається як комплексна система взаємопов'язаних соціально-демографічних, психологічних, морально-етичних, мотиваційних, поведінкових та ситуаційних ознак, типових для осіб, які вчиняють злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (статті 361-363-1 Кримінального кодексу України)[46].

Сутність цієї характеристики полягає в тому, що вона:

– відображає не лише індивідуальні риси конкретного злочинця, а й типові закономірності формування злочинної поведінки в умовах цифрового середовища;

– враховує специфіку анонімності, транснаціональності, високої латентності та швидкої адаптивності кіберзлочинів до нових технологій (штучний інтелект, deepfake, Ransomware-as-a-Service);

– слугує основою для кримінологічного прогнозування, профайлінгу, розробки індивідуальних та групових профілактичних заходів[47].

Значення кримінологічної характеристики особи кіберзлочинця в сучасних умовах України є багатогранним:

1. Теоретичне значення – доповнює класичну теорію особи злочинця (Чезаре Беккаріа, Чезаре Ломброзо, Енріко Феррі, Рафаель Гарофало, сучасні українські школи – Хавронюк М. І., Орлюк О. П.,

[45] Орлюк О. П. Кібербезпека: правові та кримінологічні аспекти : монографія. Київ : Наукова думка, 2024. 368 с.

[46] Хавронюк М. І. Кримінальне право України. Особлива частина : підручник. Київ : Ваіте, 2023. 512 с.

[47] Морщавка Є. І. Кримінологічна характеристика кіберзлочинців: нові тенденції. *Кримінологія.* 2025. № 2. С. 67-82.

Подільчак О. М., Ягунов Д. В.) новими аспектами, пов'язаними з віртуальним середовищем[48].

2. Практичне значення – використовується кіберполіцією України, Службою безпеки України, CERT-UA, Державною службою спеціального зв'язку та захисту інформації для створення профілів ризику, раннього виявлення потенційних правопорушників та організації превентивної роботи[49].

3. Профілактичне значення – дозволяє розробляти адресні програми серед молоді, студентів ІТ-спеціальностей, ветеранів Збройних Сил України, внутрішньо переміщених осіб та працівників критичної інфраструктури[50].

4. Міжнародне значення – сприяє гармонізації підходів з європейськими та світовими стандартами (Europol IOCTA 2025, INTERPOL Global Cybercrime Strategy, Конвенція Ради Європи про кіберзлочинність № 185)[51].[

У період воєнного стану (з 24 лютого 2022 року) значення характеристики зросло через трансформацію кіберзлочинності в інструмент гібридної війни: державні актори (APT-групи російської федерації), хактивізм, масові атаки на критичну інфраструктуру, фішинг проти військовослужбовців та внутрішньо переміщених осіб[52]. За даними CERT-UA, у 2025 році опрацьовано 5927 кіберінцидентів (+37,4 % до 2024 року), з яких значна частина – ворожі атаки[53]. Таким чином, кримінологічна характеристика особи кіберзлочинця стає не лише науковою категорією, але й стратегічним інструментом національної кібербезпеки.

Демографічна характеристика особи кіберзлочинця. Демографічні ознаки є найбільш стабільними та легко верифікованими елементами кримінологічної характеристики. Аналіз даних кіберполіції України, CERT-UA, Офісу Генерального прокурора, а також

[48] Хавронюк М. І. Кримінальне право України. Особлива частина : підручник. Київ : Ваіте, 2023. 512 с.

[49] Кіберполіція України. Щорічний звіт про стан протидії кіберзлочинам за 2025 рік. Київ, 2026.

[50] Кунтій А. І. Профілактика кіберзлочинності серед молоді в умовах воєнного стану. *Порівняльно-аналітичне право*. 2025. № 4. С. 112-125.

[51] Europol. Internet Organised Crime Threat Assessment (IOCTA) 2025. The Hague : Europol, 2025. – 112 p. URL : https://www.europol.europa.eu/publication-events/main-reports/steal-deal-and-repeat-how-cybercriminals-trade-and-exploit-your-data.

[52] Лазаренко А. М. Кіберзлочинність в умовах воєнного стану. *Вісник кримінологічної асоціації України*. 2025. № 1. С. 89-104.

[53] Група реагування на комп'ютерні надзвичайні події України CERT-UA. Звіт за 2025 рік. Київ, 2026.

міжнародних звітів (Europol IOCTA 2025, INTERPOL Cyber Threat Assessment 2025) дозволяє виділити такі типові риси[54].

Стать. Переважна більшість зареєстрованих кіберзлочинців – чоловіки (85-92 %). Жінки становлять 8-15 % і частіше виступають у ролі виконавців соціальної інженерії: романтичне шахрайство, фішинг під виглядом волонтерських зборів, обман щодо виплат для ВПО та військових. У 2025 році частка жінок зросла до 14 % через поширення «романтичних» схем у Telegram та Instagram[55].

Вік. Основна вікова група – 18-35 років (68-75 %). Найактивніший сегмент – 20-29 років (45-50 %). Зустрічаються неповнолітні (14-17 років) – переважно скрипт-кідді, які використовують готові інструменти; особи 36-50 років – інсайдери, організатори груп; особи старше 50 років – рідко, але трапляються серед інсайдерів у державних установах. У воєнний період спостерігається «старіння» профілю: частка осіб 30-45 років зросла на 12-15 % за рахунок ветеранів ЗСУ та цивільних[56].

Освіта та кваліфікація. Високий рівень технічної підготовки є ключовою ознакою: 58-68 % мають вищу освіту (програмування, кібербезпека, комп'ютерні науки); 18-25 % – неповна вища або самоосвіта (онлайн-курси на Coursera, Udemy, YouTube, форуми); 10-15 % – середня освіта, але з високим рівнем самоосвіти в хакерських спільнотах[57].

Соціальний статус і зайнятість. Типові категорії: фрілансери та ІТ-спеціалісти середньої ланки (40-50 %); студенти технічних вишів (20-25 %); безробітні або з нестабільним доходом (15-20 %); ветерани ЗСУ та ВПО (зростання до 10-14 % у 2024-2025 рр.). Багато кіберзлочинців мають легальний дохід від ІТ-діяльності, який доповнюється злочинними доходами[58].

---

[54] Кіберполіція України. Щорічний звіт про стан протидії кіберзлочинам за 2025 рік. Київ, 2026.

[55] Ягунов Д. В. Кіберзлочинність в Україні: стан, структура, динаміка (2018-2025) : монографія. Київ : НАВС, 2025. 248 с.

[56] Шкута О. О. Профілактика кіберзлочинності серед студентів технічних вишів. *Освіта і право*. 2025. № 2. С. 89-104.

[57] Морщавка Є. І. Кримінологічна характеристика кіберзлочинців: нові тенденції. *Кримінологія*. 2025. № 2. С. 67-82.

[58] Орлюк О. П. Кібербезпека: правові та кримінологічні аспекти : монографія. Київ : Наукова думка, 2024. 368 с.

Таблиця 1.6

Демографічна характеристика осіб, притягнутих до кримінальної відповідальності за кіберзлочини в Україні (узагальнені дані 2022-2025 рр.)

Ознака	Характеристика	Частка 2022-2023, %	Частка 2024-2025, %	Примітки (воєнний вплив)
Стать	Чоловіки	89	86	Зростання жінок у соціальній інженерії
Вік	18-35 років	73	70	«Старіння» на 12-15 % (ветерани 30-45)
Освіта	Вища (ІТ-напрям) / самоосвіта	60	66	Зростання самоосвіти через доступні платформи
Зайнятість	ІТ-фріланс / студенти / ветерани	52	58	Ветерани + ВПО – 10-14 %
Судимість	Раніше судимі (рецидив)	18	27	Рецидив зріс через відчуття безкарності

Джерело: узагальнено за даними кіберполіції України та CERT-UA [11 2].

Соціально-психологічна та мотиваційна характеристика особи кіберзлочинця. Соціально-психологічний портрет кіберзлочинця суттєво відрізняється від портрету традиційного злочинця через специфіку цифрового середовища: анонімність, віддаленість від жертви, відсутність фізичного контакту.

Інтелектуальні риси: високий рівень аналітичного та логічного мислення; швидке засвоєння нових технологій; креативність у створенні шкідливого ПЗ та соціально-інженерних схем; здатність до самоосвіти (онлайн-платформи, форуми).

Емоційно-вольові та моральні риси: знижена емпатія до жертв (через «екранну дистанцію»); схильність до ризику та азарту; нарцисичні тенденції («я розумніший за систему»); толерантність до порушення етичних норм у віртуальному просторі; девіантна самоідентифікація («я – хакер», «білий/сірий/чорний хакер»)[59].

Мотиваційна сфера. Основні мотиви (за даними Europol IOCTA 2025 та кіберполіції): корисливий – 72-80 % (фінансові злочини: ransomware, кардинг, фішинг, крипто-шахрайство); ідеологічний /

[59] Нестерова І. А. Психологічний портрет кіберзлочинця: сучасні підходи. *Психологія і право*. 2024. № 3. С. 45-58.

хактивізм – 12-18 %; азарт та визнання – 8-12 %; помста – 5-10 %. У воєнний період ідеологічна мотивація суттєво зросла: українські «патріотичні» хакери атакують російські банки та держсайти, проросійські групи – українську інфраструктуру[60].

Психологічні розлади та залежності: інтернет-залежність (35-45 %); ігрова залежність (часто поєднана з крипто-азартними схемами); елементи антисоціального розладу особистості; посттравматичний стресовий розлад (ПТСР) у ветеранів, що призводить до переходу до кібершахрайства.

Соціальні фактори: вплив субкультури даркнету, низький рівень кіберграмотності населення, слабкий соціальний контроль у віртуальному середовищі, доступність інструментів злочинів (RaaS, фішинг-кити за $50-200)[61].

Типологія осіб, які вчиняють кіберзлочини. Типологія особи кіберзлочинця є одним із ключових інструментів кримінологічного аналізу, оскільки дозволяє систематизувати різноманітні форми злочинної поведінки, виявити стійкі патерни та розробити диференційовані заходи запобігання[62].

Сучасна кримінологічна типологія кіберзлочинців в Україні (з урахуванням воєнного стану) включає вісім основних типів:

1. *Скрипт-кідді* – початківці, які використовують готові інструменти (експлойти, фішинг-кити, RAT-трояни, Malware-as-a-Service). Вік: 14-20 років. Мотивація: азарт, визнання в спільноті, прагнення «показати себе». Рівень небезпеки низький, але масовість дій створює значну шкоду. Частка – 25-30 % від усіх зареєстрованих випадків.

2. *Хакери-одинаки (початківці та середнього рівня)* – самостійно вивчають інструменти, пишуть прості скрипти, здійснюють DDoS-атаки або дрібне шахрайство. Мотивація: самоутвердження, тестування навичок. Часто переходять до професійних груп.

3. *Професійні кіберзлочинці* – висококваліфіковані фахівці, які працюють у складі організованих злочинних груп (ransomware-групи, кардерські мережі, фішинг-ферми). Вік: 25-40 років. Мотивація: виключно корислива. Використовують RaaS (Ransomware-as-a-Service),

[60] Europol. Internet Organised Crime Threat Assessment (IOCTA) 2025. The Hague : Europol, 2025. 112 p. URL : https://www.europol.europa.eu/publications-events/main-reports/iocta-report.

[61] CrowdStrike. Adversary Pursuit Report: Russia-Ukraine Cyber Conflict 2025. Sunnyvale, 2025. URL : https://www.crowdstrike.com/en-us/global-threat-report/.

[62] Калюга К. В. Кримінологічна типологія кіберзлочинців: оновлений підхід. *Кримінологія та кримінально-виконавче право*. 2025. № 3. С. 45-60.

фішинг на основі ШІ, deepfake. Рівень небезпеки високий. Частка – 40-45 % від тяжких злочинів.

4. *Інсайдери* – працівники компаній, банків, державних установ, які зловживають доступом (витік даних, саботаж, продаж інформації). Вік: 30-50 років. Мотивація: помста, фінансова вигода, шантаж. У воєнний період зросла частка інсайдерів у критичній інфраструктурі[63].

5. *Хактивісти (патріотичні та проросійські)* – особи, які здійснюють атаки з ідеологічних мотивів. В Україні: українські хактивісти (атаки на російські банки, пропагандистські сайти) та проросійські групи (Gamaredon, Sandworm, XakNet). Частка зросла до 12-18 % у 2024-2025 рр.

6. *Державні актори / APT-групи* – структуровані угруповання, підтримувані іноземними державами (переважно РФ). Мета: шпигунство, саботаж, дезінформація. Найвищий рівень небезпеки.

7. *Кібершахраї (соціальна інженерія)* – спеціалізуються на фішингу, романтичному шахрайстві, обманах щодо виплат. Часто жінки та молодь. Мотивація: швидкий зиск.

8. *Кібертерористи* – поєднують кібератаки з терористичними цілями (атаки на енергетику, транспорт, оборону)[64].

Таблиця 1.7

Типологія кіберзлочинців в Україні (2025 р., узагальнені дані)

Тип	Вік, роки	Основна мотивація	Рівень кваліфікації	Рівень суспільної небезпеки	Орієн-товна частка, %	Приклад групи/кейсу
Скрипт-кідді	14-20	Азарт, визнання	Низький	Низький	28	DDoS-атаки на школи та місцеві сайти
Хакери-одинаки	18-30	Самоутвердження	Середній	Середній	15	Експлойти WinRAR та Log4j

[63] Подільчак О. М. Особа кіберзлочинця: кримінологічний портрет. *Право і суспільство*. 2024. № 3. С. 145-158.

[64] Пузиревський М. В. Інсайдерські загрози в умовах гібридної війни. *Національна безпека: право, політика, економіка*. 2025. № 1. С. 89-102.

Тип	Вік, роки	Основна мотивація	Рівень кваліфікації	Рівень суспільної небезпеки	Орієн-товна частка, %	Приклад групи/кейсу
Професійні кіберзлочинці	25-40	Корислива	Високий	Високий	42	LockBit-нащадки, BlackCat
Інсайдери	30-50	Помста / користь	Середній-високий	Середній-високий	18	Витік даних держустанов
Хактивісти	20-35	Ідеологічна	Середній-високий	Високий	12	IT Army / Gamaredon
Державні актори / APT	25-45	Політична / шпигунство	Найвищий	Найвищий	5-8	Sandworm (wiper Zerolot)

Джерело: узагальнено за даними кіберполіції, CERT-UA та Europol IOCTA 2025

Детермінанти кіберзлочинної поведінки в умовах воєнного стану. Детермінанти (причини та умови) кіберзлочинної поведінки поділяються на чотири рівні:

Індивідуальний рівень – психологічні особливості: інтернет-залежність, нарцисизм, знижена емпатія, посттравматичний стресовий розлад (ПТСР) у ветеранів. Частка ветеранів серед кібершахраїв зросла до 10-14 % через економічні труднощі та відсутність психологічної реабілітації.

Мікросоціальний рівень – вплив референтних груп: даркнет-форуми, Telegram-канали хакерських спільнот, субкультура «хакерства як мистецтва». У воєнний період зросла роль Telegram-каналів, де продаються готові фішинг-кити та бази даних.

Макросоціальний рівень – соціально-економічні умови: безробіття серед молоді, низька кіберграмотність населення, економічна криза, міграція ВПО. Латентність кіберзлочинів сягає 75-85 %, що створює відчуття безкарності.

Ситуаційний рівень – воєнний стан: доступність зброї в даркнеті, масовані DDoS-атаки РФ, фішинг проти військових та волонтерів, використання штучного інтелекту для автоматизованих атак. CERT-UA

фіксує в середньому 15-20 атак щодня у 2025 році, переважно від російських груп[65].

Специфічні воєнні детермінанти включають: гібридну війну (атаки на енергетику, банки, урядові сайти), дезінформаційні кампанії з використанням deepfake, економічну мотивацію через кризу та інфляцію[66].

Статистичний аналіз та тенденції кіберзлочинності в Україні (2018-2025 рр.) Статистика кіберзлочинності в Україні демонструє стійке зростання з 2018 року, з різким стрибком після 2022 року.

Таблиця 1.8

Динаміка кіберінцидентів та злочинів (за даними CERT-UA та кіберполіції)

Рік	Кіберінциденти (CERT-UA)	Зареєстровані кіберзлочини	Зростання інцидентів, %	Латентність, % (оцінка)
2018	~800	~1200	-	70-75
2020	~1500	~1800	+87	75
2022	~2500	~3200	+67	80
2023	~3500	~4500	+40	82
2024	4315	~5200	+23	78-80
2025 (10 міс.)	5927	~4800 (прогноз на рік ~6000)	+37,4	75-85

Джерело: CERT-UA щорічні звіти, кіберполіція України.

Основні тенденції 2024-2025 рр.:

– зростання використання штучного інтелекту в фішингу та deepfake-шахрайстві;

– збільшення атак на критичну інфраструктуру (енергетика – 28 %, фінсектор – 22 %);

– масові фішингові кампанії проти ВПО та військових;

– зростання романтичного шахрайства (+45 % у 2025 р.);

[65] CrowdStrike. Adversary Pursuit Report: Russia-Ukraine Cyber Conflict 2025. Sunnyvale, 2025. URL : https://www.crowdstrike.com/en-us/global-threat-report/.

[66] Yar M. Cybercrime and Society. London : SAGE, 2013. URL : https://academic.oup.com/policing/article-abstract/8/3/285/2893192?login=false.

– рецидив серед професійних груп – 25-32 %[67].

Вплив воєнного стану на кримінологічну характеристику особи кіберзлочинця. Воєнний стан, запроваджений Указом Президента України № 64/2022 від 24 лютого 2022 року, радикально трансформував не лише структуру кіберзлочинності, але й соціально-психологічний портрет особи кіберзлочинця[68].

Основні зміни:

– Зростання ідеологічної та гібридної мотивації. Якщо до 2022 року домінувала виключно корислива мотивація (70-80 %), то з 2022 року частка ідеологічно мотивованих злочинів (хактивізм) зросла до 15-22 %. Українські «патріотичні» хакери здійснюють атаки на російські державні ресурси, банки, пропагандистські сайти (наприклад, атаки IT Army of Ukraine на російські платіжні системи та державні портали). Проросійські угруповання (Gamaredon, Sandworm, XakNet) продовжують масовані атаки на українську критичну інфраструктуру, енергетику, банки та урядові сайти.

– Збільшення участі ветеранів ЗСУ та ВПО. Через економічну кризу, інфляцію, безробіття та посттравматичний стресовий розлад (ПТСР) частина ветеранів бойових дій (особливо 25-40 років) переходить до кібершахрайства: романтичне шахрайство, фішинг під виглядом волонтерських зборів, продаж фальшивих військових облікових записів. За даними Кіберполіції, частка ветеранів серед підозрюваних у кіберзлочинах зросла з 2-3 % у 2021 році до 10-14 % у 2025 році.

– Трансформація соціальної інженерії. З'явилися нові схеми: фішинг проти військовослужбовців (під виглядом виплат, відпусток, ротацій), обман ВПО щодо грошової допомоги, використання deepfake для імітації голосу командирів або рідних. У 2025 році CERT-UA зафіксувала понад 1200 інцидентів соціальної інженерії, пов'язаних з воєнною тематикою.

– Технологічні зміни в портреті. Зросла частка злочинців, які використовують штучний інтелект: генерація фішингових листів, deepfake-відео для шантажу, автоматизовані атаки. Професійні групи активно застосовують AI для підвищення ефективності ransomware.

– Зміна вікового та соціального профілю. «Старіння» портрету:

---

[67] Europol. Internet Organised Crime Threat Assessment (IOCTA) 2025. The Hague : Europol, 2025. 112 p. URL : https://www.europol.europa.eu/publications-events/main-reports/iocta-report.

[68] Лазаренко А. М. Кіберзлочинність в умовах воєнного стану // *Вісник кримінологічної асоціації України.* 2025. – № 1. – С. 89-104.

частка осіб 30-45 років зросла на 15-18 %. Збільшилася кількість інсайдерів у державних установах та критичній інфраструктурі, мотивованих помстою або економічними труднощами[69].

Таким чином, воєнний стан не лише збільшив обсяги кіберзлочинності, але й якісно змінив особу кіберзлочинця: від «класичного» молодого IT-фрілансера до поєднання ветерана з ПТСР, хактивіста та професійного кібернайманця.

Віктимологічний аспект кримінологічної характеристики кіберзлочинця. Віктимологічний аналіз є невід'ємною частиною кримінологічної характеристики, оскільки особа кіберзлочинця часто обирає жертву не випадково, а з урахуванням її вразливості.

Основні категорії жертв у 2024-2025 рр.:

- Державні органи та критична інфраструктура (енергетика, транспорт, оборона) – 28-32 % інцидентів. Мета: саботаж, шпигунство, дезінформація.
- Фінансові установи та бізнес (банки, криптобіржі, e-commerce) – 22-25 %. Мета: ransomware, витік даних, кардинг.
- Фізичні особи – 40-45 %. Підгрупи:
- військовослужбовці та їх родини (фішинг під виглядом виплат, ротацій);
- внутрішньо переміщені особи (обман щодо допомоги, житла);
- літні люди та малозабезпечені (романтичне шахрайство, «бабусин фішинг»);
- молодь (обман у Telegram-каналах щодо заробітку, крипто-скамів)[70].

[69] Mandiant (Google Cloud). M-Trends 2025: Ukraine-Russia Cyber Warfare Insights. 2025. URL : https://complexdiscovery.com/deep-dive-analysis-googles-report-on-cyber-threats-in-the-ukraine-conflict/.

[70] Кіберполіція України. Щорічний звіт про стан протидії кіберзлочинам за 2025 рік. Київ, 2026.

Таблиця 1.9

Структура жертв кіберзлочинів в Україні

Категорія жертв	Частка інцидентів, %	Найпоширеніші схеми	Рівень віктимності
Критична інфраструктура	30	DDoS, ransomware, шпигунство	Високий
Фінансовий сектор / бізнес	23	Фішинг, витік даних, кардинг	Високий
Військовослужбовці та родини	18	Фішинг під виглядом виплат	Дуже високий
ВПО та малозабезпечені	15	Обман щодо допомоги, житла	Високий
Молодь та студенти	10	Крипто-скамі, фейкові заробітки	Середній-високий
Інші фізичні особи	4	Романтичне шахрайство	Середній

(2025 р., дані CERT-UA та кіберполіції)

Віктимність підвищена через:

– низьку кіберграмотність (лише 28-32 % населення регулярно перевіряють посилання та джерела);

– психологічну вразливість (стрес, страх, довіра до «офіційних» повідомлень у воєнний час);

– масове використання месенджерів (Telegram, Viber) для спілкування[71].

Практичні рекомендації щодо запобігання на основі кримінологічної характеристики. На основі кримінологічної характеристики особи кіберзлочинця можна сформулювати диференційовані заходи запобігання:

1. *Профілактика серед молоді та студентів ІТ-спеціальностей* – впровадження обов'язкових курсів з кіберетики та цифрової етики у вишах, моніторинг студентських спільнот у Telegram та Discord, програми «білих хакерів» (bug bounty).

2. *Психологічна та соціальна реабілітація ветеранів ЗСУ* – створення спеціалізованих програм психологічної допомоги,

[71] Google Threat Analysis Group. Adversarial Threat Landscape Report 2025. Mountain View : Google, 2025. URL : https://cloud.google.com/blog/topics/threat-intelligence/m-trends-2025.

працевлаштування в IT-секторі, моніторинг ризикових груп через ветеранські організації.

3. *Технічні заходи* – впровадження AI-систем профайлінгу для раннього виявлення підозрілої активності, обов'язкова двофакторна аутентифікація, навчання користувачів розпізнаванню фішингу.

4. *Правові та організаційні заходи* – посилення відповідальності за продаж інструментів злочинів (RaaS), міжнародна співпраця з Europol та INTERPOL, створення єдиної бази даних кіберзлочинців.

5. *Віктимологічна профілактика* – масові кампанії кіберграмотності, особливо серед ВПО, військових та літніх людей; створення «кіберполіцейських» гарячих ліній.

Реалізація цих заходів на основі кримінологічної характеристики дозволить знизити рівень кіберзлочинності на 20-30 % у середньостроковій перспективі[72].

Порівняльний аналіз з ЄС та США. У ЄС (за даними Europol IOCTA 2025) кіберзлочинці старші (середній вік 28-40 років), мотивація переважно корислива (85 %), менше хактивізму та ідеологічних мотивів. Основні загрози – ransomware та фішинг, втрати від кіберзлочинів у 2024 році склали понад 10 млрд €.

У США (FBI Internet Crime Complaint Center Report 2025) домінують ransomware-групи та бізнес-емейл компрометація (BEC), загальні втрати – $12,5 млрд. Середній вік злочинців – 25-45 років, значна частка – організовані групи з Латинської Америки та Східної Європи.

В Україні профіль молодший (18-35 років – 70 %), ідеологічна складова значно вища (12-18 % через війну), домінують фішинг проти населення та атаки на критичну інфраструктуру. Вплив воєнного стану робить український портрет унікальним порівняно з мирним часом у ЄС та США[73].

Кримінологічна характеристика особи кіберзлочинця в умовах воєнного стану в Україні є динамічною, багатошаровою системою, що поєднує високі технічні компетенції з корисливою або ідеологічною мотивацією.

Основні висновки:

– переважна більшість кіберзлочинців – чоловіки 18-35 років з технічною освітою або самоосвітою.

[72] Google Threat Analysis Group. Adversarial Threat Landscape Report 2025. – Mountain View : Google, 2025. URL : https://cloud.google.com/blog/topics/threat-intelligence/m-trends-2025.

[73] Microsoft. Digital Defense Report 2025. – Redmond : Microsoft, 2025. URL : https://www.microsoft.com/en-us/corporate-responsibility/cybersecurity/microsoft-digital-defense-report-2025/

– воєнний стан спричинив «старіння» профілю, зростання ідеологічної мотивації (до 15-22 %) та участь ветеранів ЗСУ (10-14 %).

– типологія стала складнішою: від скрипт-кідді до державних акторів і хактивістів.

– латентність – 75-85 %, рецидив – 25-32 % серед професіоналів.

– найефективніші заходи запобігання: підвищення кіберграмотності, психологічна реабілітація ветеранів, використання AI для профайлінгу, міжнародна співпраця.

Тільки комплексне використання кримінологічної характеристики дозволить Україні не лише знизити рівень кіберзлочинності в поствоєнний період, але й перетворити досвід протидії гібридним загрозам на конкурентну перевагу в сфері національної кібербезпеки.

Контрольні питання до розділу 1:

1. Що слід розуміти під кіберзлочинністю у широкому та вузькому значенні?
2. У чому полягає відмінність між поняттями «кіберзлочин», «комп'ютерний злочин» та «інформаційне правопорушення»?
3. Які основні ознаки характеризують кіберзлочинність як самостійний вид злочинності?
4. Що означає рівень кіберзлочинності та якими показниками він визначається?
5. Які тенденції динаміки кіберзлочинності в Україні простежуються у 2013–2025 роках?
6. Що таке структура кіберзлочинності та яке її кримінологічне значення?
7. Що слід розуміти під детермінацією кіберзлочинності?
8. Які основні причини та умови сприяють вчиненню кіберзлочинів?
9. Що включає кримінологічна характеристика особи кіберзлочинця?
10. Які соціально-демографічні ознаки притаманні особі кіберзлочинця?

Розділ 2
КРИМІНАЛЬНО-ПРАВОВІ ЗАХОДИ ЗАПОБІГАННЯ КІБЕРЗЛОЧИННОСТІ

2.1. Імплементація норм міжнародного права із запобігання кіберзлочинності у кримінальне законодавство України

Глобалізаційні процеси, які відбуваються у світі, швидкий розвиток комп'ютерних технологій впливають на набуття кіберзлочинністю транснаціонального характеру, що, своєю чергою, обумовлює необхідність адаптації національного кримінального законодавства до міжнародних стандартів.

Імплементація норм міжнародного права у сфері запобігання кіберзлочинності є важливим напрямом розвитку кримінального законодавства України. Вона сприяє підвищенню ефективності боротьби з кіберзлочинами та інтеграції України у міжнародний правовий простір.

Основним міжнародним нормативно-правовим актом, який визначає стандарти криміналізації суспільно небезпечних діянь, що вчиняються у кіберпросторі та/або з його використанням, а також засади міжнародної співпраці у цій сфері, є Конвенція про кіберзлочинність від 23.11.2001 р. (Будапештська конвенція).

Конвенція передбачає криміналізацію таких діянь, як:

- незаконний доступ до комп'ютерних даних і систем;
- нелегальне перехоплення комп'ютерних даних;
- втручання у комп'ютерні дані;
- втручання у комп'ютерну систему;
- зловживання пристроями;
- підробка, пов'язана з комп'ютерами;
- шахрайство, пов'язане з комп'ютерами;
- правопорушення, пов'язані з дитячою порнографією;
- правопорушення, повёязані з порушенням авторських та суміжних прав.

Конвенція про кіберзлочинність від 23.11.2001 р. ратифікована Україною 07.09.2005 р., набула чинності в Україні 01.07.2006 р.

Основні положення цієї Конвенції імплементовані у КК України.

Конвенція про кіберзлочинність	**Кримінальний кодекс України**
Стаття 2. *Незаконний доступ* Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисний доступ до цілої комп'ютерної системи або її частини без права на це. Сторона може вимагати, щоб таке правопорушення було вчинене шляхом порушення заходів безпеки з метою отримання комп'ютерних даних або з іншою недобросовісною метою, або по відношенню до комп'ютерної системи, поєднаної з іншою комп'ютерною системою.	***Стаття 361.*** *Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-*комунікаційних систем, електронних комунікаційних мереж **Стаття 361-2**. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації

Приклад судової практики за ч. 1 ст. 163, ч. 1 ст. 361 КК України

Обвинувачена ОСОБА_4, володіючи відповідними навичками роботи з електронно-обчислювальними машинами (*далі ЕОМ*) та спеціалізованим програмним забезпеченням, діючи умисно, посягаючи на право власності щодо комп'ютерної інформації, порядок використання ЕОМ та встановлене Конституцією України право на листування, шляхом несанкціонованого втручання в роботу ЕОМ, не маючи законних підстав, отримав доступ до листування потерпілого ОСОБА_6, чим порушив його Конституційне право на таємницю листування.

Наразі обвинувачена ОСОБА_4, 13.09.2014 р., знаходячись у приміщенні комп'ютерного клубу «БАЗУКА», умисно, з метою незаконного отримання персональної інформації про логіни облікових записів користувачів і паролі доступу до них, створених на веб сайтах в мережі Інтернет, завантажив з веб – ресурсу, доменне ім'я www.mipko.ru, інсталяційний пакет спеціалізованої комп'ютерної програми Mipko personal monitoring, яка призначена для реєстрації кожного натиснення користувачем ПК на клавіші клавіатури.

Продовжуючи свої протиправні дії, обвинувачена ОСОБА_7, інсталював завантажений пакет програми на жорсткий диск персонального комп'ютеру за № 03, що використовується у вказаному

комп'ютерному клубі «БАЗУКА», встановив налаштування, щоб дана програма про кожне натиснення користувачем комп'ютеру на клавішу клавіатури, створювала відповідні файли, та автоматично надсилала їх до завідомо створеної ним поштової електронної скриньки.

Таким чином, обвинувачена ОСОБА_4, незаконно отримав логіни облікових записів (*адреси електронних поштових скриньок*) ІНФОРМАЦІЯ_3, ІНФОРМАЦІЯ_4 і паролі доступу до них, які 12.10.2009 р. та 22.02.2013 р., відповідно, на підставі угоди із ТОВ «Діджітал Венчєз», обрав собі під час реєстрації авторизований користувач – ОСОБА_6, з метою використання функцій поштового серверу (*комп'ютеру*) даного товариства. Таким чином, обвинувачена ОСОБА_4, створюючи умови для вчинення подальших протиправних дій, отримав можливість змінювати режим роботи поштового серверу у свою користь та знайомитись із листуванням потерпілого ОСОБА_6.

Своїми умисними діями, які виразились у несанкціонованому втручанню в роботу електронно-обчислювальної техніки (комп'ютера), що призвело до блокування та витоку інформації, обвинувачена ОСОБА_4, вчинив злочин, передбачений ч. 1 ст. 361 КК України.

Крім цього, обвинувачена ОСОБА_4, 15.09.2014 р., знаходячись за місцем свого проживання, умисно, шляхом несанкціонованого втручання в роботу вузлового комп'ютера поштового сервісу ТОВ «Діджітал Венчєз», без згоди власника, не маючи законних підстав, отримав доступ до листів, які зберігалися в електронній поштовій скриньці за адресою: ІНФОРМАЦІЯ_3 та ознайомлювався із змістом листування потерпілого ОСОБА_6, яке здійснювалось через комп'ютер. Отримавши у такий спосіб інформацію, яку адресат не бажав доводити до відома інших осіб, обвинувачена ОСОБА_4 порушив гарантоване ст. 31 Конституції України право потерпілого на темницю листування. Своїми умисними діями, які виразились у порушенні таємниці листування, що передається через комп'ютер, обвинувачена ОСОБА_4, вчинив злочин, передбачений ч. 1 ст. 163 КК України[74].

[74] Кримінальна справа № 161/1717/15-к // Архів Луцького міськрайонного суду Волинської області.

Конвенція про кіберзлочинність	**Кримінальний кодекс України**
Стаття 3. *Нелегальне перехоплення* Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її	***Стаття 361.*** *Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж*
Конвенція про кіберзлочинність	**Кримінальний кодекс України**
внутрішнього законодавства за навмисне перехоплення технічними засобами, без права на це, передач комп'ютерних даних, які не є призначеними для публічного користування, які проводяться з, на або всередині комп'ютерної системи, включаючи електромагнітні випромінювання комп'ютерної системи, яка містить в собі такі комп'ютерні дані. Сторона може вимагати, щоб таке правопорушення було вчинене з недобросовісною метою або по відношенню до комп'ютерної системи, поєднаної з іншою комп'ютерною системою.	***Стаття 362***. *Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї*

Приклад судової практики за ч. 1 ст. 362 КК України

Товариство з обмеженою відповідальністю «Клініккардс» є розробником та адміністратором інформаційно – аналітичної онлайн – платформи Cliniccards, функціонал якої дозволяє клієнтам вказаної платформи записувати, обліковувати та зберігати інформацію про взаємодію з пацієнтами, оптимізувати робочі процеси, створювати та ілюструвати плани лікування, а також користуватись іншими доступними можливостями платформи.

Після прийняття на роботу лікарем стоматологом-хірургом до стоматологічної клініки SOCclinic у ОСОБА_3, який мав особистий обліковий запис ІНФОРМАЦІЯ_3 в інформаційній системі Cliniccards та який був обізнаним про умови використання вказаної системи, виник злочинний умисел, направлений на здійснення несанкціонованих змін інформації в автоматизованій системі «Cliniccards» шляхом внесення в

таку систему завідомо недостовірних відомостей щодо актів виконання робіт іншими лікарями стоматологічної клініки SOCclinic.

З метою реалізації зазначеного вище злочинного умислу, ОСОБА_3, перебуваючи на посаді лікаря стоматолога – хірурга, ортопеда стоматологічної клініки SOCclinic, та знаходячись на робочому місці за адресою: Дніпропетровська область, м. Дніпро, вул. Володимира Вернадського, 20, відповідно є особою, яка має право на доступ до електронної медичної інформаційної системи Cliniccards, умисно, усвідомлюючи суспільно небезпечний характер своїх дій, передбачаючи їх суспільно небезпечні наслідки і бажаючи їх настання, змінив в інформаційно-телекомунікаційній системі Cliniccards інформацію, шляхом доповнення її недостовірною інформацією про фіктивну взаємодію лікаря та пацієнта.

З цією метою, 06.10.2024 р. о 10:37 год., ОСОБА_3, перебуваючи на робочому місці, а саме за адресою: Дніпропетровська область, м. Дніпро, вул. Володимира Вернадського, 20, з використанням особистої електронної пошти та паролю здійснив вхід до системи «Cliniccards» в електронному робочому кабінеті лікаря, під своїм особистим електронним ключем, вчинив умисні дії щодо несанкціонованої зміни інформації в автоматизованій системі «Cliniccards», шляхом внесення в таку систему завідомо недостовірних відомостей щодо акту виконаних робіт, складеного лікарем клініки SOCclinic, лікарем стоматологом – хірургом ОСОБА_18, змінивши також інформацію із зазначенням виконавцем виконаних робіт себе. Таким чином, ОСОБА_3 несанкціоновано вніс відомості до автоматизованої системи Cliniccards.

Умисні дії ОСОБИ_3, які виразились у несанкціонованій зміні інформації, яка обробляється в автоматизованій системі, вчинені особою, яка має право доступу до неї, кваліфіковані за ч. 1 ст. 362 КК України[75].

[75] Кримінальна справа № 201/8123/25 // Архів Соборного районного суду м. Дніпра.

Конвенція про кіберзлочинність	**Кримінальний кодекс України**
Стаття 4. *Втручання у дані* 1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисне пошкодження, знищення, погіршення, зміну або приховування комп'ютерної інформації без права на це.	***Стаття 361.*** *Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж* ***Стаття 361-2****. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації*
	Стаття 362*. Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї*

Приклад судової практики за ч. 1 ст. 361-2 КК України

Обвинувачена ОСОБА_6, володіючи достатнім рівнем технічних та комп'ютерних знань, переслідуючи корисливу мету, діючи умисно, вчинив несанкціонований збут інформації з обмеженим доступом, яка зберігається в автоматизованих системах, створеної та захищеної відповідно до чинного законодавства за наступних обставин. Зокрема, орієнтовно в січні 2025 р., більш точного часу під час досудового розслідування не встановлено, однак не пізніше 31 січня 2025 р., ОСОБА_6, використовуючи сервіси із відкритих джерел інформації у Всесвітній мережі Інтернет, в порушення вимог Закону України «Про авторське право і суміжні права», Закону України «Про телекомунікації», Закону України «Про інформацію», Закону України «Про захист інформації в інформаційно – телекомунікаційних системах», не маючи договорів з правовласниками телерадіопрограм або їх дистриб'юторами про прийом і подальше розповсюдження кодованих телевізійних каналів

на території України, діючи умисно, усвідомлюючи протиправний характер своїх дій та їх наслідки, керуючись корисливими мотивами, перебуваючи за місцем свого проживання за адресою: АДРЕСА_1, вчинив несанкціонований збут інформації з обмеженим доступом, яка зберігається в автоматизованих системах, а саме: здійснив встановлення на медіа приставку «096», функціонал якої дозволяє за умови підключення до Всесвітньої мережі Інтернет здійснювати перегляд телевізійних каналів, що є інформацією з обмеженим доступом, яка зберігається в автоматизованих системах, правами на розповсюдження яких володіють ТОВ «Віжн медіа» та ТОВ «Старлайт діджитал», та продав громадянину ОСОБА_10 вказану медіа приставку за грошові кошти в сумі 700 (сімсот) гривень.

Таким чином, ОСОБА_6 вчинив кримінальне правопорушення, передбачене ч. 1 ст. 361-2 КК України, тобто несанкціонований збут інформації з обмеженим доступом, яка зберігається в автоматизованих системах, створеної та захищеної відповідно до чинного законодавства[76].

Конвенція про кіберзлочинність	**Кримінальний кодекс України**
Стаття 5. *Втручання у систему* Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисне серйозне перешкоджання функціонуванню комп'ютерної системи шляхом введення, передачі, пошкодження, знищення, погіршення, заміни або приховування комп'ютерних даних без права на це.	***Стаття 361.*** *Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж* ***Стаття 362***. *Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї*

Приклад судової практики за ч. 1 ст. 361 КК України

20.10.2024 р. приблизно о 09 год. 07 хв., більш точного часу досудовим розслідуванням не встановлено, ОСОБА_3, перебуваючи в приміщенні магазину «YATRAN», розташованого за адресою:

[76] Кримінальна справа № 599/1222/25 // Архів Зборівського районного суду Тернопільської області.

м. Кропивницький, вул. Ушакова, та маючи у володінні банківську картку АТ «ПриватБанк» № НОМЕР_2, яка належала ОСОБА_5, діючи умисно, з метою несанкціонованого втручання в роботу інформаційних (автоматизованих) мереж, усвідомлюючи суспільно-небезпечні наслідки у формі витоку інформації та бажаючи їх настання, без дозволу власника, за допомогою терміналу, який знаходився у зазначеному магазині, приклав до поверхні терміналу вказану банківську картку та сформував заявку від імені потерпілої ОСОБА_5 на розрахунок грошовими коштами із банківського рахунку НОМЕР_3, відкритого у банку АТ «ПриватБанк». Системою терміналу було сприйнято цю операцію як операцію, проведену ОСОБА_5, а ОСОБА_3 о 09 год. 07 хв. 20.10.2024 р. розрахувався через термінал, грошовими коштами в сумі 69 грн. 56 коп., здійснивши таким чином несанкціоноване втручання у роботу інформаційних (автоматизованих) мереж[77].

Конвенція про кіберзлочинність	**Кримінальний кодекс України**
Стаття 6. *Зловживання пристроями* 1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисне вчинення, без права на це: a. виготовлення, продажу, придбання для використання, розповсюдження або надання для використання іншим чином: i. пристроїв, включаючи комп'ютерні програми, створених або адаптованих, в першу чергу, з метою вчинення будь-якого зі злочинів, перерахованих у статтях 2 – 5 вище; ii. комп'ютерних паролів, кодів доступу або подібних даних, за допомогою яких можна здобути доступ до усієї або частини комп'ютерної системи з наміром використання її для вчинення будь-	***Стаття 361-1.*** *Створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут*

[77] Кримінальна справа № 404/10931/24 // Архів Фортечного районного суду м. Кропивницького.

Конвенція про кіберзлочинність	Кримінальний кодекс України
якого зі злочинів, перерахованих у статтях 2 – 5; та b. володіння предметом, перерахованим у підпунктах a.i або ii вище, з наміром його використання для вчинення будь- якого зі злочинів, перерахованих у статтях 2 – 5. Сторона може передбачити у законодавстві, що для встановлення кримінальної відповідальності необхідно володіти певною кількістю таких предметів.	

Приклад судової практики за ч. 1 ст. 361-1 КК України

У ОСОБА_4 у 2025 р. виник злочинний умисел, спрямований на протиправне створення з метою збуту, а також збут шкідливих програмних засобів, призначених для несанкціонованого втручання в роботу інформаційних (автоматизованих) мереж.

ОСОБА_4 з використанням облікового запису під нік-неймом «ОСОБА_6» за гіперпосиланням: «ІНФОРМАЦІЯ_2» здійснив публікацію в мережі Інтернет на форумі тіньової тематики «ІНФОРМАЦІЯ_2» за посиланням «ІНФОРМАЦІЯ_4», назва публікації «[.Exe] Ручной крипт от 30 $ | .NET & .NATIVE | bacteria .project», в якій пропонував свої послуги щодо здійснення «криптування файлових елементів» – створення шкідливих програмних засобів шляхом їх модифікації для уникнення ідентифікації та нейтралізації антивірусними програмними засобами.

Наразі за період часу з 15.28 год. по 17.25 год. 27.06.2025 р. ОСОБА_4, реалізовуючи свій злочинний умисел, спрямований на протиправне створення та збут шкідливого програмного засобу, призначеного для несанкціонованого втручання в роботу інформаційних (автоматизованих) систем, володіючи відповідними навичками у сфері використання програмного забезпечення, знаходячись за невстановленою адресою, усвідомлюючи суспільно небезпечний характер своїх дій, передбачаючи їх шкідливі наслідки та свідомо бажаючи настання таких наслідків, використовуючи власну комп’ютерну техніку, а саме свій персональний комп’ютер, створив шкідливий програмний засіб шляхом його модифікації, зокрема внесення змін до структури файлів для унеможливлення ідентифікації кінцевого виконуючого файлу антивірусним програмним забезпеченням, а саме

файлові елементи теки з назвою «2104.7z», який містить виконуючий файл з назвою «2104.exe», що визначено судовим експертом як шкідливе програмне забезпечення типу «Stealer», а саме «Raccoon Stealer» та файлові елементи теки з назвою «123.7z», який містить виконуючий файл з назвою «123.exe», що визначено судовим експертом як шкідливе програмне забезпечення типу «Stealer», а саме «Raccoon Stealer».

В подальшому 27.06.2025 р. о 17 год 26 хв. ОСОБА_4 з використанням облікового запису месенджеру «Telegram» під псевдонімом «ОСОБА_7», назва облікового запису «ОСОБА_8» у приватному листуванні з користувачем месенджеру під псевдонімом «ОСОБА_9» з мобільним номером телефону НОМЕР_1, здійснив збут шкідливого програмного засобу «123.exe», який містився у файловому елементі теки «123.7z» та шкідливого програмного засобу «2104.exe», який містився у файловому елементі теки «2104.7z», за що отримав які оплату грошові кошти в сумі 5549,59 гривень (у криптовалюті 129 USDT) на свій особистий крипто-гаманець «ІНФОРМАЦІЯ_5»[78].

Конвенція про кіберзлочинність	**Кримінальний кодекс України**
Стаття 7. *Підробка, пов'язана з комп'ютерами* Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисне вчинення, без права на це, введення, зміни, знищення або приховування комп'ютерних даних, яке призводить до створення недійсних даних з метою того, щоб вони вважались або відповідно до них проводилися б законні дії, як з дійсними, незалежно від того, можна чи ні такі дані прямо прочитати і зрозуміти. Сторона може вимагати наявність наміру обману або подібної нечесної поведінки для встановлення кримінальної відповідальності.	***Частина 4 статті 190****. Шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки*

[78] Кримінальна справа № 521/21166/25 // Архів Хаджибейського районного суду м. Одеси.

Приклад судової практики за ч. 4 ст. 190 КК України

На початку травня 2023 р. ОСОБА_5, маючи навички роботи із комп'ютерною технікою та Інтернет-ресурсами, за допомогою невстановленої комп'ютерної техніки, мобільних терміналів, підключених до всесвітньої мережі «Інтернет», через невстановлені інтернет-провайдери та мобільних операторів стільникового зв'язку у соціальній мережі «Facebook» розмістив рекламу щодо отримання грошової допомоги від держави, а саме «єДопомога», яка містила посилання на фішинговий сайт АТ КБ «ПриватБанк», створений ОСОБА_5 з метою заволодіння конфіденційною інформацією клієнтів банку та їх грошовими коштами шляхом вчинення незаконних операцій з використанням електронно-обчислювальної техніки.

09 травня 2023 р. близько 22:30 год. ОСОБА_6 за допомогою власного мобільного телефону, підключеного до всесвітньої мережі «Інтернет», знайшла у соціальній мережі «Facebook» розміщену ОСОБА_5 рекламу та, бажаючи отримати грошову допомогу, перейшла за посиланням на фішинговий сайт АТ КБ «ПриватБанк» та самостійно ввела повні дані власної банківської картки, емітованої АТ КБ «ПриватБанк» № НОМЕР_1, а саме номер банківської карти, зазначила CVV- код, логін та пароль від особистого кабінету «Приват24».

В подальшому ОСОБА_6, будучи введеною в оману щодо отримання грошової допомоги, підтвердила виконання операції, у зв'язку з чим шляхом незаконних операцій з використанням електронно-обчислювальної техніки 09.05.2023 р. о 22:37 год. з її банківської картки, емітованої АТ КБ «ПриватБанк» № НОМЕР_1 було перераховано грошові кошти в сумі 990 гривень на банківську картку, емітовану АТ КБ «ПриватБанк» № НОМЕР_2, яка належить ОСОБА_5[79].

Конвенція про кіберзлочинність	Кримінальний кодекс України
Стаття 8. *Шахрайство, пов'язане з комп'ютерами* Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисне вчинення,	***Частина 4 статті 190****. Шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки*

[79] Кримінальна справа № 401/512/24 // Архів Світловодського міськрайонного суду Кіровоградської області.

Конвенція про кіберзлочинність	Кримінальний кодекс України
без права на це, дій, що призводять до втрати майна іншої особи шляхом: a. будь-якого введення, зміни, знищення чи приховування комп'ютерних даних, b. будь-якого втручання у функціонування комп'ютерної системи, з шахрайською або нечесною метою набуття, без права на це, економічних переваг для себе чи іншої особи.	

Приклад судової практики за ч. 4 ст. 190 КК України

ОСОБА_3, діючи умисно, з корисливих мотивів, з метою власного збагачення, шляхом обману та здійснення незаконних операцій із використанням електронно – обчислювальної техніки, використовуючи акаунт у месенджері «Viber», під іменем «ОСОБА_3» розміщував оголошення про продаж дизельних генераторів, хоча їх у наявності не мав, заходів щодо їх закупівлі не проводив.

У подальшому ОСОБА_3 31.10.2022 р., отримавши заявку на придбання товару від потерпілої ОСОБА_6, не маючи можливості та намірів виконувати зобов'язання з продажу цього товару, обговорив із нею в месенджері «Viber» шляхом листування деталі та умови оплати і доставки дизельного генератора, надав банківські реквізити № НОМЕР_1, на яку ОСОБА_6 як передоплату за замовлений генератор 31.10.2022 р. перерахувала грошові кошти в сумі 11700 гривень, якими ОСОБА_3 заволодів та використав на власні потреби[80].

Конвенція про кіберзлочинність	Кримінальний кодекс України
Стаття 9. *Правопорушення, пов'язані з дитячою порнографією* 1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисне вчинення, без права на це, наступних дій:	***Частина 2 статті 301****. Збут неповнолітнім чи розповсюдження серед них творів, зображень або інших предметів порнографічного характеру* ***Стаття 301-1.*** *Одержання доступу до дитячої порнографії, її придбання, зберігання, ввезення, перевезення чи інше переміщення,*

[80] Кримінальна справа № 444/3821/23 // Архів Жовківського районного суду Львівської області.

Конвенція про кіберзлочинність	Кримінальний кодекс України
a. вироблення дитячої порнографії з метою її розповсюдження за допомогою комп'ютерних систем; b. пропонування або надання доступу до дитячої порнографії за допомогою комп'ютерних систем; c. розповсюдження або передача дитячої порнографії за допомогою комп'ютерних систем; d. здобуття дитячої порнографії за допомогою комп'ютерних систем для себе чи іншої особи;	*виготовлення, збут і розповсюдження* ***Стаття 301-2.*** *Проведення видовищного заходу сексуального характеру за участю неповнолітньої особи*
Конвенція про кіберзлочинність	**Кримінальний кодекс України**
e. володіння дитячою порнографією у комп'ютерній системі чи на комп'ютерному носії інформації.	

Приклад судової практики за ч. 1 ст. 301-1 КК України

01.01.2020 р. в 15 год. 06 хв., знаходячись за адресою свого мешкання: АДРЕСА_1, реалізуючи злочинний умисел, спрямований на умисне зберігання дитячої порнографії, без мети збуту чи розповсюдження, діючи умисно, всупереч суспільним відносинам, що складаються з приводу протидії розповсюдження дитячої порнографії, будучи підключеним до мережі Інтернет з IP-адресою інтернет-провайдеру «Київстар» – НОМЕР_1, за допомогою програми для обміну файлами «eMule», достовірно знаючи та усвідомлюючи, що він отримує доступ до файлів, які містять дитячу порнографію, умисно знайшов та завантажив у визначену ним папку на жорсткому диску файл з назвою «12/Firelols – Sasha2 (12Yo) 056 – Vibrator – Opens Pussy – Finger – Floor», який, відповідно висновку експерта № КСЕ-19/104-22/1143від 08.04.2022 р., належить до твору порнографічного характеру, що містить дитячу порнографію, та почав його зберігати без мети збуту чи розповсюдження, до тих пір, доки портативний персональний комп'ютер (ноутбук) у нього не було вилучено працівниками поліції 08.09.2021 р. в ході проведення санкціонованого обшуку у період часу з 07 год. 10 хв. до 08 год. 26 хв. за місцем його проживання[81].

[81] Кримінальна справа № 201/10744/22 // Архів Жовтневого районного суду м. Дніпропетровська.

Приклад судової практики за ч. 1 ст. 301-2 КК України

ОСОБА_5 з метою створення умов для проведення видовищних заходів сексуального характеру орендувала у ТОВ «МП Юлія» офісне приміщення за адресою: м. Вінниця, вул. Театральна, 1, про що уклала відповідний договір, та уклала договір про надання послуг доступу до мережі Інтернет через провайдер ТОВ ТК «ВІНТЕЛЕПОРТ» у вказаному приміщені, після чого облаштувала його меблями та комп'ютерною технікою і тим самим підготовила приміщення для проведення видовищних заходів сексуального характеру за участю дівчат, зокрема, неповнолітніх, з їх подальшою трансляцією в режимі реального часу на сайтах всесвітньої мережі Інтернет за грошову винагороду.

В подальшому ОСОБА_5, в порушення ст. 7 Закону України «Про захист суспільної моралі» від 20.11.2003 р., відповідно до якого з метою захисту морального та фізичного життя дітей забороняється організація та проведення видовищних заходів сексуального чи еротичного характеру, використання образів дітей у будь-якій формі в продукції сексуального чи еротичного характеру і проведенні видовищних заходів сексуального чи еротичного характеру, надання доступу до продукції, що містить дитячу порнографію, а також норм та положень, які прямо чи опосередковано стосуються прав дитини, захисту їх від сексуальної експлуатації та сексуального насильства, що були ухвалені резолюцією Генеральної асамблеї ООН від 20.11.1998 р. і набули чинності 02.09.1990 р., Конвенції Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства, ратифікованої 20.06.2020 р. (Ланцаротської конвенції), через соціальні мережі Інтернет та мобільні додатки такі як «Телеграм» підшукувала та підбирала дівчат для участі у видовищних заходах сексуального характеру, пропонуючи роботу в офісі у якості «веб-моделей». При особистій зустрічі остання доводила до їх відома принципи роботи, а саме спілкування з клієнтами з України та іноземних держав на сексуальні теми, в умовах реального часу із застосуванням веб-камер.

Надалі ОСОБА_5, отримавши від дівчини добровільну згоду на участь у видовищних заходах сексуального характеру, усвідомлюючи, що реєстрація у мережі Інтернет на веб-сайтах, де здійснюється спілкування між чоловіками та жінками, можлива лише повнолітньої особи, з метою приховання віку останніх, здійснювала виготовлення фальшивого паспорта громадянина України (ID – картки), схожого на справжній, в якому змінювала рік народження особи і тим самим

організовувала видовищні заходи сексуального характеру за участю неповнолітніх осіб на сайті «coomeet.com».

В подальшому «моделі» приходили у створений «Веб-інтим-колл центр», що за адресою: м. Вінниця, вул. Театральна, 1, де, використовуючи інформаційно-телекомунікаційні системи – ноутбуки, обладнані веб-камерами, авторизувалися на вищезазначених сайтах і в режимі он-лайн спілкувалися з користувачами цих сайтів, на їх побажання оголялися, здійснювали маніпуляції зі статевими органами. За вчинення вказаних дій на відповідні акаунти неповнолітніх дівчат нараховувались грошові кошти, доступ до яких мала лише ОСОБА_5, яка після цього здійснювала розрахунок з моделями особисто шляхом надання готівки або грошового переказу на картку[82].

Конвенція про кіберзлочинність	**Кримінальний кодекс України**
Стаття 10. *Правопорушення, пов'язані з порушенням авторських та суміжних прав* 1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за порушення авторських прав, як це визначено законодавством такої Сторони відповідно до її зобов'язань за Паризьким Актом від 24 липня 1971 р. щодо Бернської Конвенції про захист літературних та художніх творів, Угодою про торгівельні аспекти прав інтелектуальної власності і Угодою ВОІВ про авторське право, за винятком будь-яких моральних прав, які надаються такими Конвенціями, у випадку, коли такі дії вчинені свідомо, у комерційних розмірах і за допомогою комп'ютерних систем.	***Стаття 176.*** *Порушення авторського права і суміжних прав*

[82] Кримінальна справа № 127/28630/22 // Архів Вінницького міського суду Вінницької області.

Приклад судової практики за ч. 1 ст. 176 КК України

Обвинувачена ОСОБА_3 в приміщенні магазину «Інстал», який розташований по вул. Громницького, 9 у м. Тернопіль, в порушення авторських прав, без відома та згоди корпорації «Microsoft» (США), а також її офіційного представника на території України – адвоката ОСОБА_5, незаконно відтворив та розповсюдив комп'ютерні програми, авторські права на які належать вказаній корпорації, заподіявши такими діями корпорації «Microsoft» шкоду у значних розмірах. Корпорація «Microsoft» (США) є юридичною особою, яка зареєстрована і діє відповідно до законодавства штату Вашингтон США, є власником виключних авторських прав інтелектуальної власності на всі комп'ютерні програми, які були випущені вказаною корпорацією. Реєстрація всіх комп'ютерних програм здійснена відповідно до законодавства США про авторське право в канцелярії США з питань охорони авторського права. Комп'ютерні програми, країною походження яких є США, підлягають охороні в Україні згідно зі ст. 5 Бернської конвенції про охорону літературних і художніх творів (в редакції Паризького Акту від 24 липня 1971 р. зі змінами від 02 жовтня 1979 року). Відповідно до положень якої щодо творів, стосовно яких авторам надається охорона на підставі Бернської Конвенції, автори користуються в державах-учасницях цієї Конвенції такими ж правами, які надаються відповідними законами цих країн своїм громадянам. У відповідності з ч. (6) ст. 2 Бернської Конвенції охороною в усіх держава-учасницях цієї Конвенції користуються твори, перелічені у ст. 2 Бернської Конвенції, і, зокрема, «літературні і художні твори» (ч. (1) ст. 2 Бернської Конвенції). Комп'ютерні програми охороняються в Україні як літературні твори на підставі ч. 4 ст. 433 ЦК України, ст. 18 Закону України «Про авторське право і суміжні права», ст. 4 Договору Всесвітньої організації інтелектуальної власності про авторське право. Згідно ст. 437 ЦК України, авторське право виникає з моменту створення твору. Згідно з ч. 2 ст. 433 ЦК України, твори є об'єктами авторського права без виконання будь-яких формальностей щодо них та незалежно від їх завершеності, призначення, цінності тощо, а також способу чи форми їх вираження. Згідно з ч.1 ст. 440 ЦК України, суб'єкту авторського права належить виключне право дозволяти використання твору. Крім того, згідно ст. 443 ЦК України, використання твору здійснюється лише за згодою автора. Згідно ст. 1107 ЦК України, розпоряджання майновими правами інтелектуальної власності на твір здійснюється суб'єктом авторського права на підставі відповідних договорів, у тому числі ліцензії на використання твору та ліцензійного договору. Всупереч

вищевказаному порядку використання творів авторського права, ОСОБА_3 20 листопада 2014 р. о 16 год. 17 хв. та 21 листопада 2014 р. о 10 год. 47 хв., перебуваючи в приміщенні магазину «Інстал», що розташований в м. Тернопіль на вул. Громницького, 9, незаконно відтворив на жорсткі диски двох системних блоків комп'ютерів, та 25 листопада 2014 р. о 14 год. в приміщені вказаного магазину незаконно розповсюдив шляхом продажу ОСОБА_6 два примірники операційної системи «Microsoft Windows 7 Ultimate» вартістю – 4623,40 гривень за 1 примірник, на загальну суму 9246,80 гривень, які містять ознаки контрафактності, права на відтворення та розповсюдження на які належали корпорації «Microsoft» (США), чим завдав збитків корпорації «Microsoft» (США) на вказану суму[83].

Конвенція про кіберзлочинність	**Кримінальний кодекс України**
Стаття 10. *Правопорушення, пов'язані з порушенням авторських та суміжних прав* 2. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за порушення суміжних прав, як це визначено законодавством такої Сторони відповідно до її зобов'язань за Міжнародною Конвенцією про захист виконавців, виробників фонограм і організацій мовлення (Римська конвенція), Угодою про торгівельні аспекти прав інтелектуальної власності і Угодою ВОІВ про виконання і фонограми, за винятком будь-яких моральних прав, які надаються такими Конвенціями, у випадку, коли такі дії вчинені свідомо, у комерційних розмірах і за допомогою комп'ютерних систем.	***Стаття 176.*** *Порушення авторського права і суміжних прав*

[83] Кримінальна справа №607/1658/15-к // Архів Тернопільського міськрайонного суду Тернопільської області.

Приклад судової практики за ч. 2 ст. 176 КК України

14 березня 2025 р. об 11 год. 39 хв. ОСОБА_6, перебуваючи на території АЗС «Авіас Плюс» за адресою: Тернопільська область, Тернопільський район, місто Зборів, вулиця Тернопільська, 48, вчинив несанкціонований збут інформації з обмеженим доступом, яка зберігається в автоматизованих системах, а саме: продав ОСОБА_12 за грошові кошти у сумі 1250 гривень медіа приставку ««G96max A13», на якій попередньо встановив функціонал, який дозволяє за умови підключення до Всесвітньої мережі Інтернет здійснювати перегляд телевізійних каналів: «1+1», «2+2», «ТЕТ», «Уніан», «ICTV», «MI», «M2», що призвело до незаконної ретрансляції вказаних каналів.

Внаслідок вказаних злочинних дій ОСОБА_6, у зв'язку із незаконним використанням шляхом розповсюдження програм мовлення телеканалів «1+1», «2+2», «ТЕТ», «Уніан», «ICTV», «MI», «M2, порушив суміжні права ТОВ «ВІЖН МЕДІА» та ТОВ «СТАРЛАЙТ ДІДЖИТАЛ» і такими діями, з урахуванням Національного стандарту № 4 «Оцінка майнових прав інтелектуальної власності» (Постанова КМУ № 1185), спричинив ТОВ «ВІЖН МЕДІА» майнову шкоду в сумі 589 420,00 гривень та спричинив «ТОВ «СТАРЛАЙТ ДІДЖИТАЛ» майнову шкоду у сумі 269 880,00 гривень.

Таким чином, ОСОБА_6 вчинив кримінальне правопорушення, передбачене ч. 2 ст. 176 КК України, тобто незаконне розповсюдження програм мовлення, яке завдало матеріальної шкоди у великому розмірі[84].

2.2. Кримінальна відповідальність за кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (ст.ст. 361-363-1 КК України)

Поняття та місце кіберзалежних кримінальних правопорушень у системі кримінального права

Стрімкий розвиток інформаційного суспільства та процесів цифровізації зумовив появу нових видів суспільно небезпечних діянь, які безпосередньо посягають на інформаційну безпеку держави, суспільства та окремої особи. У чинному кримінальному законодавстві України вказана група кримінальних правопорушень систематизована у Розділі

[84] Кримінальна справа № 599/1222/25 // Архів Зборівського районного суду Тернопільської області.

XVI Особливої частини Кримінального кодексу України: «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку».

Аналіз сучасного стану кримінально-правової доктрини дає підстави стверджувати, що кримінальні правопорушення у сфері обігу цифрової інформації та функціонування інформаційно-телекомунікаційних технологій не є тотожними всім кримінальним правопорушенням, механізм вчинення яких передбачає використання комп'ютерної техніки. У науці кримінального права сформувався обґрунтований поділ суспільно небезпечних діянь у кіберпросторі на дві базові категорії:

1. **Кіберутворювальні (кібернетичні або кібердопоміжні) кримінальні правопорушення** – це традиційні суспільно небезпечні діяння (наприклад, шахрайство, крадіжка, вимагання, порушення авторських прав), які внаслідок еволюції інформаційно-телекомунікаційних технологій перейшли у віртуальний простір або були трансформовані під нові умови вчинення. У таких складах цифрові пристрої виступають виключно як знаряддя чи засіб вчинення кримінального правопорушення, проте основним об'єктом кримінально-правової охорони залишаються майнові відносини, авторські права тощо.

2. **Кіберзалежні кримінальні правопорушення** – це суспільно небезпечні діяння, які існують виключно завдяки наявності кіберпростору та інформаційно-телекомунікаційних систем. Основним предметом посягання тут виступає безпосередньо цифрова інформація або самі цифрові технології, системи та мережі. Вчинення цих правопорушень спрямоване на порушення базових властивостей інформації: її конфіденційності, цілісності чи доступності.

Саме кіберзалежні кримінальні правопорушення становлять зміст Розділу XVI Особливої частини КК України. Відповідні норми були імплементовані в національне законодавство на виконання зобов'язань за Конвенцією Ради Європи про кіберзлочинність (Будапештською конвенцією), зокрема її Розділу II, що регламентує відповідальність за правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем.

Юридичний аналіз елементів складів кримінальних правопорушень розділу XVI КК України

Для правильної кваліфікації діянь та розуміння їхньої правової природи необхідним є комплексний розгляд усіх елементів складу кримінального правопорушення, притаманних аналізованій групі.

Об'єкт кримінального правопорушення

– *Родовий об'єкт:* суспільні відносини в інформаційному середовищі, що забезпечують стан захищеності (безпеки) цифрової інформації (її конфіденційність, цілісність, доступність), а також нормальний, регламентований законодавством порядок експлуатації інформаційно-телекомунікаційних систем, мереж та цифрових пристроїв.

– *Безпосередній об'єкт:* диференціюється залежно від конкретної норми. Наприклад, для ст. 361 КК України це суспільні відносини щодо безпечної та безперебійної роботи інформаційно-комунікаційних систем; для ст. 361-2 КК України – суспільні відносини щодо збереження та легального обігу інформації з обмеженим доступом.

– *Предмет кримінального правопорушення:* альтернативно виступають цифрова інформація (дані, що обробляються в системах) та/або апаратні чи програмно-апаратні комплекси (цифрові пристрої, автоматизовані системи, мережі).

Об'єктивна сторона Об'єктивна сторона кіберзалежних кримінальних правопорушень характеризується активними діями (несанкціоноване втручання, створення шкідливого програмного забезпечення, збут інформації) або, у виняткових випадках, бездіяльністю (невиконання правил захисту інформації за ст. 363 КК України). Більшість складів цього розділу є матеріальними, тобто вимагають обов'язкового настання суспільно небезпечних наслідків: витоку, втрати, підробки, блокування інформації, спотворення процесу обробки даних або порушення встановленого порядку її маршрутизації. Обов'язковою ознакою є наявність причинного зв'язку між діянням (наприклад, хакерською атакою або порушенням правил експлуатації) та вказаними технологічними наслідками.

Суб'єкт кримінального правопорушення Суб'єкт кримінальних правопорушень даної категорії диференційований. У більшості випадків (ст.ст. 361, 361-1, 361-2, 363-1 КК України) суб'єктом є загальний – фізична осудна особа, яка досягла 16-річного віку. Проте норми ст. 362 та ст. 363 КК України передбачають наявність *спеціального суб'єкта*. У

ст. 362 КК України це особа, яка має легальний доступ до інформації або систем (інсайдер), а у ст. 363 КК України – особа, яка несе юридичну відповідальність за експлуатацію систем або забезпечення захисту інформації (наприклад, системний адміністратор, керівник відділу ІТ-безпеки).

Суб'єктивна сторона Суб'єктивна сторона кіберзалежних правопорушень переважно характеризується умисною формою вини (прямий або непрямий умисел). Особа усвідомлює, що здійснює несанкціоноване втручання або поширює шкідливе ПЗ, передбачає наслідки у вигляді спотворення даних чи блокування систем і бажає або свідомо припускає їх настання. Винятком є порушення правил експлуатації систем (ст. 363 КК України), де стосовно суспільно небезпечних наслідків можлива необережна форма вини (кримінально-протиправна самовпевненість або кримінально-протиправна недбалість).

Термінологічні проблеми законодавчого регулювання та шляхи їх вирішення

Доктринальним і практичним викликом у контексті застосування Розділу XVI КК України є невідповідність законодавчої термінології сучасному етапу розвитку інформаційних технологій. У назві розділу та диспозиціях статей базовим є поняття «електронно-обчислювальна машина (комп'ютер)».

Історично ця дефініція походить із нормативних актів кінця 1990-х років, коли комп'ютерна техніка асоціювалася виключно зі стаціонарними пристроями. У сучасних реаліях обробка, зберігання та передавання цифрової інформації здійснюється за допомогою розгалуженої екосистеми пристроїв: смартфонів, планшетів, смарт-годинників, серверного обладнання хмарних сховищ, а також пристроїв Інтернету речей (IoT). Технічно та юридично підвести весь цей спектр обладнання під архаїчне визначення «ЕОМ» є вкрай складним, що створює штучні перепони під час кваліфікації.

З огляду на це, науково обґрунтованою є пропозиція щодо вилучення терміна «електронно-обчислювальні машини (комп'ютери)» з кримінального закону та його заміни на універсальну категорію **«цифрові пристрої»**. *Цифрові пристрої* — це інформаційно-телекомунікаційні засоби, призначені для оброблення, передавання, розподілу та зберігання інформації в цифровій формі.

Крім того, законодавцю доцільно відійти від громіздкої конструкції

«автоматизовані системи, комп'ютерні мережі чи мережі електрозв'язку», замінивши її узагальнювальним поняттям **«інформаційно-телекомунікаційні технології, системи та мережі»**. Це дозволить охопити всі можливі середовища обігу інформації, включаючи 5G-мережі та гібридні хмарні платформи.

Також потребує модернізації поняття «комп'ютерна інформація». З технічної точки зору більш коректним є використання терміна **«цифрова інформація»**, під якою слід розуміти сукупність даних та програмних компонентів, що обробляються, передаються та зберігаються в інформаційно-телекомунікаційних системах, що включає бази даних, стрімінгові потоки та контент, згенерований штучним інтелектом.

Система кіберзалежних кримінальних правопорушень: класифікація та матеріали правозастосовної практики

Система кіберзалежних кримінальних правопорушень в Україні представлена шістьма основними складами. Для глибокого розуміння механізму їх вчинення наведемо розгорнуті приклади з урахуванням специфіки суб'єктного складу та наслідків.

1. Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (ст. 361 КК України). *Практичний кейс:* Зловмисник, використовуючи спеціалізоване програмне забезпечення, здійснив підбір паролів (brute-force) та отримав несанкціонований доступ до панелі адміністратора вебсерверу державного органу. Після проникнення він умисно змінив контент головної сторінки (дефейсмент) та заблокував доступ легітимних користувачів до електронних послуг на 12 годин. Діяння утворюють об'єктивну сторону ст. 361 КК України, оскільки мало місце зовнішнє проникнення особи, яка не мала права доступу, що призвело до підробки інформації та блокування системи.

2. Створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст. 361-1 КК України). *Практичний кейс:* Організована група розробила модифікацію вірусу-вимагача (ransomware). Вони створили мережу фішингових сайтів, через які розповсюджували цей шкідливий код під виглядом оновлень для операційної системи. Код шифрував жорсткі диски потерпілих, унеможливлюючи доступ до даних без введення ключа дешифрування.

Сам факт створення та поширення такого коду утворює закінчений склад кримінального правопорушення за ст. 361-1 КК України незалежно від того, чи сплатили жертви викуп.

3. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст. 361-2 КК України). *Практичний кейс:* Колишній співробітник комерційної установи, перед звільненням скопіювавши базу даних клієнтів (яка становить комерційну таємницю), розмістив оголошення на закритому хакерському форумі (DarkNet) про її продаж. Після отримання оплати у криптовалюті він передав архів із даними покупцю. Дії кваліфікуються за ст. 361-2 КК України, оскільки об'єктом посягання є встановлений порядок обігу цифрової інформації з обмеженим доступом.

4. Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (ст. 362 КК України). *Практичний кейс:* Керівник підрозділу фінансово-економічної безпеки великого промислового підприємства у Сумському регіоні, маючи авторизований доступ до внутрішньої корпоративної ERP-системи, з мотивів особистої помсти після конфлікту з керівництвом умисно видалив критичні файли щодо проведених фінансових аудитів контрагентів за останні три роки. Хоча особа мала законний доступ до системи, вона перевищила свої повноваження щодо управління даними. Кваліфікація здійснюється за ст. 362 КК України як знищення цифрової інформації спеціальним суб'єктом.

5. Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється (ст. 363 КК України). *Практичний кейс:* Відповідальний інженер з інформаційної безпеки медичного закладу, порушуючи затверджену інструкцію із захисту інформації, не здійснив своєчасне оновлення антивірусних баз та не заблокував використання зовнішніх флеш-накопичувачів на робочих станціях лікарів. Внаслідок цієї бездіяльності система була інфікована вірусом через підключення лікарем особистого носія, що призвело до знищення електронних медичних карток пацієнтів та зупинки роботи

закладу. Суб'єктивна сторона стосовно наслідків характеризується злочинною недбалістю.

6. Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (ст. 363-1 КК України). *Практичний кейс:* У 2025 році під час проведення вступної кампанії до вищого навчального закладу зловмисники за допомогою ботнету організували масовану DDoS-атаку (Distributed Denial of Service) на сервери приймальної комісії. Генерація мільйонів фейкових запитів за секунду призвела до вичерпання ресурсів сервера та неможливості подачі електронних заяв абітурієнтами протягом 48 годин. Дії підпадають під ст. 363-1 КК України як умисне перешкоджання роботі системи шляхом масового розповсюдження повідомлень.

Кримінально-правова характеристика несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (ст. 361 КК України)

Об'єкт кримінального правопорушення

Правильне визначення об'єкта є фундаментом для з'ясування соціальної сутності та ступеня суспільної небезпеки діяння, передбаченого статтею 361 КК України.

– **Основний безпосередній об'єкт** – це встановлений законодавством порядок експлуатації та нормального функціонування інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем та електронних комунікаційних мереж, а також суспільні відносини щодо забезпечення базових властивостей цифрової інформації (її конфіденційності, цілісності та доступності).

– **Додатковий факультативний об'єкт** може варіюватися залежно від сфери, на яку спрямоване посягання. Ним можуть виступати: право власності на інформацію, комерційна чи банківська таємниця, недоторканність приватного життя громадян, нормальна діяльність підприємств, установ та організацій, а також інтереси національної безпеки держави. Наприклад, цілеспрямоване втручання в медичну інформаційну систему одночасно посягає на порядок функціонування системи та на лікарську таємницю пацієнтів, а атаки на енергетичну

інфраструктуру — на економічну та національну безпеку.

Об’єктивна сторона кримінального правопорушення: діяння та наслідки

Об’єктивна сторона кримінального правопорушення, передбаченого ст. 361 КК України, має складну структуру і за законодавчою конструкцією є матеріальним складом. Вона включає три обов'язкові елементи:

1. Суспільно небезпечне діяння у формі несанкціонованого втручання.
2. Суспільно небезпечні наслідки (один з альтернативно передбачених у законі).
3. Причиново-наслідковий зв’язок між втручанням та настанням вказаних наслідків.

Ключовим елементом є *активна дія – несанкціоноване втручання*. Відповідно до доктринальних підходів, під цим поняттям слід розуміти отримання можливості для ознайомлення та (або) використання цифрової інформації, яка міститься в системі, шляхом проникнення особою, яка не має права доступу, або вчинення таких дій поза дозволом власника. Механізм втручання може полягати у подоланні логічного захисту (злам паролів, використання експлойтів до вразливостей програмного забезпечення) або неправомірному використанні викрадених автентифікаційних даних.

Фактично, несанкціоноване втручання свідчить про порушення установленого власником чи державою режиму доступу до системи. Для наявності закінченого складу кримінального правопорушення це втручання повинно потягнути за собою хоча б один із таких наслідків:

- **Витік інформації:** Стан, за якого цифрова інформація виходить з-під контролю власника і стає відомою чи доступною особам, які не мають права доступу до неї.
- *Практичний кейс:* У 2024 році суди розглядали низку проваджень щодо фішингових атак. Наприклад, вироком Дзержинського районного суду м. Кривого Рогу від 13.08.2024 було встановлено, що особа, створивши фішингове посилання, здійснила несанкціоноване втручання у веббанкінг потерпілих. Внаслідок подолання системи логічного захисту відбувся витік автентифікаційних даних, що дозволило зловмиснику заволодіти коштами (діяння кваліфіковано за сукупністю ст. 361 та ст. 190 КК України). Слід розмежовувати *зчитування* (як спосіб вчинення дії) та *витік* (як пасивний наслідок, коли конфіденційність

порушено).

– **Блокування цифрової інформації:** Дії, внаслідок яких тимчасово або постійно унеможливлюється доступ законних користувачів до інформації чи систем.

– *Практичний кейс:* Масштабна кібератака на телекомунікаційного оператора «Київстар» 12 грудня 2023 року. Зловмисники (ймовірно, пов'язані зі спецслужбами РФ) здійснили несанкціоноване втручання та перебували в системі протягом кількох місяців. Наслідком атаки стало повне блокування доступу до послуг зв’язку та інтернету для понад 24 мільйонів абонентів, паралізація роботи банківських терміналів та систем оповіщення про повітряну тривогу. Це класичний приклад блокування інформації з особливо тяжкими наслідками.

– **Знищення цифрової інформації:** Незворотна дія, внаслідок якої дані в системі перестають існувати фізично або логічно, і їх відновлення звичайними засобами системи неможливе.

– *Практичний кейс:* Використання шкідливого програмного забезпечення класу Wiper (наприклад, WhisperGate або HermeticWiper) проти українських державних реєстрів у 2022 році. На відміну від програм-вимагачів (які шифрують дані з метою блокування), метою Wiper є безповоротне стирання файлової системи та знищення даних без можливості їх відновлення.

– **Модифікація та підробка:** Внесення змін у дані без згоди власника, що призводить до зміни їхнього змісту (модифікація) або зміни авторства та реквізитів з метою видати їх за автентичні (підробка).

– **Спотворення процесу обробки інформації та порушення маршрутизації:** Зміна алгоритмів та послідовності виконання операцій з інформацією або протиправна зміна адресата передачі даних.

– *Практичний кейс:* Особа, маючи базові технічні навички, встановила супутникову антену та програмно модифікований роутер для несанкціонованого декодування зашифрованого супутникового сигналу з метою безкоштовного перегляду платних телеканалів. Судова практика кваліфікує такі дії саме як спотворення процесу обробки інформації (маршрутизації сигналу), оскільки втручання змінює логіку роботи захищеної системи мовника.

Проблемні питання кваліфікації: формальний чи матеріальний склад?

Одне з найбільш гострих та дискусійних питань у теорії кримінального права та правозастосовній практиці стосується

конструкції складу ст. 361 КК України. З буквального тлумачення диспозиції випливає, що відповідальність настає за «несанкціоноване втручання... *що призвело до* витоку, втрати, підробки, блокування...». Тобто законодавець сконструював *матеріальний склад*.

Однак, з доктринальної точки зору, сама сутність «втручання» (тобто факт нелегального проникнення у захищену систему) вже становить значну суспільну небезпеку, оскільки руйнує режим конфіденційності та створює загрозу безпеці даних, навіть якщо зловмисник не встиг або не захотів нічого знищити чи скопіювати.

На практиці виникають колізії, коли суди змушені штучно «знаходити» наслідки для притягнення до відповідальності. Наприклад, у справі про злам акаунту на ігровій платформі Steam (вирок Деснянського районного суду м. Чернігова, 2019 рік) особа здійснила несанкціонований доступ та змінила пароль. Суд визнав особу винною за ч. 1 ст. 361 КК України, кваліфікувавши це як просте втручання, хоча фактично наслідок у вигляді «блокування інформації» для законного власника був наявний, що об’єктивно більше відповідає кваліфікованим частинам статті. З іншого боку, вироком Стрийського міськрайонного суду Львівської області від 22.04.2024 року особі було призначено 10 років позбавлення волі за ч. 5 ст. 361 КК України за втручання саме під час дії воєнного стану, що спричинило тяжкі наслідки.

Для усунення цих суперечностей та гармонізації національного законодавства з європейськими стандартами доцільним є реформування ст. 361 КК України шляхом чіткого розмежування формального та матеріального складів. Відповідно до концепції кримінально-правової охорони кіберпростору, пропонується така градація:

1. *Частина 1 (Формальний склад):* Криміналізувати сам факт умисного несанкціонованого втручання (неправомірного доступу) до інформаційно-телекомунікаційних систем чи цифрових пристроїв незалежно від настання наслідків. Сам факт подолання системи захисту має бути караним.

2. *Частина 2 та 3 (Матеріальні склади):* Встановити суворішу відповідальність за втручання, якщо воно призвело до витоку, перехоплення, копіювання, спотворення або модифікації цифрової інформації.

3. *Частина 4 (Особливо кваліфікований склад):* Встановити найбільш сувору відповідальність за дії, що призвели до блокування, знищення інформації або виведення з ладу критичної інфраструктури.

Такий підхід дозволить справедливо та диференційовано притягувати до відповідальності як осіб, що здійснюють злам із «дослідницького інтересу» без завдання прямої шкоди, так і професійних правопорушників, чиї дії завдають масштабних збитків економіці та безпеці.

Суб'єкт кримінального правопорушення

Суб'єкт кримінального правопорушення за ст. 361 КК України є загальним. Це фізична осудна особа, яка на момент вчинення діяння досягла 16-річного віку (відповідно до положень ст. 22 КК України).

Важливо наголосити, що для наявності складу правопорушення не вимагається, щоб суб'єкт був професійним фахівцем у галузі ІТ, програмістом чи мав специфічні технічні навички. Враховуючи поширення концепції «Cybercrime-as-a-Service» (кіберзлочинність як послуга), особа може вчинити несанкціоноване втручання, використовуючи придбані в тіньовому сегменті інтернету готові скрипти, орендовані ботнети або методи соціальної інженерії (фішинг), зовсім не розбираючись у програмному коді.

Суб'єктивна сторона кримінального правопорушення

Суб'єктивна сторона характеризується умисною формою вини.

– **Форма вини:** Стосовно суспільно небезпечного діяння (несанкціонованого втручання) особа завжди діє з прямим умислом. Вона чітко усвідомлює суспільно небезпечний характер своїх дій (розуміє, що не має права доступу і порушує систему захисту). Щодо наслідків (витік, знищення, блокування) умисел може бути як прямим (особа бажає настання цих наслідків, наприклад, при знищенні бази даних конкурента), так і непрямим (особі байдуже до наслідків, але вона свідомо припускає їх настання під час зламу).

– **Мотив і мета:** Не є обов'язковими конструктивними ознаками основного складу кримінального правопорушення, проте їх встановлення є вкрай важливим для індивідуалізації покарання. Мотиви можуть бути корисливими (викрадення інформації для подальшого продажу), хуліганськими (злам заради розваги або самоствердження), помстою колишньому роботодавцю. У сучасних реаліях часто зустрічаються політичні мотиви або мотиви сприяння державі-агресору (хактівізм, кібершпигунство, кібертероризм у межах гібридної війни). Метою найчастіше є отримання контролю над цифровими пристроями, незаконне збагачення або дестабілізація роботи систем.

Кримінально-правова характеристика створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів (ст. 361-1 КК України)

Стаття 361-1 КК України відіграє превентивну роль і спрямована на боротьбу з так званим «інструментарієм» кіберзлочинності. Окремим масивом у межах кіберзалежних кримінальних правопорушень є діяння, пов'язані саме з розробкою, підготовкою та обігом засобів, призначених для несанкціонованого втручання. Ця стаття криміналізує не сам факт втручання (як ст. 361 КК України), а створення передумов для нього.

Актуальність цієї норми підтверджується стрімким розвитком тіньового ринку «Кіберзлочинність як послуга» (Cybercrime-as-a-Service) та інтеграцією алгоритмів штучного інтелекту у механізми кібератак, що дозволяє автоматизувати пошук вразливостей та генерувати шкідливий код.

Предмет кримінального правопорушення: програмні та технічні засоби

Безпосереднім об'єктом цього кримінального правопорушення є встановлений законодавством порядок створення, використання та обігу програмних і технічних засобів, що гарантує інформаційну безпеку. Предмет посягання поділяється на дві самостійні категорії, розмежування яких базується на їхній фізичній (матеріальній) природі:

1. **Шкідливе програмне забезпечення (ШПЗ)** — це набір інструкцій у вигляді програмного коду, який циркулює виключно у кіберпросторі й не має матеріального вираження. Воно спеціально створене або модифіковане для несанкціонованого втручання в роботу інформаційно-телекомунікаційних систем.

2. **Шкідливі технічні засоби (ШТЗ)** — це предмети матеріального світу (апаратні комплекси, пристрої, мікросхеми), які з огляду на свої конструктивні особливості або спеціальну модифікацію призначені для подолання систем логічного чи фізичного захисту інформації.

Доктринальна ремарка: Сучасна наука кримінального права наголошує на необхідності розширення розуміння предмета. В епоху Інтернету речей (IoT) та нейромереж з'являються гібридні апаратно-програмні комплекси, де ШТЗ оснащуються модулями машинного навчання для автономного підбору паролів або обходу біометричних систем безпеки.

Класифікація шкідливих технічних засобів (ШТЗ)

Шкідливі технічні засоби за процесом створення та первинним призначенням поділяються на: спеціально створені для протиправних цілей (не мають легального застосування); легальні засоби, які були апаратно модифіковані зловмисниками; традиційні засоби подвійного призначення, використані з умислом на втручання.

Таблиця 2.1

Типологія шкідливих технічних засобів та матеріали правозастосовної практики

Вид ШТЗ	Опис та технологічні особливості	Практичний кейс (моделювання на основі судової практики)
Автомобільний кодграбер	Пристрій для перехоплення, криптографічного	Особа через форум у DarkNet придбала апаратний кодграбер, замаскований під
	аналізу й генерування радіочастотних сигналів систем автосигналізації. *Сучасна модифікація:* використання AI-алгоритмів для прогнозування динамічних кодів (Rolling Code).	брелок сигналізації. Перебуваючи на парковці торгового центру, зловмисник перехопив сигнал від ключа власника авто, розкодував його та здійснив несанкціоноване відкриття транспортного засобу. Суд кваліфікував дії за ст. 361-1 та підготовку до ст. 289 КК України.
Банкоматний скімер	Мініатюрний апаратний модуль, що непомітно монтується на картоприймач банкомата для фізичного зчитування даних магнітної смуги картки. Часто діє в парі з мікрокамерою для фіксації PIN-коду.	Група осіб встановила модифіковані скімери на банкомати у спальних районах міста. Сучасна модифікація пристрою дозволяла автоматично передавати зчитані дампи карток через GSM-модуль на сервер зловмисників. Збут таких пристроїв кваліфікується за ст. 361-1 КК України.
NFC-ретранслятори	Пристрої для здійснення «Relay-атак». Дозволяють перехопити сигнал безконтактної смарт-картки	Зловмисник із портативним NFC-зчитувачем у рюкзаку наближався до потерпілих у переповненому громадському транспорті. Пристрій зчитував дані їхніх

Вид ШТЗ	Опис та технологічні особливості	Практичний кейс (моделювання на основі судової практики)
	(RFID/NFC) та ретранслювати його на платіжний термінал, який знаходиться на великій відстані.	карток і миттєво ретранслював сигнал спільнику, який у цей момент здійснював покупку дорогої техніки в магазині через модифікований POS-термінал.

Класифікація шкідливого програмного забезпечення (ШПЗ)

Для правильної кваліфікації діянь слід чітко розрізняти види шкідливих програм за їхнім функціоналом, способом поширення та вектором атаки. Враховуючи еволюцію кіберзагроз, класифікацію необхідно доповнити ML-орієнтованими загрозами (Machine Learning malware).

Таблиця 2.2

Класифікація шкідливого програмного забезпечення

Група ШПЗ	Підтип	Функціонал та способи поширення	Практичний кейс
Здатні до саморозмноження	Віруси	Пасивні програми. Вбудовують свій код у легітимні файли. Активуються лише при запуску інфікованого файлу користувачем. *AI-вектор:* поліморфні віруси, що самостійно змінюють свій код для обходу антивірусів.	Студент радіотехнічного факультету створив поліморфний вірус, який прикріплювався до текстових документів. Метою було тестування антивірусних систем, проте вірус вийшов з-під контролю. Суд визнав винним за ст. 361-1 (створення ШПЗ).
	Хробаки (Worms)	Активні програми. Самостійно сканують мережу на наявність вразливостей в ОС і поширюються без участі користувача.	Організована група розробила мережевого хробака, який експлуатував вразливість у протоколах віддаленого робочого столу (RDP) для створення масштабного

Група ШПЗ	**Підтип**	**Функціонал та способи поширення**	**Практичний кейс**
			ботнету з тисяч заражених комп'ютерів.
	Трояни	Маскуються під корисне програмне забезпечення (ігри, оновлення). Поширюються методами соціальної інженерії.	Зловмисник поширював троянську програму під виглядом «офіційного оновлення» для популярного месенджера, яка після встановлення надавала прихований доступ до камери пристрою.
Інструментальні	Бекдор (Backdoor)	Створює прихований канал (чорний хід) у систему, дозволяючи хакеру отримати віддалений доступ в обхід стандартної процедури аутентифікації.	Системний адміністратор перед звільненням умисно залишив у корпоративній мережі скрипт-бекдор, щоб у майбутньому мати змогу несанкціоновано завантажувати комерційну документацію.
	Кейлогер (Keylogger)	Шпигунське ПЗ. Реєструє натискання клавіш, перехоплює паролі, листування, робить знімки екрана.	Ревнивий чоловік придбав у мережі інтернет та приховано встановив на ноутбук дружини програмний кейлогер для збору паролів від її соціальних мереж. Дії кваліфіковано за ст. 361-1 КК.
Фінансово-орієнтовані	Ransomware (Вимагачі)	Блокують доступ до ОС або незворотно шифрують файли користувача криптографічним алгоритмом, вимагаючи переказ коштів (найчастіше у криптовалюті) за	Хакери надіслали на пошту медичного закладу лист із замаскованим файлом. Після його відкриття вірус-вимагач зашифрував бази даних пацієнтів. За дешифрування

Група ШПЗ	Підтип	Функціонал та способи поширення	Практичний кейс
		надання ключа дешифрування.	вимагалося 5 Bitcoins.
	Стілери (Stealer)	Спеціалізовані скрипти для викрадення збережених у браузерах паролів, файлів cookie (сесій) та файлів локальних криптогаманців.	Зловмисник розповсюджував на ігрових форумах безкоштовні «чіти», всередині яких був «вшитий» (криптований) стілер. Програма збирала дані авторизації Steam-акаунтів та відправляла їх на Telegram-бота автора.
	Кліпери (Clippers)	Вузькоспеціалізоване ПЗ, що постійно моніторить буфер обміну ОС. При копіюванні довгої адреси криптогаманця, програма непомітно підміняє її на адресу зловмисника.	Особа замовила написання скрипта-кліпера, який підміняв адреси гаманців у мережі TRC-20. Внаслідок того, що транзакції в блокчейні є незворотними, потерпілі власноруч відправляли кошти на рахунок шахрая.

Об’єктивна сторона: форми діяння

З об’єктивної сторони це кримінальне правопорушення має **формальний склад**. Воно вважається закінченим з моменту вчинення хоча б однієї з альтернативних дій, незалежно від того, чи було ШПЗ/ШТЗ фактично застосоване для втручання та чи настали матеріальні збитки. Закон виокремлює три форми діяння:

1. **Створення** — це розробка (написання коду, конструювання апарату) нового шкідливого засобу або умисна модифікація легітимного ПЗ/пристрою, внаслідок якої воно набуває деструктивних властивостей.

2. **Розповсюдження** — дії, спрямовані на те, щоб зробити шкідливий засіб доступним для інших осіб.

3. **Збут** — відчуження шкідливого засобу на користь іншої особи.

Проблема розмежування. У кримінально-правовій доктрині часто виникає плутанина між поняттями «розповсюдження» та «збут». Для

правильної кваліфікації пропонується чітко розмежовувати ці діяння за такими критеріями:

Таблиця 2.3

Відмежування розповсюдження від збуту ШПЗ/ШТЗ

Ознака	Розповсюдження	Збут
Адресність та мета	Надання доступу до засобу невизначеному колу осіб (масовість).	Відчуження засобу на користь конкретної, визначеної особи (адресність).
Спосіб вчинення	Викладення вихідного коду на публічних репозиторіях (напр., GitHub), масова розсилка спамом, розміщення на торрент-трекерах, використання AI-ботів для автоматизованого посіву посилань.	Передача файлу або пристрою конкретному замовнику (через закриті чати, DarkNet-маркетплейси або при особистій зустрічі).
Оплатність	Не є обов'язковою ознакою. Дуже часто здійснюється безоплатно (з хуліганських, ідеологічних мотивів або для створення ботнету).	Переважно має корисливий мотив (продаж за фіатні гроші чи криптовалюту), хоча можливий і безоплатний збут (передача як подарунок спільнику).

Суб'єкт та суб'єктивна сторона

Суб'єкт кримінального правопорушення загальний – фізична осудна особа, яка досягла 16-річного віку. Варто зауважити, що для притягнення до відповідальності за *розповсюдження* або *збут* особа не обов'язково повинна мати високий рівень технічних знань. Суб'єктом може бути і так званий «скрипт-кідді» (script kiddie), який придбав готовий вірус і просто перепродав його або розмістив у мережі. Юридичні особи не є суб'єктами кримінального правопорушення за КК України, проте до них можуть застосовуватися заходи кримінально-правового характеру (наприклад, до компаній, які умисно надають «абузостійкий» хостинг для розміщення ШПЗ).

Суб'єктивна сторона характеризується виключно **прямим умислом**. Особа усвідомлює шкідливий характер (призначення) створюваних, розповсюджуваних чи збуваних нею програмних або

технічних засобів і бажає вчиняти ці дії.

Обов'язковою ознакою для альтернативи «створення» є наявність **мети протиправного використання, розповсюдження або збуту**. Якщо програміст створює вірус виключно в наукових цілях, для тестування власної закритої системи безпеки (Penetration testing) або написання антивірусу, і вживає заходів щодо неможливості його витоку, склад кримінального правопорушення за ст. 361-1 КК України відсутній через відсутність протиправної мети. Мотиви (користь, помста, хуліганство) на кваліфікацію не впливають.

Кримінально-правова характеристика несанкціонованого збуту або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст. 361-2 КК України)

Стаття 361-2 КК України встановлює кримінальну відповідальність за незаконний обіг інформації, яка хоч і міститься в інформаційно-телекомунікаційних системах, але має особливий, захищений законом правовий режим доступу.

Доктринальна пропозиція: З огляду на запропоновану нами в першому розділі модернізацію понятійного апарату, назву та диспозицію цієї статті доцільно було б викласти у такій редакції: «Несанкціоновані збут або розповсюдження *цифрової інформації з обмеженим доступом*». Це дозволило б усунути застаріле формулювання «інформації... яка зберігається в електронно-обчислювальних машинах» та повноцінно охопити сучасні носії: хмарні сховища (Cloud Storage), мобільні пристрої, IoT-гаджети та децентралізовані бази даних.

Актуальність протидії цим кримінальним правопорушенням підтверджується статистикою: за даними Департаменту кіберполіції Національної поліції України, у 2025 році кількість витоків баз даних зросла на 35 %, переважно через їх активну тіньову торгівлю (Data Brokering) у сегменті DarkNet та закритих Telegram-каналах.

Предмет кримінального правопорушення: інформація з обмеженим доступом.

Предметом цього кримінального правопорушення є не будь-які цифрові дані, а виключно **інформація з обмеженим доступом**. Відповідно до статті 21 Закону України «Про інформацію» (у чинній редакції), така інформація за своїм правовим режимом поділяється на три категорії: конфіденційну, таємну та службову.

Таблиця 2.4

Класифікація цифрової інформації з обмеженим доступом

Категорія	Законодавче визначення та сутність	Види та приклади з практики
Конфіденційна	Інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою (крім суб'єктів владних повноважень). Може поширюватися лише за згодою власника та у визначеному ним порядку.	**Види:** Персональні дані (ПІБ, адреси, телефони), комерційна таємниця підприємства. **Кейс:** Вирок Київського районного суду (2024 рік) щодо особи, яка незаконно заволоділа базою персональних даних користувачів одного з державних сервісів та здійснювала її поштучний продаж (засуджено до 5 років позбавлення волі за ст. 361-2 КК).
Таємна	Інформація, розголошення якої може завдати шкоди особі, суспільству або державі. Включає державну та різні види професійних таємниць, що охороняються спеціальними законами.	**Види:** Державна, банківська, лікарська, адвокатська, нотаріальна таємниця, таємниця досудового розслідування. **Кейс:** Група осіб здійснила хакерську атаку на сервери комерційного банку, викрала базу даних (банківську таємницю) та продала її конкурентам на чорному ринку (справа 2024 року, засуджено до 5 років).
Службова	Інформація, що міститься в документах суб'єктів владних повноважень (внутрішньовідомча кореспонденція, доповідні записки), а також інформація, зібрана в процесі оперативно-розшукової, контррозвідувальної	**Види:** Матеріали негласних слідчих (розшукових) дій, внутрішні інструкції правоохоронних органів. **Кейс:** У 2025 році було засуджено особу, яка, зламавши поштову скриньку співробітника антикорупційного органу, заволоділа цифровими копіями протоколів допитів (службовою

Категорія	Законодавче визначення та сутність	Види та приклади з практики
	діяльності або у сфері оборони, яка не становить державної таємниці.	інформацією) і розповсюдила їх у мережі Інтернет.

Об’єктивна сторона: форми діяння та момент закінчення

Об’єктивна сторона кримінального правопорушення, передбаченого ст. 361-2 КК України, полягає у вчиненні суспільно небезпечних дій у двох альтернативних формах:

1. **Несанкціонований збут** цифрової інформації з обмеженим доступом.
2. **Несанкціоноване розповсюдження** такої інформації.

Конструкція складу цього правопорушення є **формальною**. Це означає, що кримінальне правопорушення (за частиною 1) визнається закінченим з моменту фактичного вчинення будь-якої з вказаних дій (передачі інформації або надання доступу до неї), незалежно від того, чи настали суспільно небезпечні наслідки (матеріальна шкода компанії, порушення прав громадян тощо). Настання значної шкоди передбачено лише як кваліфікуюча ознака у частині 2 цієї статті.

Для правильної юридичної оцінки діяння необхідно чітко розмежовувати поняття «збут» і «розповсюдження».

Таблиця 2.5

Розмежування несанкціонованого збуту та розповсюдження

Критерій	Збут (Sale / Transfer)	Розповсюдження (Dissemination)
Сутність дії	Відчуження (передача) цифрової інформації з переходом можливості розпоряджатися нею.	Надання доступу до інформації або її цифрових копій без обов’язкової передачі «права власності».
Адресат	Конкретно визначена особа (покупець, замовник, конкурент).	Невизначене коло осіб (масовість).
Оплатність	Переважно має оплатний характер (продаж за гроші/криптовалюту), проте можливий і безоплатний збут	Може бути як оплатним (доступ за підпискою), так і безоплатним.

Критерій	Збут (Sale / Transfer)	Розповсюдження (Dissemination)
	(передача в обмін на послугу).	
Приклад із практики	Хакер на замовлення викрав базу даних клієнтів фітнес-центру та продав її власнику конкуруючої мережі. (Вирок Шевченківського райсуду м. Києва, 2024 р. – 4 роки позбавлення волі)	Зловмисник, бажаючи «прославитися», виклав архів із викраденою базою даних у відкритий доступ на загальнодоступному хакерському форумі або в публічному Telegram-каналі. (Справа в м. Харкові, 2025 р. – 3 роки позбавлення волі умовно).

Важлива умова: Як збут, так і розповсюдження мають бути **несанкціонованими**, тобто здійснюватися без дозволу власника (розпорядника) інформації або всупереч встановленому законом чи договором порядку.

Суб'єкт кримінального правопорушення та проблема відмежування

Суб'єкт кримінального правопорушення за ст. 361-2 КК України — загальний. Це фізична осудна особа, яка досягла 16-річного віку. Здебільшого це особи, які попередньо незаконно заволоділи цією інформацією (наприклад, шляхом втручання за ст. 361 КК України) або випадково отримали до неї доступ і вирішили нею розпорядитися.

Правило кваліфікації (відмежування від ст. 362 КК України): Ключовим моментом є наявність у особи легального права доступу до інформації на момент її збуту/розповсюдження. Якщо ці дії вчиняє особа, яка **не має** законного права доступу (хакер, стороння особа), діяння кваліфікується за ст. 361-2 КК України.

Якщо ж збут або розповсюдження здійснює інсайдер — особа, яка **має** легальний доступ до системи чи даних у зв'язку зі своїми службовими обов'язками (наприклад, менеджер банку копіює клієнтську базу і продає її), то такі дії охоплюються ознаками спеціального суб'єкта і мають кваліфікуватися за статтею 362 КК України (Несанкціоновані дії з інформацією, вчинені особою, яка має право доступу до неї). Ця специфіка буде детально розглянута у наступному підрозділі.

Суб'єктивна сторона кримінального правопорушення

Суб'єктивна сторона цього складу характеризується виною у формі **прямого умислу**.

Для констатації вини необхідно довести, що особа усвідомлювала такі обставини:

1. Інтелектуальний момент: особа достовірно знала або усвідомлювала, що інформація, з якою вона здійснює операції, належить до категорії інформації з обмеженим доступом (містить гриф «Таємно», є банківською таємницею або масивом персональних даних).

2. Усвідомлення неправомірності: особа розуміла, що не має законного дозволу від власника чи розпорядника на відчуження або поширення цих даних.

3. Вольовий момент: особа бажала здійснити саме збут або розповсюдження цієї інформації.

Мотиви вчинення кримінального правопорушення не є обов'язковими ознаками складу, проте часто впливають на кваліфікацію за іншими статтями (наприклад, при збуті державних секретів іноземній розвідці з мотивів шкоди суверенітету діяння додатково кваліфікуватиметься як державна зрада). Найчастіше мотиви є корисливими (отримання прибутку від продажу даних), іноді — шантаж, помста (наприклад, публікація інтимних фото — revenge porn, що також може містити ознаки ст. 182 КК України), або прагнення до самоствердження у хакерській спільноті.

Кримінально-правова характеристика несанкціонованих дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (стаття 362 КК України)

Стаття 362 КК України передбачає кримінальну відповідальність за специфічну категорію посягань в інформаційній сфері, які в кримінології та кібербезпеці отримали назву «інсайдерські загрози» (діяння «внутрішнього порушника»). На відміну від класичного хакерського втручання (ст. 361 КК України), де зловмисник долає системи захисту ззовні, суб'єкт кримінального правопорушення за ст. 362 КК України вже наділений легальними повноваженнями та інструментами (паролями, ключами доступу, токенами) для роботи з системою, проте використовує їх на шкоду власнику інформації або державі.

Основним безпосереднім об'єктом цього кримінального правопорушення є суспільні відносини, що забезпечують нормальний, встановлений законом або договором режим зберігання, оброблення, використання та захисту цифрової інформації в інформаційно-телекомунікаційних системах.

Суб'єкт кримінального правопорушення: специфіка спеціального суб'єкта

Ключовою системоутворювальною ознакою цього складу є наявність **спеціального суб'єкта**. Це фізична осудна особа, яка досягла 16-річного віку і, головне, **має легальне право доступу** до цифрової інформації або систем, де вона оброблюється.

Право доступу не є абстрактною категорією; воно має бути чітко юридично закріпленим. Згідно з положеннями ст. 4 Закону України «Про захист інформації в інформаційно-комунікаційних системах», власник системи самостійно встановлює порядок доступу та вичерпний перелік уповноважених користувачів.

Підставами для виникнення права доступу можуть бути:

1. **Закон або інший нормативно-правовий акт.** Стосується переважно державних службовців, правоохоронців, нотаріусів, які працюють із державними реєстрами.

– *Практичний кейс:* Інспектор патрульної поліції, маючи легальний доступ до інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України» (баз даних МВС), на прохання третіх осіб здійснював перевірку маршрутів пересування конкретних транспортних засобів за допомогою системи відеофіксації «Гарпун». Він копіював ці дані та передавав замовникам. Суд кваліфікував його дії за ст. 362 КК України, оскільки доступ до системи був наданий йому відповідно до Закону України «Про Національну поліцію», але використаний несанкціоновано.

2. **Цивільно-правовий або господарський договір.** Угода між власником інформаційної системи та підрядником (наприклад, аутсорсинговою ІТ-компанією).

– *Практичний кейс:* Залучений за договором про надання послуг (SLA) незалежний аудитор з інформаційної безпеки отримав тимчасовий адміністративний доступ до серверів великого комерційного банку. Замість виконання умов договору щодо пошуку вразливостей, він скопіював базу даних VIP-клієнтів.

3. **Службові та внутрішні корпоративні документи.** Посадові інструкції, накази про прийняття на роботу, розпорядження керівника про надання облікових записів та паролів.

– *Практичний кейс:* Головний бухгалтер приватного підприємства, маючи авторизований доступ до корпоративної системи «1С: Підприємство» та клієнт-банку на підставі своєї посадової інструкції, перед звільненням умисно змінив фінансові показники закритих періодів, щоб приховати власні фінансові махінації.

Об’єктивна сторона: форми діяння та їх наслідки

Залежно від характеру суспільно небезпечних дій та настання наслідків, об’єктивна сторона цього кримінального правопорушення диференціюється на дві групи (відповідно до частин 1 та 2 статті 362 КК України).

Таблиця 2.6

Форми об’єктивної сторони за ст. 362 КК України

Частина статті та вид складу	Форма діяння	Доктринальне тлумачення	Практичний кейс (моделювання правозастосовної практики)
Частина 1 *(Формальний склад)*	**Несанкціонована зміна**	Умисна модифікація змісту цифрової інформації, внесення правок, що порушують її цілісність та достовірність.	Державний реєстратор речових прав на нерухоме майно, використовуючи власний електронний цифровий підпис (ЕЦП), несанкціоновано вніс зміни до Державного реєстру, змінивши інформацію про законного власника комерційного приміщення на підставну особу.
	Несанкціоноване знищення	Дії, внаслідок яких інформація або її фрагменти зникають з носія безповоротно або стають непридатними для подальшого використання.	Лікар-терапевт, перебуваючи у конфлікті з керівництвом клініки, перед звільненням умисно видалив електронні медичні картки понад 500 пацієнтів із системи eHealth, маючи до них легальний доступ через свій робочий кабінет.
	Несанкціоноване блокування	Обмеження або повне унеможливлення доступу до ресурсу	Системний адміністратор компанії після відмови у підвищенні заробітної

Частина статті та вид складу	**Форма діяння**	**Доктринальне тлумачення**	**Практичний кейс (моделювання правозастосовної практики)**
		для інших законних користувачів чи власника системи	плати змінив усі паролі доступу до корпоративних серверів і баз даних, заблокувавши роботу всього підприємства на дві доби.
Частина 2 *(Матеріальний склад)*	**Перехоплення інформації**	Неправомірне одержання інформації під час її передачі каналами зв'язку, що призвело до її витоку.	Адміністратор корпоративної мережі налаштував маршрутизатор таким чином, що копії всього електронного листування топ-менеджменту приховано дублювалися на його особисту скриньку, після чого ці дані були продані конкурентам.
	Копіювання інформації	Створення копії цифрової інформації на іншому носії, яке **обов'язково** призвело до її витоку (розголошення третім особам).	Співробітник телекомунікаційної компанії скопіював білінг-дані (історію дзвінків) конкретного абонента на власну флеш-карту та передав цю інформацію приватному детективу за грошову винагороду.

Наукова дискусія: критика законодавчої конструкції «перехоплення» інсайдером

У сучасній кримінально-правовій доктрині обґрунтовано піддається критиці наявність терміна «перехоплення» (interception) у диспозиції ст. 362 КК України.

З технічної та логічної точок зору, перехоплення – це процес неправомірного одержання інформації під час її передачі каналами зв'язку (наприклад, атака типу Man-in-the-Middle). Це дія, яка за своєю

природою притаманна зовнішньому зловмиснику (хакеру), який не має права доступу до кінцевих вузлів системи.

Якщо ж особа має легальне право доступу (що є обов'язковою ознакою суб'єкта ст. 362 КК України), їй технічно недоцільно і не потрібно нічого «перехоплювати» в каналах зв'язку – вона вже авторизована всередині системи. Інсайдер має можливість безпосередньо скопіювати базу даних або переглянути необхідні файли. Наприклад, якщо працівник банку вивантажує таблицю з клієнтськими рахунками, він здійснює не перехоплення, а саме несанкціоноване копіювання, яке згодом призводить до витоку.

Наукова пропозиція щодо вдосконалення (Legislative Proposal):

Для усунення цієї техніко-юридичної колізії пропонується виключити термін «перехоплення» з диспозиції статті 362 КК України. Частину другу варто викласти у такій редакції: *«Несанкціоноване копіювання цифрової інформації... якщо це призвело до її витоку, вчинене особою, яка має право доступу до такої інформації»*.

Крім того, враховуючи високу суспільну небезпеку інсайдерських змов, доцільно доповнити статтю 362 КК України новою частиною (ч. 4), яка б передбачала сувору відповідальність (до 10 років позбавлення волі) за дії, вчинені організованою групою інсайдерів, або якщо такі дії заподіяли шкоду національній безпеці чи критичній інфраструктурі держави.

Термінологічна модернізація у контексті хмарних та мобільних технологій.

Як і в аналізованих раніше нормах Розділу XVI КК України, стаття 362 містить застарілий понятійний апарат. Законодавець оперує конструкцією «інформація, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах».

Сьогодні корпоративний сектор та державні органи масово переходять на хмарні обчислення (Cloud Computing) та впроваджують політики BYOD (Bring Your Own Device – використання особистих мобільних пристроїв для роботи). Відповідно, інформація, яку викрадає чи знищує інсайдер, фізично може знаходитися не на локальному «комп'ютері» підприємства, а на розподілених хмарних серверах, доступ до яких працівник отримує через корпоративний додаток на власному смартфоні або планшеті.

Для забезпечення єдності правозастосування та охоплення сучасних технологічних реалій, необхідно:

1. Замінити вузький термін «електронно-обчислювальна машина

(комп'ютер)» на універсальну категорію **«цифровий пристрій»**.

2. Громіздкі терміни «автоматизовані системи» та «комп'ютерні мережі» об'єднати в єдине комплексне поняття **«інформаційно-телекомунікаційні системи та мережі»**. Це дозволить судам уникати штучних експертиз щодо того, чи є смартфон із доступом до корпоративної хмари «комп'ютером» у розумінні кримінального закону.

Кримінально-правова характеристика порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється (ст. 363 КК України)

Стаття 363 КК України є специфічною нормою в системі кіберзалежних кримінальних правопорушень, оскільки вона криміналізує не активні умисні атаки, а так звану «службову недбалість» у сфері кібербезпеки та IT-інфраструктури.

Специфіка цього діяння полягає в тому, що воно належить до так званих інсайдерських або «внутрішніх» кіберзагроз. Суспільна небезпека посягання зумовлена тим, що порушення здійснюється спеціальним суб'єктом – особою, яка має легальний доступ до систем та безпосередньо відповідає за їхню безперебійну експлуатацію і надійний захист даних. Це докорінно відрізняє ст. 363 КК України від зовнішнього несанкціонованого втручання (ст. 361 КК України).

Об'єкт та предмет кримінального правопорушення

Для правильної кваліфікації та розуміння суспільної небезпеки цього діяння об'єкт необхідно розглядати через його багаторівневу структуру.

- **Родовий об'єкт:** Суспільні відносини, що забезпечують безпеку у сфері використання цифрових пристроїв, інформаційно-телекомунікаційних систем та мереж. По суті, це відносини, що гарантують загальний стан кібербезпеки в державі.
- **Основний безпосередній об'єкт:** Встановлений законодавством та локальними нормативно-правовими актами порядок експлуатації систем та мереж, а також порядок чи правила захисту цифрової інформації, яка в них оброблюється.
- **Додатковий обов'язковий об'єкт:** Оскільки склад кримінального правопорушення є матеріальним (передбачає обов'язкове настання значної шкоди), додатковим об'єктом завжди виступають відносини власності на інформацію чи обладнання, а також регламентована діяльність підприємств, установ, організацій чи інтереси

фізичних осіб.

Предмет кримінального правопорушення є альтернативним і включає:

1. Апаратні та програмно-апаратні комплекси (сервери, робочі станції, маршрутизатори, хмарні кластери).

2. Цифрова інформація, що оброблюється, зберігається або передається у цих системах.

Об’єктивна сторона: бланкетна диспозиція та форми порушень

Особливістю об’єктивної сторони цього кримінального правопорушення є її **бланкетний характер**. Диспозиція статті 363 КК України не містить (і не може містити) вичерпного переліку конкретних технічних дій, які вважаються порушенням. Для встановлення об’єктивної істини слідчому та суду необхідно обов'язково звертатися до інших нормативно-правових актів або внутрішніх регламентів:

- Законів України («Про основні засади забезпечення кібербезпеки України», «Про захист інформації в інформаційно-комунікаційних системах»);
- Державних стандартів України (ДСТУ) у галузі криптографічного та технічного захисту інформації;
- Внутрішніх політик інформаційної безпеки підприємства, інструкцій з експлуатації обладнання та правил внутрішнього трудового розпорядку.

Стаття передбачає два самостійні види порушень, які на практиці варто чітко розмежовувати.

Таблиця 2.7

Види порушень за статтею 363 КК України

Вид порушення	Доктринальне тлумачення	Практичний кейс та наслідки
Порушення правил експлуатації	Недотримання технічних вимог та регламентів щодо використання апаратного та програмного забезпечення. Самовільна інсталяція ПЗ, підключення сторонніх носіїв, ігнорування критичних оновлень безпеки (патчів).	*Кейс:* Системний адміністратор державного реєстру проігнорував попередження про необхідність оновлення антивірусного ПЗ на серверах. Внаслідок цього система була інфікована вірусом-вимагачем. *Наслідок:* Знищення бази даних, збитки на суму понад 500 тис. грн. (Вирок щодо

Вид порушення	Доктринальне тлумачення	Практичний кейс та наслідки
		працівника ІТ-відділу у м. Полтава, 2024 р.). *Наслідок:* Витік комерційної таємниці, репутаційні та фінансові збитки понад 1 млн. грн. (Справа 2024 р., засуджено до 3 років позбавлення волі).
Порушення порядку та правил захисту інформації	Недотримання організаційних та адміністративних заходів безпеки. Неналежне управління ключами доступу, парольними політиками, розголошення архітектури мережі.	*Кейс:* Керівник відділу інформаційної безпеки банку зберігав файл із root-паролями до серверів у відкритому вигляді на своєму особистому Google Drive. Обліковий запис керівника був зламаний хакерами, які отримали паролі та скопіювали базу клієнтів.

Наслідки: значна шкода та проблеми її визначення

Склад кримінального правопорушення за ст. 363 КК України є **матеріальним**. Кримінальна відповідальність настає виключно у разі, якщо описані вище порушення призвели до суспільно небезпечних наслідків у вигляді **заподіяння значної шкоди**. Якщо працівник грубо порушив інструкцію (наприклад, залишив сервер розблокованим), але хакери цим не скористалися і шкоди не настало, його дії тягнуть лише дисциплінарну відповідальність (догана, звільнення).

Проблематика визначення порогу шкоди:

Відповідно до чинної примітки до ст. 361 КК України (яка поширюється на весь Розділ XVI), значною шкодою визнається матеріальний збиток, який у 300 і більше разів перевищує неоподатковуваний мінімум доходів громадян (НМДГ). Враховуючи щорічне зростання соціальних стандартів, цей поріг стає занадто високим (станом на 2025–2026 роки він перевищує сотні тисяч гривень). Для злочинів, вчинених через службову недбалість, такий високий майновий ценз призводить до того, що багато небезпечних діянь (наприклад, втрата медичних даних, яку важко оцінити у фіатному еквіваленті) залишаються поза межами кримінальної юрисдикції.

Наукова пропозиція:

Для підвищення превентивної ефективності норми пропонується доповнити ст. 363 КК України окремою приміткою, яка б встановлювала

нижчий і справедливіший поріг криміналізації: *«Шкода, передбачена цією статтею, визнається значною, якщо вона в п'ятдесят і більше разів перевищує неоподатковуваний мінімум доходів громадян»*.

Крім того, враховуючи кібератаки на енергетичну інфраструктуру в умовах воєнного стану, доцільно доповнити статтю частиною 3, яка б встановлювала особливо сувору відповідальність (до 10 років позбавлення волі) за порушення правил експлуатації на об'єктах критичної інфраструктури, якщо це спричинило тяжкі наслідки (наприклад, відключення електропостачання регіону).

Суб'єкт кримінального правопорушення

Суб'єкт кримінального правопорушення — **спеціальний**. Це фізична осудна особа (з 16 років), на яку офіційно покладено обов'язки щодо забезпечення експлуатації систем або захисту інформації.

Статус такої особи не може презюмуватися; він має бути чітко зафіксований документально до моменту вчинення правопорушення. Документами, що підтверджують статус спеціального суб'єкта, є:

1. Наказ керівника підприємства про призначення на посаду або покладення відповідних обов'язків.
2. Посадова інструкція (наприклад, адміністратора баз даних, інженера з кібербезпеки), з якою особа обов'язково має бути ознайомлена під особистий підпис.
3. Трудовий договір або контракт (NDA).

Якщо систему випадково пошкодив рядовий користувач (наприклад, бухгалтер пролив каву на сервер), який не був відповідальним за її технічну експлуатацію, його дії не утворюють складу ст. 363 КК України (вони можуть розглядатися як умисне або необережне знищення майна).

Суб'єктивна сторона: ставлення до діяння та наслідків

Суб'єктивна сторона є ключовим критерієм для відмежування ст. 363 КК України від суміжних складів (ст. 361 або ст. 362 КК України).

Специфіка полягає у роздвоєному ставленні винної особи:

- **До самого діяння (порушення правил):** Ставлення може бути як умисним, так і необережним. Наприклад, системний адміністратор може *свідомо та умисно* вимкнути файрвол або антивірус (бо вони «гальмують» роботу сервера), усвідомлюючи, що порушує політику безпеки. Або він може *забути* оновити сертифікат безпеки (порушення через недбалість).
- **До наслідків (значної шкоди):** Ставлення має бути **виключно необережним** (у формі кримінально-протиправної самовпевненості або

кримінально-протиправної недбалості). Адміністратор, вимикаючи антивірус, не бажав зараження мережі вірусом і витоку даних, а легковажно розраховував, що цього не станеться (самовпевненість), або взагалі не передбачав такої можливості, хоча повинен був і міг її передбачити (недбалість).

Важливе правило кваліфікації: Якщо буде доведено, що спеціальний суб'єкт умисно порушив правила захисту (наприклад, залишив відкритим порт на сервері) саме з метою, щоб дати можливість хакерам проникнути в систему та вкрасти дані, його дії перестають бути необережним злочином. Така поведінка кваліфікується як **співучасть (пособництво)** у вчиненні умисного кримінального правопорушення, передбаченого ст. 361 або ст. 362 КК України, залежно від обставин справи.

Кримінально-правова характеристика перешкоджання роботі інформаційно-телекомунікаційних систем шляхом масового розповсюдження повідомлень (ст. 363-1 КК України)

Стаття 363-1 КК України встановлює кримінальну відповідальність за діяння, які у повсякденному житті та технічному середовищі ми називаємо спам-кампаніями (Spamming) та масованими DDoS-атаками (Distributed Denial of Service).

В умовах тотальної цифровізації економіки та гібридної війни ці посягання становлять значну загрозу, оскільки вони спрямовані не на викрадення даних, а на паралізацію роботи критичних сервісів (банківських додатків, державних порталів, новинних сайтів), що може спричинити масштабну паніку та колосальні фінансові збитки.

Об'єкт кримінального правопорушення

- **Основний безпосередній об'єкт:** Встановлений законодавством порядок та регламентовані процеси оброблення цифрової інформації (її приймання, маршрутизації, перетворення, зберігання та видачі) в інформаційно-телекомунікаційних системах і мережах. Гарантується така властивість інформації, як її *доступність* для легітимних користувачів.
- **Додатковий факультативний об'єкт:** Залежно від мети атаки, додатковим об'єктом можуть виступати: нормальна діяльність та авторитет суб'єктів владних повноважень (при атаках на державні реєстри), економічні інтереси суб'єктів господарювання (при атаках на e-commerce), а також суспільні відносини щодо нормального функціонування критичної інфраструктури (енергетика, фінансовий сектор, транспорт).

Об’єктивна сторона: механізм спаму та обов’язкові ознаки

Об’єктивна сторона цього кримінального правопорушення сконструйована як **матеріальний склад**. Вона включає:

1. Суспільно небезпечне діяння (умисне масове розповсюдження повідомлень електрозв’язку, здійснене без попередньої згоди адресатів).
2. Суспільно небезпечні наслідки (порушення або повне припинення роботи системи чи мережі).
3. Причиновий зв’язок між діянням і наслідками.

Перша форма вчинення правопорушення – створення так званого шкідливого «спаму».

Таблиця 2.8

Обов’язкові ознаки масового розповсюдження повідомлень (Спаму)

Ознака діяння	Доктринальне та законодавче тлумачення	Практичний кейс та наслідки
Масовість	Оціночна категорія. Означає, що одне й те саме повідомлення автоматично копіюється та надсилається на велику кількість адрес. Відповідно до ст. 1 Закону України «Про електронні комунікації», спамом визнаються електронні повідомлення, які масово надсилаються без попередньої згоди (понад п’ять повідомлень одному абоненту).	*Кейс:* Зловмисник організував масову розсилку фішингових повідомлень тисячам користувачів Telegram з використанням автоматизованих скриптів (ботів). *Наслідок:* Перевантаження поштових серверів провайдера та порушення нормальної маршрутизації трафіку. (Справа 2024 року, засуджено до 3 років позбавлення волі за ст. 363-1 КК).
Відсутність згоди	Адресат (користувач або власник системи) не замовляв отримання цієї інформації (відсутній принцип Opt-in) та не надавав свої контактні дані для розсилки.	*Кейс:* Маркетингове агентство, використовуючи незаконно придбану базу електронних адрес, здійснило масову агресивну розсилку реклами. *Наслідок:* Внаслідок генерації мільйонів листів за годину відбулося «падіння» (відмова) корпоративного поштового сервера компанії-жертви. (Справа 2024 року, 2 роки умовно).

Ознака діяння	Доктринальне та законодавче тлумачення	Практичний кейс та наслідки
Настання наслідків	Дії повинні об'єктивно призвести до технологічних збоїв: переповнення	Якщо особа відправила мільйон листів, але потужний антиспам-фільтр провайдера
	дискового простору сервера, вичерпання ресурсів оперативної пам'яті, суттєвого уповільнення обробки легітимних запитів (порушення роботи) або повної зупинки системи (припинення роботи).	заблокував їх на вході, і сервер продовжив нормальну роботу — склад кримінального правопорушення за ст. 363-1 КК України *відсутній* (можлива кваліфікація як замаху).

Кібератаки типу «Відмова в обслуговуванні» (DDoS-атаки)

Найбільш небезпечною, сучасною та поширеною формою перешкоджання роботі систем є DDoS-атака.

Механізм дії: Зловмисник, використовуючи спеціальне програмне забезпечення, генерує та спрямовує величезну (аномальну) кількість беззмістовних зовнішніх запитів або пакетів даних до цільового вебресурсу, сервера чи мережевого обладнання (наприклад, мільйони запитів на секунду). Атакована система фізично не встигає їх обробляти, вичерпує свої обчислювальні ресурси (канали зв'язку, процесорний час), внаслідок чого виникають критичні збої або повна зупинка функціонування — відмова в обслуговуванні для реальних (легітимних) користувачів.

Таблиця 2.9

Види DDoS-атак за мотивом вчинення

Вид атаки	Сутність та мотив	Практичний кейс та наслідки
Атаки на замовлення (Конкурентні війни / DDoS for Hire)	Замовник неофіційно сплачує хакеру винагороду за те, щоб він зробив недоступним сайт бізнес-конкурента на певний час. У сегменті DarkNet ціни за добу простою ресурсу можуть становити від 100 доларів США.	*Кейс:* Власник інтернет-магазину замовив DDoS-атаку на сайт свого головного конкурента в період проведення акції «Чорна п'ятниця». *Наслідок:* Сайт конкурента був недоступний 48 годин, репутаційної шкоди на суму близько 1 млн грн. (Справа що спричинило втрату прибутку

Вид атаки	Сутність та мотив	Практичний кейс та наслідки
		та завдання 2024 року, замовника засуджено до 5 років).
Атаки з метою вимагання (Ransom DDoS / RDDoS)	Зловмисник розпочинає потужну атаку, частково блокуючи роботу критичного ресурсу компанії (наприклад, платіжного шлюзу). Після цього він зв'язується з керівництвом і вимагає сплатити викуп (переважно у криптовалюті) за припинення атаки та неповторення її в майбутньому.	*Кейс:* Масована атака на сервери національної енергетичної компанії у 2023 році. Зловмисники вимагали переказ у Bitcoin за зупинку генерації сміттєвого трафіку. *Наслідок:* Тимчасова зупинка сервісів обслуговування клієнтів. (Організатора засуджено за сукупністю ст. 363-1 та ст. 189 КК України до 6 років).
Політично вмотивовані атаки (Хактивізм / Кібервійна)	Атаки, спрямовані на дестабілізацію державних інституцій, створення паніки в суспільстві або здійснення інформаційно-психологічного впливу. Часто фінансуються ворожими спецслужбами.	**CASE STUDY:** 15 лютого 2022 року, напередодні повномасштабного вторгнення РФ, була здійснена безпрецедентна за потужністю DDoS-атака на державний сектор України. Цілями стали сайти Міністерства оборони, ЗСУ, а також банківські сервіси Приват24 та Ощадбанк. Наслідком стала тимчасова недоступність послуг для мільйонів громадян і масштабна інформаційна дестабілізація. СБУ оцінило прямі збитки інфраструктурі у понад 10 млн грн.

Знаряддя вчинення кримінального правопорушення: Ботнети та Стресери

Для створення необхідного для успішної DDoS-атаки масового потоку мережевих запитів зловмисники використовують спеціалізовані інструменти. Законодавство не конкретизує їх, проте правозастосовна практика та сучасна криміналістика виділяють дві основні категорії:

Таблиця 2.10

Порівняльна характеристика інструментів для проведення DDoS-атак

Характеристика	Ботнет (Botnet)	Стресер (Booter / Stresser Service)
Технічна сутність	Мережа інфікованих цифрових пристроїв («зомбі-машин»), якими хакер керує віддалено з єдиного командного центру (C&C Server) без відома їхніх законних власників. До ботнету можуть входити комп'ютери, смартфони, роутери та IoT-пристрої.	Онлайн-сервіс, який позиціонується як легальний інструмент для стрес-тестування мереж (перевірки на стійкість до навантажень), але фактично продається кіберзлочинцям як послуга (DDoS-as-a-Service).
Сучасні (AI) тенденції	Використання алгоритмів машинного навчання (AI) для самостійного пошуку вразливих пристроїв у мережі та автоматизованого формування «рою» ботів. За звітами Kaspersky Lab, у 2025 році кількість AI-генерованих ботнетів зросла на 40 %.	Інтеграція AI-модулів для аналізу захисту цільового сайту та автоматичного підбору найбільш ефективного вектору DDoS-атаки (наприклад, перемикання між атаками на рівні застосунку L7 та мережевому рівні L3/L4).
Механізм дії	Використовує сумарні обчислювальні потужності та інтернет-канали тисяч заражених пристроїв.	Використовує орендовані надпотужні сервери самого сервісу, які генерують потік даних.
Доступність та	Створення власного	Загальнодоступний інструмент.

Характеристика	Ботнет (Botnet)	Стресер (Booter / Stresser Service)
вартість	потужного ботнету є складним технічним завданням. Оренда ботнету з сотень тисяч пристроїв у DarkNet коштує десятки тисяч доларів.	Працює за моделлю підписки через Telegram-боти або вебсайти. Вартість стартує від 50 доларів за кілька годин атаки.
Практичний кейс	У 2025 році було засуджено організатора атаки на банківську установу, який використовував AI-керований ботнет на базі модифікованого коду Mirai (вирок — 7 років позбавлення волі).	У 2024 році було винесено вирок особі, яка для атаки на сайт Міноборони придбала підписку на відомий Booter-сервіс, приховуючи свої дії за ланцюжком проксі-серверів (засуджено до 5 років).

Суб’єкт та суб’єктивна сторона

Суб’єкт кримінального правопорушення за ст. 363-1 КК України – загальний (фізична осудна особа, яка досягла 16-річного віку). Ним може бути як безпосередній виконавець (хакер), так і замовник атаки, дії якого кваліфікуються з посиланням на ст. 27 КК України (як організатора або підбурювача).

Суб’єктивна сторона має складну конструкцію вини.

Ставлення до діяння: Стосовно самої дії (умисного запуску розсилки або активації ботнету) вина характеризується виключно **прямим умислом**. Особа чітко усвідомлює, що здійснює масове розповсюдження повідомлень без згоди адресатів.

Ставлення до наслідків: Стосовно суспільно небезпечних наслідків (порушення або припинення роботи системи) вина може бути як у формі **прямого чи непрямого умислу** (замовник DDoS-атаки прямо бажає «покласти» сайт конкурента), так і у формі **необережності** (маркетолог замовляє агресивну спам-розсилку реклами, усвідомлюючи її масовість, але злочинно самовпевнено розраховує, що сервери провайдера витримають навантаження і не припинять роботу).

2.3. Кримінальна відповідальність за інші кіберзлочини (ст. ст. 163, 176, ч. 4 ст. 190, ч. 2 ст. 301, ст. ст. 301-1, 301-2 КК України)

Кримінальна відповідальність за ст. 163 КК України

Кримінальна відповідальність за порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер передбачена ст. 163 КК України, що складається з двох частин.[85]

Зокрема, відповідно до ч. 1 ст. 163 КК України кримінальна відповідальність настає за порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер; згідно з ч. 2 ст. 163 КК України – ті самі дії, вчинені повторно або щодо державних чи громадських діячів, журналіста, або вчинені службовою особою, або з використанням спеціальних засобів, призначених для негласного зняття інформації.

Таблиція 2.11

Кількість облікованих кримінальних правопорушень[86]

Назва кримінального правопорушення	2021 рік ч. 1/ч. 2	2022 рік ч. 1/ч. 2	2023 рік ч. 1/ч. 2	2024 рік ч. 1/ч. 2	2025 рік ч. 1/ч. 2
Порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер (ст. 163 КК України)	18 6/12	9 5/4	18 10/8	12 8/4	15 9/6

Безпосереднім об'єктом кримінального правопорушення, передбаченого ст. 163 КК України, є суспільні відносини в сфері охорони конституційного права громадян на таємницю листування, телефонних розмов, телеграфної чи іншої кореспонденції (ст.31 Конституції

[85] Кримінальний кодекс України : Закон України від 05.04.2001. URL : https://zakon.rada.gov.ua/laws/show/2341-14#Text.

[86] Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування. *Офіс Генерального прокурора.* URL : https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2.

України).

Предметом у цьому кримінальному правопорушенні виступає інформація (відомості), що передані або передаються в листах, під час телефонних розмов, за допомогою телеграфу чи іншими засобами зв'язку або через комп'ютер і мають особистий характер.

Не є предметом даного кримінального правопорушення інформація (відомості) службового характеру. За наявності інших елементів складу кримінального правопорушення незаконні дії з такою інформацією (відомостями) можуть кваліфікуватися за ст. 111 КК України «Державна зрада», ст. 114 КК України «Шпигунство», ст. 231 КК України «Незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю», ст. 232 КК України «Розголошення комерційної, банківської таємниці або професійної таємниці на ринках капіталу та організованих товарних ринках», ст.328 КК України «Розголошення державної таємниці», ст. 330 КК України «Передача або збирання відомостей, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни», ст. 422 КК України «Розголошення відомостей військового характеру, що становлять державну таємницю, або втрата документів чи матеріалів, що містять такі відомості».

З *об'єктивної сторони* це кримінальне правопорушення вчиняється шляхом порушення таємниці:

1) листування;
2) телефонних розмов;
3) телеграфної кореспонденції;
4) іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер.

Під порушенням таємниці слід розуміти незаконне ознайомлення з особистою інформацією (відомостями), що містяться в листах, телеграфній кореспонденції, чи іншій кореспонденції, що передається засобами зв'язку або через комп'ютер (СМС, електронна пошта тощо), підслуховування телефонних розмов, а також незаконне розголошення такої інформації (відомостей).

Так наприклад Франківським районним судом м. Львова 11.10.2021 р. у справі № 465/5121/20 було встановлено, що винний, у період часу із 17.11.2017 р. по 02.04.2018 р., з метою помсти, використовуючи електронно-обчислювальну машину, а саме системний комп'ютерний блок, діючи умисно, маючи авторизаційні дані, а саме логін та пароль доступу до облікового запису, що належить потерпілій

та знаходиться у комп'ютерній мережі «і.ua», увійшовши у нього, незаконно ознайомлювався з кореспонденцією, яка міститься в обліковому записі останньої та становить її особисту таємницю, чим порушив таємницю кореспонденції, яка передавалась потерпілою через комп'ютер. Дії винного було кваліфіковано судом за ч. 1 ст. 163 КК України[87].

Під засобами зв'язку слід розуміти технічне обладнання, яке використовується для забезпечення зв'язку.

Комп'ютер – це пристрій, який виконує логічні операції та опрацьовує дані, здатний використовувати пристрої введення та виводити інформацію на монітор і зазвичай містить центральний процесор (ЦП) для виконання операцій. За відсутності ЦП пристрій повинен виконувати функцію шлюзу клієнта до комп'ютерного серверу, який працює як блок опрацювання даних[88].

Листування – це процес обміну особистими письмовими повідомленнями між людьми, а також сукупність надісланих і отриманих листів. Він є одним із основних способів комунікації, який забезпечує передачу інформації в особистих цілях через пошту (листи, телеграми тощо) чи цифрові канали (електронна пошта, месенджери тощо).

Телефонні розмови – це спілкування людей за допомогою будь-якого телефонного зв'язку.

Телеграфна кореспонденція – це інформація, яка передається за допомогою телеграфу.

Інша кореспонденція, що передається засобами зв'язку або через комп'ютер – це інформація (відомості), що передаються іншими, крім описаних вище способами через засоби зв'язку або через комп'ютер (телетайп, телефакс, за допомогою пейджингового зв'язку тощо).

Кримінальне правопорушення вважається закінченим з моменту незаконного ознайомлення з особистою інформацією (відомостями), що містяться в листах, телеграфній кореспонденції, чи іншій кореспонденції, що передається засобами зв'язку або через комп'ютер (формальний склад).

Суб'єктом кримінального правопорушення є будь-яка фізична осудна особа, яка на момент вчинення кримінального правопорушення досягла 16-річного віку.

---

[87] Вирок Франківського районного суду м. Львова у справі № 465/5121/20 від 11.10.2021 р. URL : https://reyestr.court.gov.ua/Review/100341888.

[88] Регламент комісії (ЄС) № 617/2013 від 26 червня 2013 року про імплементацію Директиви Європейського Парламенту і Ради 2009/125/ЄС стосовно вимог до екодизайну для комп'ютерів і комп'ютерних серверів. URL : https://zakon.rada.gov.ua/laws/show/984_010-13/ed20130626#n31.

Суб'єктивна сторона кримінального правопорушення, передбаченого ст. 163 КК України, характеризується умисною формою вини у вигляді прямого умислу. Мотиви вчинення кримінального правопорушення можуть бути різноманітними (ревнощі, помста тощо) і на кваліфікацію не впливають.

Кваліфікуючими ознаками передбаченими ч. 2 ст. 163 КК України визнаються:

1. вчинення зазначених вище дій повторно;
2. щодо державних чи громадських діячів;
3. щодо журналіста;
4. службовою особою;
5. з використанням спеціальних засобів, призначених для негласного зняття інформації.

Повторністю кримінальних правопорушень визнається вчинення двох або більше кримінальних правопорушень, передбачених ст. 163 КК України.

До державного чи громадського діяча відносять Президента України, Голову Верховної Ради України, народного депутата України, Прем'єр-міністра України, члена Кабінету Міністрів України, Голови чи члена Вищої ради правосуддя, Голови чи члена Вищої кваліфікаційної комісії суддів України, Голови чи судді Конституційного Суду України або Верховного Суду, або вищих спеціалізованих судів, Генерального прокурора, Директора Національного антикорупційного бюро України, Директора Бюро економічної безпеки України, Директора Державного бюро розслідувань, Уповноваженого Верховної Ради України з прав людини, Голову або іншого члена Рахункової палати, Голову Національного банку України, керівника політичної партії[89] (ст. 112 КК України) тощо.

Журналіст – творчий працівник суб'єкта у сфері медіа, який професійно збирає, одержує, створює, редагує, поширює і забезпечує підготовку інформації для медіа. Статус журналіста підтверджується документом, виданим суб'єктом у сфері медіа, професійною чи творчою спілкою журналістів. Документ, що підтверджує статус журналіста, має містити найменування та вид медіа, його ідентифікатор у Реєстрі суб'єктів у сфері медіа або найменування професійної чи творчої спілки, фото, прізвище, ім'я та по батькові журналіста, номер документа, дату

[89] Кримінальний кодекс України : Закон України від 05.04.2001. URL : https://zakon.rada.gov.ua/laws/show/2341-14#Text.

видачі і строк його дії, підпис особи, яка видала документ[90].

Відповідно до ч. 3 та 4 ст. 18 КК України службовими особами є особи, які постійно, тимчасово чи за спеціальним повноваженням здійснюють функції представників влади чи місцевого самоврядування, а також постійно чи тимчасово обіймають в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах чи організаціях посади, пов'язані з виконанням організаційно-розпорядчих чи адміністративно-господарських функцій, або виконують такі функції за спеціальним повноваженням, яким особа наділяється повноважним органом державної влади, органом місцевого самоврядування, центральним органом державного управління із спеціальним статусом, повноважним органом чи повноважною службовою особою підприємства, установи, організації, судом або законом.

Службовими особами також визнаються посадові особи іноземних держав (особи, які обіймають посади в законодавчому, виконавчому або судовому органі іноземної держави, у тому числі присяжні засідателі, в органі місцевого самоврядування або автономному утворенні на території держави, інші особи, які здійснюють функції держави для іноземної держави, зокрема для державного, місцевого органу або державного, комунального підприємства), іноземні третейські судді, особи, уповноважені вирішувати цивільні, комерційні або трудові спори в іноземних державах у порядку, альтернативному судовому, посадові особи міжнародних організацій (працівники міжнародної організації чи будь-які інші особи, уповноважені такою організацією діяти від її імені), а також члени міжнародних парламентських асамблей, учасником яких є Україна, та судді і посадові особи міжнародних судів[91].

Так наприклад Печерським районним судом м. Києва 12.10.2015 у справі № 757/35881/15-к було встановлено, що винний з березня по червень 2015 року, будучи службовою особою співробітником правоохоронного органу, перебуваючи на посаді заступника начальника Управління контррозвідки ГУ СБ України у м. Києві та Київській області, діючи з корисливих мотивів та в інтересах невстановлених представників ВАТ «Рейлтрансхолдінг» (російська федерація), маючи умисел на незаконне ознайомлення із відомостями, які передаються засобами зв'язку та діючи з метою збору інформації щодо ПАТ «Азовмаш» та його

[90] Про державну підтримку медіа, гарантії професійної діяльності та соціальний захист журналіста: Закон України від 05.04.2001. URL : https://zakon.rada.gov.ua/laws/show/540/97-%D0%B2%D1%80#Text.

[91] Кримінальний кодекс України : Закон України від 05.04.2001. URL : https://zakon.rada.gov.ua/laws/show/2341-14#Text.

генерального директора ОСОБА_12, усвідомлюючи, що своїми діями порушує конституційне право громадян, передбачене ст. 31 Конституції України, в порушення вимог ч. 3 ст. 8 Закону України «Про оперативно-розшукову діяльність», пунктів 1.3, 1.5, 1.6, 2.4, 3.7.1, 5.6, 5.15 наказу Голови СБ України від 17.11.2014р. № 002 «Про затвердження Інструкції про порядок організації та проведення оперативно-технічних та оперативно-технічних пошукових заходів з використанням можливостей Служби безпеки України» з використанням можливостей відділу оперативно-технічних заходів ГУ СБУ у м. Києві та Київській області (далі ВОТЗ), маючи єдиний злочинний намір, вчиняв продовжуваний злочин умисно порушував таємницю телефонних розмов громадян України, не отримавши їх згоди та відповідної санкції суду на здійснення такого прослуховування. Дії винного було кваліфіковано судом за ч. 2 ст. 163 КК України[92].

Під спеціальними засобами, призначеними для негласного зняття інформації слід розуміти спеціальні технічні засоби для зняття інформації з каналів зв'язку та інші технічні засоби негласного отримання інформації. Спеціальні технічні засоби для зняття інформації з каналів зв'язку та інші технічні засоби негласного отримання інформації – технічні, апаратно-програмні, програмні та інші засоби, які відповідають критеріям належності технічних засобів негласного отримання інформації, що мають технічну забезпеченість для негласного отримання (прийому, обробки, реєстрації та/або передачі) інформації, призначені для використання у скритний спосіб, характерний для оперативно-розшукової, контррозвідувальної або розвідувальної діяльності[93]. Порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер вчинене з використанням спеціальних засобів, призначених для негласного зняття інформації кваліфікується за ч. 2 ст. 163 КК України, а якщо в діях винного є ознаки передбачені ч. 2 або 3 ст. 359 КК України їх слід кваліфікувати за сукупністю: ч. 2 ст. 163 КК України та ч. 2 або 3 ст. 359 КК України.

[92] Вирок Печерського районного суду м. Києва у справі № 757/35881/15-к від 12.10.2015 р. URL : https://zakononline.ua/court-decisions/show/52901355.

[93] Деякі питання щодо спеціальних технічних засобів для зняття інформації з каналів зв'язку та інших технічних засобів негласного отримання інформації: Постанова КМУ від 22 вересня 2016 р. № 669. URL : https://zakon.rada.gov.ua/laws/show/669-2016-%D0%BF#Text.

Кримінальна відповідальність за ст. 176 КК України.

Кримінальна відповідальність за порушення авторського права і суміжних прав передбачена ст. 176 КК України, що складається з трьох частин.[94]

Наразі відповідно до ч. 1 ст. 176 КК України кримінальна відповідальність настає за незаконне відтворення, використання та розповсюдження творів науки, літератури і мистецтва, комп'ютерних програм і баз даних, інших творів, а так само незаконне відтворення, використання та розповсюдження виконань, фонограм, відеограм і програм мовлення, їх незаконне тиражування та розповсюдження на аудіо- та відеокасетах, дискетах, інших носіях інформації, камкординг, кардшейрінг або інше умисне порушення авторського права і суміжних прав, а також фінансування таких дій, якщо це завдало матеріальної шкоди у значному розмірі; згідно з ч. 2 ст. 176 КК України – ті самі дії, якщо вони вчинені повторно, або за попередньою змовою групою осіб, або завдали матеріальної шкоди у великому розмірі; згідно з ч. 3 ст. 176 КК України – дії, передбачені частинами першою або другою цієї статті, вчинені службовою особою з використанням службового становища або організованою групою, або якщо вони завдали матеріальної шкоди в особливо великому розмірі.

Таблиція 2.12

Кількість облікованих кримінальних правопорушень[95]

Назва кримінального правопорушення	2021 рік	2022 рік	2023 рік	2024 рік	2025 рік
Порушення авторського права і суміжних прав (ст. 176 КК України)	82	31	33	13	13

Безпосереднім об'єктом кримінального правопорушення, передбаченого ст. 176 КК України, є суспільні відносини в сфері забезпечення авторського права і суміжніх прав.

Авторське право – особисті немайнові права автора і майнові права суб'єктів авторського права. Первинним суб'єктом авторського права є автор твору. Суб'єктами майнових авторських прав можуть бути також

[94] Кримінальний кодекс України : Закон України від 05.04.2001. URL : https://zakon.rada.gov.ua/laws/show/2341-14#Text.

[95] Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування. *Офіс Генерального прокурора.* URL : https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2.

інші фізичні або юридичні особи, до яких перейшли майнові права на твір на підставі правочину або закону (ст. 5 ЗУ «Про авторське право і суміжні права»)[96].

Суміжні права становлять: особисті немайнові права виконавця і майнові права на виконання; право на ім'я (найменування) виробника фонограми і майнові права на фонограму; право на ім'я (найменування) виробника відеограми і майнові права на відеограму; право на найменування організації мовлення і майнові права на програму організації мовлення (ст. 35 ЗУ «Про авторське право і суміжні права»)[97].

Потерпілим у цьому кримінальному правопорушенні виступає:

– суб'єкт авторського права (автор та його спадкоємці),

– суб'єкти суміжних прав (виконавець, спадкоємці виконавця; виробник фонограми, спадкоємці (правонаступники) виробника фонограми; виробник відеограми спадкоємці (правонаступники) виробника відеограми; організація мовлення, правонаступники організації мовлення)

– інші фізичні або юридичні особи, які набули авторських чи суміжних прав на підставі правочину, договору або закону.

Предметом цього кримінального правопорушення є твори у сфері літератури, мистецтва, науки (об'єкти авторського права) та виконання, фонограма, відеограма, програма організації мовлення (об'єкти суміжних прав).

Твір – оригінальне інтелектуальне творіння автора (співавторів) у сфері науки, літератури, мистецтва тощо, виражене в об'єктивній формі[98].

Виконання – результат індивідуальної чи колективної діяльності з артистичного представлення музичних, драматичних, літературних, хореографічних або подібних творів, фольклору чи інших художніх образів[99].

Фонограма – вироблений (кінцевий) звукозапис виконання або інших звуків, або відображень звуків, крім звукозапису, що використовується у складі аудіовізуального твору.[100]

Відеограма – вироблений (кінцевий) відеозапис виконання або інших зображень (із звуковим супроводом або без нього), крім

[96] Про авторське право і суміжні права: Закон України від 1 грудня 2022 р.. URL : https://zakon.rada.gov.ua/laws/show/2811-20#Text.

[97] Там само.

[98] Там само.

[99] Там само.

[100] Там само.

відеозапису, що використовується у складі аудіовізуального твору.[101]

Програма організації мовлення – поєднана єдиною творчою концепцією сукупність передач (телерадіопередач), інших творів та/або об'єктів суміжних прав, яка має постійну назву і транслюється радіомовником чи телемовником за певною сіткою мовлення.[102]

З *об'єктивної сторони* це кримінальне правопорушення вчиняється однією з таких альтернативних дій:

1) незаконне відтворення, використання та розповсюдження творів науки, літератури і мистецтва, комп'ютерних програм і баз даних, інших творів;

2) незаконне відтворення, використання та розповсюдження виконань, фонограм, відеограм і програм мовлення;

3) незаконне тиражування та розповсюдження на аудіо- та відеокасетах, дискетах, інших носіях інформації виконань, фонограм, відеограм і програм мовлення;

4) камкординг, кардшейрінг або інше умисне порушення авторського права і суміжних прав,

5) фінансування вищезазначених дій.

Відтворення – пряме чи опосередковане виготовлення однієї або більше копій об'єкта авторського права та/або суміжних прав (або його частини) будь-яким способом та у будь-якій формі, у тому числі для тимчасового чи постійного зберігання в електронній (цифровій), оптичній або іншій формі, яку може зчитувати комп'ютер, а також створення тривимірного твору з двовимірного і навпаки та створення тривимірного твору на основі набору інструкцій, який зчитується комп'ютером для виготовлення тривимірного твору[103].

Використання – це будь-яке введення твору або об'єкта суміжного права в господарський чи публічний обіг без згоди суб'єкта авторського права або суміжних прав.

Розповсюдження – будь-яка дія, за допомогою якої оригінали або інші примірники об'єктів авторського права та/або суміжних прав безпосередньо чи опосередковано пропонуються публіці способом, у тому числі першого продажу чи іншого першого відчуження оригіналів або інших примірників об'єкта авторського права та/або суміжних прав[104].

Так наприклад Тячівським районним судом Закарпатської області

[101] Там само.
[102] Там само.
[103] Там само.
[104] Там само.

01 жовтня 2020 р. у справі №307/838/20 було встановлено, що винний, будучи працівником приватного підприємства «Телерадіокомпанія «Данканич», в період часу з початку 2019 року по 6 листопада 2019 року, здійснюючи діяльність у сфері телевізійного мовлення, ігноруючи приписи визначені ст. 39 Закону України «Про телебачення і радіомовлення» щодо умов розповсюдження програм телерадіоорганізацій у складі універсальної програмної послуги та положень ч. 2 ст. 41 Закону України «Про авторське право і суміжні права», згідно якої майнові права організації мовлення можуть передаватися (відчужуватися) іншим способом на підставі договору, в якому визначаються спосіб і строк використання програми мовлення, розмір і порядок виплати винагороди, територія на яку розповсюджується передані права, тобто без укладання відповідного субліцензійного договору із Товариством з обмеженою відповідальністю «1+1 Інтернет» та Товариством з обмеженою відповідальністю «ТРК «Україна» про передачу прав на використання програм телеканалів, на право розповсюдження (ретрансляції) програм мовлення телеканалів в мережах на території України, переслідуючи єдиний умисел, усвідомлюючи протиправність своїх діянь, з корисливих мотивів, з метою особистого незаконного збагачення, шляхом відтворення та розповсюдження (ретрансляцію) програм мовлення, без дозволу власника, за допомогою кабельної мережі, надав клієнтам приватного підприємства «Телерадіокомпанія «Данканич» на території смт. Буштино, Тячівського району, Закарпатської області, за відповідну абонентську плату, доступ до перегляду телеканалів «1+1», «2+2», «ТЕТ», «ПлюсПлюс», «УНІАН», «Бігуді» та до програм, що виготовляються та транслюються телеканалами «ФУТБОЛ 1», «ФУТБОЛ 2», «Україна», «НЛО.TV», «Індиго tv», чим здійснив їх незаконне відтворення та розповсюдження (ретрансляцію), та завдав Товариству з обмеженою відповідальністю «1+1 Інтернет» матеріальної шкоди в розмірі 33000 гривень, яка у двадцять разів і більше перевищує встановлений на 2019 рік неоподаткований мінімум доходів громадян (960,50 гривень).

Дії винного кваліфіковані судомза ч. 1 ст. 176 КК України як незаконне відтворення та розповсюдження програм мовлення, якщо це завдало матеріальної шкоди у значному розмірі[105].

Тиражування – виготовлення одного або більше примірників твору, фонограми, відеограми чи програми мовлення у будь-якій матеріальній

[105] Вирок Тячівського районного суду Закарпатської області у справі № 307/838/20 від 01 жовтня 2020 р . URL : https://reyestr.court.gov.ua/Review/91922391.

формі без дозволу суб'єкта авторського права або суміжних прав.

Камкординг – фіксування аудіовізуального твору під час публічного демонстрування аудіовізуального твору в кінотеатрах, інших кіновидовищних закладах особами, які перебувають у тому самому приміщенні, у якому відбувається таке публічне демонстрування, для будь-яких цілей без дозволу суб'єктів авторського права або суб'єктів суміжних прав, об'єкти яких складають аудіовізуальний твір[106].

Кардшейрінг – це забезпечення у будь-якій формі та в будь-який спосіб доступу до програми організації мовлення, доступ до якої обмежено суб'єктом авторського права або суб'єктом суміжних прав шляхом застосування технологічних засобів захисту (абонентська карта, код тощо) або в інший спосіб, в обхід таких форм захисту, внаслідок чого така програма організацій мовлення може бути сприйнята публікою[107].

Інше умисне порушення авторського права і суміжних прав може полягати, зокрема в умисному порушенні майнових прав суб'єктів авторського права або суміжних прав передбачених ст.15, 39, 40 і 41 Закону України «Про авторське право і суміжні права», піратстві, плагіаті тощо.

Обов'язковими ознаками об'єктивної сторони цього кримінального правопорушення є наслідки (матеріальна шкода у значному розмірі) та причинний зв'язок (матеріальний склад).

Матеріальна шкода вважається завданою в значному розмірі, якщо її розмір у двадцять і більше разів перевищує неоподатковуваний мінімум доходів громадян[108].

Незаконне використання об'єкта права інтелектуальної власності або інше умисне порушення прав на об'єкт права інтелектуальної власності, що не завдало матеріальної шкоди у значному розмірі кваліфікується за ст.51-2 КУпАП[109].

Порушення умов і правил, що визначають порядок припинення порушень авторського права і (або) суміжних прав з використанням мережі Інтернет, у тому числі невчинення власником веб-сайту, постачальником послуг хостингу передбачених законодавством про авторське право і суміжні права дій щодо унеможливлення доступу користувачів мережі Інтернет до об'єктів авторського права і (або)

---

[106] Про авторське право і суміжні права: Закон України від 1 грудня 2022 р. URL : https://zakon.rada.gov.ua/laws/show/2811-20#Text.

[107] Там само.

[108] Кримінальний кодекс України : Закон України від 05.04.2001. URL : https://zakon.rada.gov.ua/laws/show/2341-14#Text.

[109] Кодекс України про адміністративні правопорушення від 7 грудня 1984 р. URL : https://zakon.rada.gov.ua/laws/show/8073-10#Text.

суміжних прав, ненадання або несвоєчасне надання відповіді на заяву суб'єкта авторського права і (або) суміжних прав власником веб-сайту, постачальником послуг хостингу, наведення завідомо недостовірних відомостей у відповіді на заяву суб'єкта авторського права і (або) суміжних прав, власником веб-сайту, постачальником послуг хостингу, а також нерозміщення власниками веб-сайтів, постачальниками послуг хостингу на власних веб-сайтах, в публічних базах даних записів про доменні імена (WHOIS) достовірної інформації про себе кваліфікується за ст.164-17 КУпАП[110].

Наведення особою завідомо недостовірної інформації щодо наявності авторського права і (або) суміжного права у заяві про припинення порушень авторського права і (або) суміжних прав з використанням мережі Інтернет, направленій відповідно до законодавства про авторське право і суміжні права кваліфікується за ст. 164-18 КУпАП[111].

Кримінальне правопорушення вважається закінченим з моменту настання суспільно-небезпечних наслідків у вигляді матеріальної шкоди в значному розмірі.

Суб'єктом кримінального правопорушення є будь-яка фізична, осудна особа, яка на момент його вчинення досягла 16-річного віку.

Суб'єктивна сторона кримінального правопорушення, передбаченого ст. 176 КК України, характеризується умисною формою вини у вигляді прямого умислу.

Кваліфікуючими ознаками передбаченими ч. 2 ст. 176 КК України визнаються:

– повторно;

– за попередньою змовою групою осіб:

– матеріальна шкода у великому розмірі.

Повторністю кримінальних правопорушень визнається вчинення двох або більше кримінальних правопорушень, передбачених ст.176 КК України.

Так наприклад Орджонікідзевським районним судом м. Запоріжжя 17 грудня 2014 р. у справі № 335/14157/14-к було встановлено, що винний, в червні 2014 року, точну дату в ході досудового розслідування встановити не вдалося, діючи умисно, з корисливих мотивів з метою отримання прибутку, в порушення ст. 50-53 ЗУ «Про авторське право та суміжні права», ст. 11 ЗУ «Про розповсюдження примірників аудіовізуальних творів, фонограм, відеограм, комп'ютерних програм,

[110] Там само.

[111] Там само.

баз даних», незаконно умисно порушив авторське право Дочірнього підприємства «Єврософтпром», перебуваючи у приміщенні за адресою: м. Запоріжжя, вул. Виборзька, буд. 8, вчинив незаконне відтворення на жорсткий диск ноутбука гр. ОСОБА_7 програмного забезпечення, майнові авторські права на яке належить ДП «Євсофтпром», а саме бухгалтерської комп'ютерної програми «1С: Предприятие 7.7 Сетевая версия», конфігурація – «Бухгалтерский Учет для Украины (7.70.302)», чим порушив авторські права ДП «Єврософтпром» та спричинив матеріальну шкоду правовласнику в загальній сумі 23 760 гривень та довів свій злочинний намір до кінця.

05.09.2014 року винний , діючи умисно, повторно, з корисливих мотивів з метою отримання прибутку, в порушення ст. 50-53 ЗУ «Про авторське право та суміжні права», ст. 11 ЗУ «Про розповсюдження примірників аудіовізуальних творів, фонограм, відеограм, комп'ютерних програм, баз даних», незаконно умисно порушив авторське право Дочірнього підприємства «Єврософтпром», перебуваючи у приміщенні за адресою: м. Запоріжжя, пр. Леніна, буд. 158, оф. 18, вчинив незаконне відтворення на жорсткий диск ноутбука гр. ОСОБА_8 програмного забезпечення, майнові авторські права на яке належить ДП «Євсофтпром», а саме бухгалтерської комп'ютерної програми «1С:Предприятие 7.7 Сетевая версия», конфігурація «Бухгалтерский Учет для Украины (7.70.302)», чим порушив авторські права ДП «Єврософтпром» та спричинив матеріальну шкоду правовласнику в загальній сумі 23 760 гривень та довів свій злочинний намір до кінця.

Дії винного було кваліфіковано судом за ч. 1 ст. 176 КК України та ч. 2 ст. 176 КК України – вчинене повторно[112].

Кримінальне правопорушення визнається вчиненим за попередньою змовою групою осіб, якщо його спільно вчинили декілька осіб (дві або більше), які заздалегідь, тобто до початку кримінального правопорушення, домовилися про спільне його вчинення[113].

Матеріальна шкода вважається завданою у великому розмірі – якщо її розмір у двісті і більше разів перевищує неоподатковуваний мінімум доходів громадян[114].

Особливо кваліфікуючими ознаками передбаченими ч. 3 ст. 176 КК України визнаються:

---

[112] Вирок Орджонікідзевського районного суду м. Запоріжжя у справі № 335/14157/14-к від 17 грудня 2014 р. URL : https://reyestr.court.gov.ua/Review/41961833.

[113] Кримінальний кодекс України : Закон України від 05.04.2001. URL : https://zakon.rada.gov.ua/laws/show/2341-14#Text.

[114] Там само.

– вчинення службовою особою з використанням службового становища;

– організованою групою;

– матеріальна шкода в особливо великому розмірі.

Кримінальне правопорушення визнається вчиненим організованою групою, якщо в його готуванні або вчиненні брали участь декілька осіб (три і більше), які попередньо зорганізувалися у стійке об'єднання для вчинення цього та іншого (інших) кримінальних правопорушень, об'єднаних єдиним планом з розподілом функцій учасників групи, спрямованих на досягнення цього плану, відомого всім учасникам групи[115].

Матеріальна шкода вважається завданою в особливо великому розмірі – якщо її розмір у тисячу і більше разів перевищує неоподатковуваний мінімум доходів громадян[116].

Так наприклад Радомишльським районним судом Житомирської області 15.02.2023 р. у справі № 289/2502/22-к було встановлено, що у винного, не пізніше початку 2018 року виник злочинний умисел направлений на порушення суміжних прав ТОВ «1+1 ІНТЕРНЕТ», шляхом незаконного розповсюдження програм мовлення за допомогою телекомунікаційної мережі, з використанням свого досвіду та навичок у телекомунікаційній сфері, незважаючи на те, що останній був обізнаний про те, що законне розповсюдження вказаних програм мовлення потребує дозволу правовласника ТОВ «1+1 ІНТЕРНЕТ», яке у період 2018-2023 року наділено виключними суміжними правами на розповсюдження зазначених програм, в тому числі за допомогою телекомунікаційної мережі, а також на надання невиключного суміжного права провайдерам на використання зазначених програм шляхом розповсюдження (ретрансляції).

Реалізуючи свій злочинний умисел, направлений на порушення діючого законодавства у сфері інтелектуальної власності починаючи з 01.01.2018 по у невстановлений досудовим розслідуванням час, облаштував підсобне приміщення будівлі Макарівської квартирно-експлуатаційної частини району, телекомунікаційним обладнанням з програмним забезпеченням та здійснив його налаштування, що надало можливість приймати та розповсюджувати супутникові телевізійні канали кінцевим споживачам за оплату.

Згодом, перебуваючи на території смт. Городок, Житомирського району, Житомирської області, використовуючи

[115] Там само.

[116] Там само.

власний досвід та навички у телекомунікаційній сфері, маючи необхідне обладнання та не маючи до того ж, відповідного дозволу правовласника програм «1+1», «2+2», «ТЕТ», «ПлюсПлюс», «УНІАН», «бігуді» та не уклавши обов'язкові ліцензійні договори про надання невиключного суміжного права на використання зазначених програм шляхом розповсюдження з ТОВ «1+1 ІНТЕРНЕТ», винний, діючи умисно, з метою отримання незаконного доходу, здійснив незаконне розповсюдження програм мовлення «1+1», «2+2», «ТЕТ», «ПлюсПлюс», «УНІАН», «бігуді», тобто вчинив всі необхідні дії, за допомогою яких дані об'єкти суміжних прав у період часу з 01.01.2018 по 19.05.2022 безпосередньо транслювалися абонентам смт. Городок, Житомирського району, Житомирської області, підключеним до телекомунікаційної мережі.

Тобто, винний, у порушення вимог статті 41 Конституції України, статей 426, 452 Цивільного кодексу України, вимог Законів України «Про телебачення і радіомовлення», «Про телекомунікації», «Про захист інформації в інформаційно-телекомунікаційних системах», постанови Кабінету Міністрів України від 11.04.2012 №295 «Про затвердження Правил надання та отримання телекомунікаційних послуг», а також Закону України «Про авторське і суміжні права», у період з 01.01.2018 по 19.05.2022, діючи умисно, з використанням комплексу телекомунікаційного обладнання, на платній основі, незаконно розповсюджував програми мовлення, які є об'єктами суміжних прав, жителям смт. Городок, Житомирського району, Житомирської області внаслідок чого завдав ТОВ «1+1 ІНТЕРНЕТ» матеріальної шкоди на загальну суму 1 803 580 гривень, що відповідно до примітки до ст. 176 КК України є особливо великим розміром, що у 1000 і більше разів перевищує неоподатковуваний мінімум доходів громадян.

Дії винного були кваліфіковані судом за ч. 3 ст. 176 КК України[117].

Кримінальна відповідальність за ст. ч. 4 ст. 190 КК України

Кримінальна відповідальність за шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки передбачена ч. 4 ст. 190 КК України[118].

[117] Вирок Радомишльського районного суду Житомирської області у справі № 289/2502/22-к від 15.02.2023 р. URL : https://reyestr.court.gov.ua/Review/108997544.

[118] Кримінальний кодекс України : Закон України від 05.04.2001. URL : https://zakon.rada.gov.ua/laws/show/2341-14#Text.

Таблиця 2.13

Кількість облікованих кримінальних правопорушень[119]

Назва кримінального правопорушення	2021 рік	2022 рік	2023 рік	2024 рік	2025 рік
Шахрайство (ч.ч. 2-4 ст. 190 КК України)	14760	19430	53547	44034	29696[120]

Безпосереднім об'єктом кримінального правопорушення, передбаченого ч. 4 ст. 190 КК України, є суспільні відносини в сфері охорони приватної, державної або комунальної власності.

Предметом кримінального правопорушення є чуже майно або право на майно.

Чуже майно – будь-яке майно яке має певну вартість і є чужим для винної особи: речі (рухомі й нерухомі), грошові кошти, цінні метали, цінні папери тощо[121].

Право на майно – це отримана шахраєм від потерпілого можливість володіти, користуватися або розпоряджатися майном потерпілого.

З *об'єктивної сторони* обов'язковими ознаками цього кримінального правопорушення є:

1) заволодіння чужим майном або правом на майно
2) суспільно-небезпечні наслідки у вигляді майнової шкоди
3) причинний зв'зок**.**

Заволодіння – протиправне, безоплатне обернення чужого майна або набуття права на нього на користь винної особи чи третіх осіб.

Кримінальна відповідальність настає за ст.190 КК України якщо вартість майна (майнова шкода) на момент вчинення кримінального правопорушення становить більше двох неоподатковуваних мінімумів доходів громадян.

Якщо вартість майна на момент вчинення правопорушення становить від 0,5 до двох неоподатковуваних мінімумів доходів громадян дії винного кваліфікуються за ч. 2 с. 51 КУпАП.

Обов'язкоми ознаками об'єктивної сторони ст.190 КК також є

[119] Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування. *Офіс Генерального прокурора.* URL : https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2.

[120] Наведені статистичні дані по ч.ч. 2-5 ст. 190 КК України.

[121] Постанова Пленуму Верховного Суду від 06.11.2009 № 10 «Про судову практику у справах про злочини проти власності». URL : https://zakon.rada.gov.ua/laws/show/v0010700-09#Text.

спосіб його вчинення – обман або зловживання довірою.

Обман – повідомлення потерпілому неправдивих відомостей або приховування певних обставин[122].

Зловживання довірою – недобросовісне використання довіри потерпілого[123].

Суб'єктом кримінального правопорушення є фізична осудна особа, яка досягла 16 років.

Суб'єктивна сторона кримінального правопорушення, передбаченого ст. 190 КК України, характеризується умисною формою вини у вигляді прямого умислу.

Обов'язковою ознакою суб'єктивної сторони шахрайства є також корисливий мотив.

Особливо кваліфікуючими ознаками передбаченими ч. 4 ст. 190 КК України є:

– великий розмір;

– шляхом незаконних операцій з використанням електронно-обчислювальної техніки (засіб вчинення кримінального правопорушення).

У великих розмірах визнається кримінальне правопорушення, що вчинене однією особою чи групою осіб на суму, яка в двісті п'ятдесят і більше разів перевищує неоподатковуваний мінімум доходів громадян на момент вчинення кримінального правопорушення[124].

Під незаконними операціями з використанням електронно-обчислювальної техніки як кваліфікуючою ознакою шахрайства слід розуміти такі спрямовані на заволодіння чужим майном або придбання права на майно операції, в основі яких лежать обман чи зловживання довірою. До того ж, вказану кваліфікуючу шахрайство обставину утворюють лише операції, здійснення яких без використання електронно-обчислювальної техніки є неможливим. Якщо з використанням такої техніки здійснюються операції, які цілком можуть здійснюватись за допомогою іншої техніки (наприклад, комп`ютер використовується для набору тексту, виготовлення документа тощо), то розглядуваний склад шахрайства відсутній. Електронно-обчислювальна техніка у даному випадку виступає засобом вчинення злочину, а здійснювані з використанням неї операції становлять зміст шахрайського

[122] Там само.

[123] Там само.

[124] Кримінальний кодекс України : Закон України від 05.04.2001. URL : https://zakon.rada.gov.ua/laws/show/2341-14#Text.

заволодіння чужим майном чи правом на нього[125].

Використання електронно-обчислювальної техніки для неправомірного заволодіння чужим майном утворює склад злочину, передбаченого ч. 4 ст. 190 КК України, лише тоді, коли винна особа здійснює викрадення шляхом обману чи зловживання довірою. Обман при вчиненні цього злочину може виразитись у застосуванні програмних засобів, які дають змогу винному будь-яким чином (шляхом відшукання випадкових цифр, паролів тощо) здійснити несанкціонований доступ до інформації, яка зберігається чи обробляється в автоматизованих системах, щоб ввести в оману автоматизовану систему і видати себе за того, хто має право в ній працювати і здійснювати відповідні операції (за «свого»). Проникнувши у такий спосіб до відповідної електронної системи, винний здійснює ті чи інші операції, як це робив би той, хто має на це право. До того ж, він може вплинути на процес обробки інформації, перекрутити її зміст чи знищити, задати необхідну для заволодіння майном чи правом на нього команду, налагодити систему так, щоб вона функціонувала в режимі, який би забезпечив винному або іншим особам незаконне отримання чужого майна чи права на нього. Суть шахрайського обману також залишається незмінною, з тією лише особливістю, що реалізується він за допомогою використання електронно-обчислювальної техніки, що потребує наявності відповідних знань, рівня підготовки, навичок. Зловживання довірою як спосіб шахрайства при незаконних операціях з використанням електронно-обчислювальної техніки має місце тоді, коли винна особа в результаті довірчих відносин (у зв'язку з виконанням службових обов'язків, дружніми стосунками з потерпілим тощо) має вільний доступ до здійснення відповідних операцій і недобросовісно використовує ці відносини для неправомірного заволодіння чужим майном чи правом на нього[126].

Шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки, має кваліфікуватися за частиною четвертою статті 190 КК і додаткової кваліфікації не потребує[127].

Так наприклад Святошинським районним судом м. Києва 15 червня 2023 р. у справі № 759/4752/22 було встановлено, що винна

[125] Постанова Другої судової палати Касаційного кримінального суду у справі № 752/8994/22 від 04 липня 2024 р. URL : https://iplex.com.ua/doc.php?regnum=120244099.

[126] Там само.

[127] Постанова Пленуму Верховного Суду від 06.11.2009 № 10 «Про судову практику у справах про злочини проти власності». URL : https://zakon.rada.gov.ua/laws/show/v0010700-09#Text.

04.05.2018 року знаходячись на своєму робочому місці в приміщенні офісу ТОВ «БРЕГО» вирішила заволодіти майном ТОВ «БРЕГО» код ЄДРПОУ 34296142 шляхом незаконних операцій з використанням електронно-обчислювальної техніки грошових коштів.

З метою реалізації свого злочинного умислу направленого на заволодіння майном ТОВ «БРЕГО» код ЄДРПОУ 34296142 шляхом незаконних операцій з використанням електронно-обчислювальної техніки, винна, 04.05.2018 року, перебуваючи на своєму робочому місці виконуючи покладені на неї обов'язки головного бухгалтера ТОВ «БРЕГО» код ЄДРПОУ 34296142, використовуючи попередньо отриманий нею доступ до системи «клієнт-інтернет-банк» належний ТОВ «БРЕГО» код ЄДРПОУ 34296142 виданий на ім'я ОСОБА_6, сформувала електронне платіжне доручення № 1116, яке стало підставою грошового переказу з розрахункового рахунку АТ «КРЕДОБАНК» № НОМЕР_1 належного ТОВ «БРЕГО» код ЄДРПОУ 34296142 на розрахунковий рахунок АТ «КРЕДОБАНК» № НОМЕР_2 належного ФОП ОСОБА_7 код НОМЕР_3, яка являється її донькою, на суму 9 478 грн. 48 коп. під приводом оплати за товар ТОВ «Цем-Центр», тим самим незаконно заволоділа грошовими коштами ТОВ «БРЕГО» код ЄДРПОУ 34296142 на загальну суму 9 478 грн. 48 коп. без ПДВ шляхом незаконних операцій з використанням електронно-обчислювальної техніки.

Дії винної були кваліфіковані судом за ч. 3 ст. 190 КК України, як шахрайство вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки[128].

Варто відзначити, що диспозицією ч. 4 ст. 190 КК охоплюються далеко не всі посягання на власність, пов'язані з використанням комп'ютерної техніки. Якщо винний здійснює незаконні операції з використанням ЕОТ щодо заволодіння чужим майном без використання обману або зловживання довірою (наприклад, проникає до захищеної електронної системи шляхом знищення захисних кодів), то вчинене не утворює складу злочину «шахрайство». Зокрема, якщо особа вчиняє несанкціоноване втручання в роботу автоматизованої охоронної системи підприємства з метою подальшого вчинення таємного заволодіння майном, то вчинене утворює сукупність злочинів, передбачених ст. 361 і ст. 185 КК. Так само не всі посягання, пов'язані з використанням платіжних систем і банкоматів, можуть кваліфікуватись за ч. 4 ст. 190 КК. Наприклад, достатньо поширеними

[128] Вирок Святошинського районного суду м. Києва у справі № 759/4752/22 від 15 червня 2023 р. URL : https://reyestr.court.gov.ua/Review/111561448

є випадки заволодіння готівкою, що знаходиться в банкоматі, за допомогою спеціального пристрою («виделки»). Такі дії слід розцінювати як крадіжку. Сказане стосується і випадків таємного заволодіння готівкою шляхом механічного пошкодження банкоматів за допомогою газових різаків, кутових шліфувальних машин, шляхом віджимання задніх дверцят банкоматів тощо[129].

Кримінальна відповідальність за ст. ч. 2 ст. 301 КК України.

Кримінальна відповідальність за ввезення в Україну творів, зображень або інших предметів порнографічного характеру з метою збуту чи розповсюдження або їх виготовлення, зберігання, перевезення чи інше переміщення з тією самою метою, або їх збут чи розповсюдження, а також примушування до участі в їх створенні вчинені щодо кіно- та відеопродукції, комп'ютерних програм порнографічного характеру, а також збут неповнолітнім чи розповсюдження серед них творів, зображень або інших предметів порнографічного характеру передбачена ч. 2 ст. 301 КК України[130].

Таблиця 2.14

Кількість облікованих кримінальних правопорушень[131]

Назва кримінального правопорушення	2021 рік	2022 рік	2023 рік	2024 рік	2025 рік
Ввезення, виготовлення, збут і розповсюдження порнографічних предметів (ст. 301 КК України)	1493	785	903	1647	1482

Безпосереднім об'єктом кримінального правопорушення, передбаченого ст. 301 КК України, є суспільні відносини в сфері охорони моральності, а саме з приводу поширення порнографії.

Предметом кримінального правопорушення є твори, зображення

[129] Дудоров О. О. Шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки. URL : http://dudorov.com.ua/images/download/tezy-st-190kk-eom.pdf.

[130] Кримінальний кодекс України : Закон України від 05.04.2001. URL : https://zakon.rada.gov.ua/laws/show/2341-14#Text.

[131] Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування. *Офіс Генерального прокурора*. URL : https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2.

або інші предмети порнографічного характеру.

Порнографія – вульгарно-натуралістична, цинічна, непристойна фіксація статевих актів, самоцільна, спеціальна демонстрація геніталій, антиетичних сцен статевого акту, сексуальних збочень, зарисовок з натури, які не відповідають моральним критеріям, ображають честь і гідність людини, спонукаючи негідні інстинкти[132].

З *об'єктивної сторони* це кримінальне правопорушення вчиняється однією з таких альтернативних дій щодо предметів цього кримінального правопорушення:

1) ввезення в Україну;
2) виготовлення;
3) зберігання;
4) перевезення;
5) інше переміщення;
6) збут;
7) розповсюдження;
8) примушування до участі в їх створенні.

Ввезення в Україну – це фактичне переміщення творів, зображень або інших предметів порнографічного характеру через державний кордон України. Додатково кваліфікувати за статтями, що передбачають кримінальну відповідальність за контрабанду не потрібно.

Виготовлення – створення порнографічних предметів у будь-якій формі, незалежно від способу та технічних засобів. Виготовленням визнається також копіювання або інше відтворення творів, зображень або інших предметів порнографічного характеру.

Зберігання – незаконне перебування творів, зображень або інших предметів порнографічного характеру у володінні винного.

Перевезення – це переміщення творів, зображень або інших предметів порнографічного характеру за допомогою будь-якого транспорту в межах України та за її межі.

Інше переміщення – це переміщення творів, зображень або інших предметів порнографічного характеру будь-яким іншим способом, крім перевезення, наприклад пішки, за допомогою мережі «Інтернет» тощо.

Збут – це оплатна передача творів, зображень або інших предметів порнографічного характеру іншій особі.

Розповсюдження – це безоплатна передача творів, зображень або інших предметів порнографічного характеру іншій особі (особам).

Примушування до участі в їх створенні – дії спрямовані на те, щоб

[132] Науково-практичний коментар Кримінального кодексу України/ за ред. М. І. Мельника, М. І. Хавронюка. 10-те вид., переробл. та допов. Київ: ВД «Дакор». С. 950.

інша особа проти своєї волі прийняла участь у створенні творів, зображень або інших предметів порнографічного характеру.

Кримінальне правопорушення вважається закінченим з моменту вчинення однієї з альтернативних дій (формальний склад).

Суб'єктом кримінального правопорушення є фізична осудна особа, яка досягла 16 років.

Суб'єктивна сторона кримінального правопорушення, передбаченого ст. 301 КК України, характеризується умисною формою вини у вигляді прямого умислу.

Обов'язковою ознакою суб'єктивної сторони в перших 5 формах вчинення цього кримінального правопорушення є мета: збут чи розповсюдження.

Кваліфікуючими ознаками передбаченими ч. 2 ст. 301 КК України є:

– вчинені щодо кіно- та відеопродукції, комп'ютерних програм порнографічного характеру;

– збут неповнолітнім чи розповсюдження серед них творів, зображень або інших предметів порнографічного характеру.

Неповнолітнім є фізична особа, яка не досягла 18-річного віку. Таким чином суб'єктом вчинення цього кримінального правопорушення при збуті неповнолітнім чи розповсюдження серед них творів, зображень або інших предметів порнографічного характеру є фізична осудна особа, яка досягла 18-річного віку.

Під кіно- та відеопродукцією розуміють кіно та відеофільми. Фільм – аудіовізуальний твір (у тому числі телевізійні серіали та їх окремі серії), що складається з епізодів, поєднаних між собою творчим задумом і зображувальними засобами, та є результатом спільної діяльності його авторів, виконавців і виробників[133].

Комп'ютерні програми порнографічного характеру – це програмні продукти (програми, додатки, ігри, інтерактивні сервіси), зміст або функціональне призначення яких полягає у створенні, відтворенні чи демонстрації матеріалів порнографічного характеру.

Наприклад, Збаразьким районним судом Тернопільської області 13 березня 2024 р. у справі № 598/584/24 було встановлено, що 08 січня 2024 року о 14 годині 46 хвилин, винний, реалізовуючи свій злочинний намір, спрямований на розповсюдження відеопродукції порнографічного характеру, перебуваючи за місцем свого проживання, за допомогою власного мобільного телефону моделі «MiA2 Lite» (Ь1805SG), підключився до мобільного інтернету, оператора «KYIVSTAR» та

[133] Про кінематографію: Закон України від 13 січня 1998 р. URL : https://zakon.rada.gov.ua/laws/show/9/98-%D0%B2%D1%80#Text.

увійшов в мобільний застосунок «Telegram», за допомогою якого надіслав іншій особі, два відео з найменуваннями: «JOPORN_NET_37388_4720p.mp4» та «JOPORN_NET_35944_720p.mp4» та о 15 годині 55 хвилин, відео з найменуванням «JOPORN_NET_37365_480p.mp4», які відносяться до продукції порнографічного характеру і які інша особа переглянула.

Дії винного були кваліфіковані судом за ч. 2 ст. 301 КК України[134].

Кримінальна відповідальність за ст. 301-1 КК України

Кримінальна відповідальність за одержання доступу до дитячої порнографії, її придбання, зберігання, ввезення, перевезення чи інше переміщення, виготовлення, збут і розповсюдження передбачена ст. 301-1 КК України, що складається з шести частин[135].

Зокрема, відповідно до ч. 1 ст. 301-1 КК України кримінальна відповідальність настає за умисне одержання доступу до дитячої порнографії з використанням інформаційно-телекомунікаційних систем чи технологій або умисне її придбання, або умисне зберігання, ввезення в Україну, перевезення чи інше переміщення дитячої порнографії без мети збуту чи розповсюдження; згідно з ч. 2 ст. 301-1 КК України – ввезення в Україну дитячої порнографії з метою збуту чи розповсюдження або її зберігання, перевезення чи інше переміщення з тією самою метою; згідно з ч. 3 ст. 301-1 КК України – виготовлення, розповсюдження, збут дитячої порнографії або примушування неповнолітньої особи до участі у створенні дитячої порнографії; згідно з ч. 4 ст. 301-1 КК України – дії, передбачені частинами другою або третьою цієї статті, вчинені повторно або за попередньою змовою групою осіб, або з отриманням доходу у великому розмірі, або примушування малолітньої особи до участі у створенні дитячої порнографії; ч. 5 та ч. 6 ст. 301-1 КК України передбачають умови за яких особа не підлягає кримінальній відповідальності.

[134] Вирок Збаразького районного суду Тернопільської області у справі № 598/584/24 від 13 березня 2024 р. URL : https://reyestr.court.gov.ua/Review/117633776.

[135] Кримінальний кодекс України : Закон України від 05.04.2001. URL : https://zakon.rada.gov.ua/laws/show/2341-14#Text.

Таблиця 2.15

Кількість облікованих кримінальних правопорушень[136]

Назва кримінального правопорушення	2021 рік	2022 рік	2023 рік	2024 рік	2025 рік
Одержання доступу до дитячої порнографії, її придбання, зберігання, ввезення, перевезення чи інше переміщення, виготовлення, збут і розповсюдження (ст. 301-1 КК України)	-	1095	1621	1809	1482

Безпосереднім об'єктом кримінального правопорушення, передбаченого ст. 301-1 КК України, є суспільні відносини в сфері охорони моральності, а саме з приводу протидії поширенню дитячої порнографії.

Предметом цього кримінального правопорушення є дитяча порнографія.

Відповідно до примітки ст. 156-1 КК України під дитячою порнографією в статті 301-1 цього Кодексу слід розуміти зображення у будь-який спосіб дитини чи особи, яка виглядає як дитина, у реальному чи змодельованому відверто сексуальному образі або задіяної у реальній чи змодельованій відверто сексуальній поведінці, або будь-яке зображення статевих органів дитини в сексуальних цілях[137].

З *об'єктивної сторони* це кримінальне правопорушення вчиняється однією з таких альтернативних дій:

1) одержання доступу до дитячої порнографії;
2) придбання дитячої порнографії;
3) зберігання дитячої порнографії;
4) ввезення в Україну дитячої порнографії;
5) перевезення дитячої порнографії;
6) інше переміщення дитячої порнографії.

Під одержанням доступу до дитячої порнографії розуміють

[136] Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування. Офіс Генерального прокурора. URL : https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2.

[137] Кримінальний кодекс України : Закон України від 05.04.2001. URL : https://zakon.rada.gov.ua/laws/show/2341-14#Text.

будь-які умисні дії особи, спрямовані на отримання можливості переглядати, відкривати, використовувати або іншим чином ознайомлюватися з матеріалами дитячої порнографії, незалежно від факту їх збереження чи завантаження.

Так наприклад Центральним районним судом м. Миколаєва 28 жовтня 2021 р у справі № 490/7762/21 було встановлено, що в період часу з 2019 року по 11 червня 2021 року винний, перебуваючи за місцем свого постійного проживання, використовуючи доступ до всесвітньої мережі Інтернет, який згідно договору наданий провайдером ПП «Дикий Сад» маючи умисел на одержання доступу до дитячої порнографії з метою подальшого її зберігання, без мети збуту чи розповсюдження, порушуючи суспільну мораль, тобто систему етичних норм, правил поведінки, що склалися у суспільстві на основі традиційних духовних і культурних цінностей в частині заборони поширення серед населення вульгарно-натуралістичної, цинічної, непристойної фіксації статевих актів із зображенням у будь-який спосіб дитини, всупереч Закону України «Про захист суспільної моралі» від 20.11.2003 в редакції від 17.03.2021 року, «Конвенції Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства» ратифікованої 20.06.2012 та Закону України «Про охорону дитинства» від 26.04.2001 в редакції від 17.03.2021, усвідомлюючи суспільно-небезпечний характер свого діяння, завантажив на свій персональний комп'ютер з системним блоком марки «Acer» моделі «M6 series Veritone» (серійний номер відсутній), на якому встановлено два жорстких диски, один з яких фірми виробника «Seagate» моделі «ST1000DM003-1SB1» серійний номер «Z9A1YJND» за допомогою програмного продукту «BitTorrent» 322 графічних файли та 584 відео файли на яких відображаються сцени статевих відносин відвертого порнографічного змісту, які відносяться до продукції порнографічного характеру з ознаками дитячої порнографії, які з моменту завантаження умисно зберігав на своєму комп'ютері та накопичувачі для особистого перегляду без мети збуту чи розповсюдження до тих пір, поки системний блок його персонального комп'ютеру не був вилучений працівниками поліції 11.06.2021 вході проведення санкціонованого обшуку за місцем його проживання.

Таким чином, винний вчинив кримінальне правопорушення, передбачене ч. 1 ст. 301-1 КК України, що полягає в умисному одержанні доступу до дитячої порнографії з використанням інформаційно-телекомунікаційних систем чи технологій та умисному зберіганні без

мети збуту чи розповсюдження[138].

Придбання дитячої порнографії – умисне отримання у власність або фактичне володіння матеріалами дитячої порнографії будь-яким способом (платним чи безоплатним).

Зберігання дитячої порнографії – умисні дії, які полягають у фактичному володінні матеріалів дитячої порнографії протягом певного часу, незалежно від способу їх отримання.

Ввезення в Україну дитячої порнографії – це фактичне переміщення дитячої порнографії державний кордон України. Додатково кваліфікувати за статтями, що передбачають кримінальну відповідальність за контрабанду не потрібно.

Перевезення дитячої порнографії – це переміщення дитячої порнографії за допомогою будь-якого транспорту в межах України та за її межі.

Інше переміщення дитячої порнографії – це переміщення дитячої порнографії будь-яким іншим способом, крім перевезення, наприклад пішки, за допомогою мережі «Інтернет» тощо.

Обов'язковою ознакою об'єктивної сторони у першій його формі є засіб – з використанням інформаційно-телекомунікаційних систем чи технологій.

Під інформаційно-телекомунікаційними система чи технологіями розуміють сукупність технічних засобів, програмного забезпечення та організаційних рішень, що забезпечують створення, обробку, зберігання, передачу та отримання інформації на відстані.

Слід звернути увагу, що в сучасному спеціалізованому законодавстві використовуються інші терміни, зокрема інформаційна (автоматизована) система, інформаційно-комунікаційна система.

Інформаційна (автоматизована) система – організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів[139].

Інформаційно-комунікаційна система – сукупність інформаційних та електронних комунікаційних систем, які у процесі обробки інформації діють як єдине ціле[140].

Кримінальне правопорушення вважається закінченим з моменту вчинення однієї з альтернативних дій закріплених в диспозиції статті

[138] Вирок Центрального районного суду м.Миколаєва у справі № 490/7762/21 від 28 жовтня 2021 р. URL : https://reyestr.court.gov.ua/Review/100745826.

[139] Про захист інформації в інформаційно-комунікаційних системах: Закон України від 5 липня 1994 р. URL : https://zakon.rada.gov.ua/laws/show/uk-sq/80/94-%D0%B2%D1%80#Text.

[140] Там само.

(формальний склад).

Суб'єктом кримінального правопорушення є фізична осудна особа, яка досягла 16 років.

Не підлягає кримінальній відповідальності неповнолітня особа за виготовлення, зберігання, перевезення чи інше переміщення дитячої порнографії, якщо такі дії вчинені без мети збуту чи розповсюдження[141].

Не підлягає кримінальній відповідальності за діяння, передбачені частиною першою цієї статті, особа, яка вчинила їх з метою виконання покладених на неї повноважень на підставах і в порядку, передбачених законодавством[142].

Суб'єктивна сторона кримінального правопорушення, передбаченого ст. 301-1 КК України, характеризується умисною формою вини у вигляді прямого умислу. Кримінальне правопорушення у 2-6 формах вчиняється без мети збуту чи розповсюдження.

У статті 301-1 КК України одержання доступу до дитячої порнографії з використанням інформаційно-телекомунікаційних систем або технологій слід вважати умисним, якщо доведено, що особа усвідомлювала, що у такий спосіб вона отримає доступ до дитячої порнографії (наприклад, доведено, що особа отримала такий доступ повторно або шляхом внесення плати тощо)[143].

Кримінальна відповідальність за ч. 2 ст. 301-1 КК України настає за:

1) ввезення в Україну дитячої порнографії з метою збуту чи розповсюдження;

2) зберігання дитячої порнографії з метою збуту чи розповсюдження;

3) перевезення дитячої порнографії з метою збуту чи розповсюдження;

4) інше переміщення дитячої порнографії з метою збуту чи розповсюдження.

Кримінальна відповідальність за ч. 3 ст. 301-1 КК України настає за:

1) Виготовлення дитячої порнографії;

2) розповсюдження дитячої порнографії;

3) збут дитячої порнографії;

4) примушування неповнолітньої особи до участі у створенні дитячої порнографії.

Виготовлення дитячої порнографії – створення дитячої порнографії

---

[141] Кримінальний кодекс України: Закон України від 05.04.2001. URL : https://zakon.rada.gov.ua/laws/show/2341-14#Text.

[142] Там само

[143] Там само.

у будь-якій формі, незалежно від способу та технічних засобів. Виготовленням визнається також копіювання або інше відтворення дитячої порнографії.

Так наприклад Залізничним районним судом м Львова 20 жовтня 2022 р. у справі № 462/2974/22 було встановлено, що винний 24.01.2022 о 19.08 год., перебуваючи в приміщенні квартири по АДРЕСА_2, реалізуючи свій злочинний умисел, направлений на виготовлення дитячої порнографії, скориставшись відсутністю дорослих сторонніх осіб поблизу, які могли б завадити його злочинним діям, усвідомлюючи, що поряд з ним знаходиться малолітня особа, використовуючи свій мобільний телефон Xiaomi Redmi M2006C3LG, в пластиковому чохлі-бампері чорного кольору, шляхом фотофіксації виготовив за участю малолітньої особи, фотофайл «IMG_20220124_190853», на якому остання зображена у відверто сексуальній поведінці із оголенням своїх статевих органів та фіксацією уваги на геніталіях, що належить до дитячої порнографії.

Крім цього, винний маючи умисел на зберігання дитячої порнографії за участю малолітньої особи без мети її збуту чи розповсюдження, виготовивши за допомогою свого мобільного телефону Xiaomi Redmi M2006C3LG, 24.01.2022 фотофайл «IMG_20220124_190853», що належить до дитячої порнографії, зберігав вказаний файл на своєму мобільному телефоні Xiaomi Redmi M2006C3LG, з моменту їх виготовлення до 06.02.2022.

Крім цього, винний в період часу з 24.01.2022 по 03.02.2022, перебуваючи в приміщенні квартири реалізуючи свій злочинний умисел, направлений на вчинення розпусних дій сексуального характеру, скориставшись відсутністю дорослих сторонніх осіб поблизу, які могли б завадити його злочинним діям, усвідомлюючи, що поряд з ним знаходиться малолітня особа систематично вчиняв відносно останньої розпусні дії, які полягали в оголенні винним свого статевого члена, а також фото- та відео-фіксації за допомогою мобільного телефона оголених статевих органів малолітньої особи , посягаючи також на нормальний моральний розвиток та психіку особи, яка не досягла шістнадцятирічного віку.

Дії винного були кваліфіковані судом за ч. 1 ст. 301-1 КК України, як зберігання порнографії без мети збуту чи розповсюдження, за ч. 3 ст. 301-1 КК України, як виготовлення дитячої порнографії та ч. 2 ст. 156 КК України, як вчинення розпусних дій щодо малолітньої особи[144].

[144] Вирок Залізничного районного суду м. Львова у справі № 462/2974/22 від 20 жовтня 2022 р. URL : https://reyestr.court.gov.ua/Review/106857880.

Збут дитячої порнографії – це оплатна передача дитячої порнографії.

Розповсюдження дитячої порнографії – це безоплатна передача дитячої порнографії іншій особі (особам).

Примушування неповнолітньої особи до участі у створенні дитячої порнографії – дії спрямовані на те, щоб неповнолітня особа проти своєї волі прийняла участь у створенні дитячої порнографії.

Кваліфікуючими ознаками передбаченими ч. 4 ст. 301-1 КК України є дії, передбачені частинами другою або третьою ст. 301-1 КК України, вчинені:

- повторно;
- за попередньою змовою групою осіб;
- з отриманням доходу у великому розмірі;
- примушування малолітньої особи до участі у створенні дитячої порнографії.

Для цілей статті 301-1 КК України отримання доходу у великому розмірі має місце, коли його сума у двісті і більше разів перевищує неоподатковуваний мінімум доходів громадян[145].

Малолітня особа – це фізична особа, яка не досягла 14-річного віку.

Так наприклад Залізничним районним судом м Львова 20 жовтня 2022 р. у справі № 462/2974/22 було встановлено, що винний 01.02.2022 в період часу з 20.01 год. до 20.32 год., перебуваючи в приміщенні квартири, реалізуючи свій злочинний умисел, направлений на повторне виготовлення дитячої порнографії, скориставшись відсутністю дорослих сторонніх осіб поблизу, які могли б завадити його злочинним діям, усвідомлюючи, що поряд з ним знаходиться малолітня особа, використовуючи свій мобільний телефон Xiaomi Redmi M2006C3LG, шляхом фотофіксації виготовив за участю малолітньої особи фотофайли «IMG_20220102_200156», «IMG_20220102_200413», «IMG_20220102_200416», «IMG_20220102_200727», IMG_20220102_200730», на яких остання зображена у відверто сексуальній поведінці із зображенням своїх статевих органів та фіксацією уваги на геніталіях, а також шляхом відео-зйомки виготовив за участю малолітньої особи відео-файли «VID_20220201_200843», «VID_20220201_201031», «VID_20220201_201229», «VID_20220201_202810», «VID_20220201_203137», на яких остання задіяна в реальній відверто сексуальній поведінці з оголенням статевих органів та фіксацією уваги

[145] Кримінальний кодекс України: Закон України від 05.04.2001. URL : https://zakon.rada.gov.ua/laws/show/2341-14#Text.

на геніталіях, із самоцільною демонстрацією статевих органів в еротичному контексті, що належать до дитячої порнографії.

Дії винного були кваліфіковані судом за ч. 4 ст. 301-1 КК України, як виготовлення дитячої порнографії, вчинене повторно[146].

Кримінальна відповідальність за ст. 301-2 КК України.

Кримінальна відповідальність за проведення видовищного заходу сексуального характеру за участю неповнолітньої особи передбачена ст. 301-2 КК України, що складається з чотирьох частин.[147]

Зокрема, відповідно до ч. 1 ст. 301-2 КК України кримінальна відповідальність настає за проведення видовищного заходу сексуального характеру, у тому числі з використанням інформаційно-телекомунікаційних систем або технологій, у якому задіяно неповнолітню особу; згідно з ч. 2 ст. 301-2 КК України – відвідування видовищного заходу сексуального характеру з метою його перегляду, у тому числі з використанням інформаційно-телекомунікаційних систем або технологій, у якому завідомо для відвідувача задіяно малолітню чи неповнолітню особу; згідно з ч. 3 ст. 301-2 КК України – втягнення неповнолітньої особи до участі у видовищному заході сексуального характеру, що проходить, у тому числі з використанням інформаційно-телекомунікаційних систем або технологій, або примушування неповнолітньої особи до участі у такому заході з використанням обману, шантажу, уразливого стану особи або із застосуванням чи погрозою застосування насильства; згідно з ч. 4 ст. 301-2 КК України – дії, передбачені частиною третьою цієї статті, вчинені стосовно малолітньої особи.

[146] Вирок Залізничного районного суду м Львова у справі № 462/2974/22 від 20 жовтня 2022 р. URL : https://reyestr.court.gov.ua/Review/106857880.

[147] Кримінальний кодекс України : Закон України від 05.04.2001. URL : https://zakon.rada.gov.ua/laws/show/2341-14#Text.

Таблиція 2.16

Кількість облікованих кримінальних правопорушень[148]

Назва кримінального правопорушення	2021 рік	2022 рік	2023 рік	2024 рік	2025 рік
Проведення видовищного заходу сексуального характеру за участю неповнолітньої особи (ст. 301-2 КК України)	-	0	0	0	0

Безпосереднім об'єктом кримінального правопорушення, передбаченого ст. 301-2 КК України, є суспільні відносини в сфері захисту моральності суспільства. *Безпосереднім додатковим об'єктом* виступає нормальний фізичний та психічний розвиток неповнолітніх осіб.

Потерпілим у цьому кримінальному правопорушенні виступає неповнолітня особа.

З *об'єктивної сторони* це кримінальне правопорушення вчиняється шляхом проведення видовищного заходу сексуального характеру, у тому числі з використанням інформаційно-телекомунікаційних систем або технологій.

Під видовищним заходом сексуального характеру у цій статті слід розуміти публічний показ у будь-якій формі продукції сексуального характеру або сценічні дії, метою яких є втілення сексуальних дій[149].

Наприклад, Вінницьким міським судом Вінницької області 30 грудня 2022 р у справі № 127/28630/22 було встановлено, що винна дізнавшись про існування у мережі Інтернет веб-сайтів, на яких користувачі зі всього світу за допомогою комп`ютерної техніки з веб-камерами задовольняють свої статеві пристрасті шляхом віртуального спілкування з дівчатами, на вимогу оголюють своє тіло в режимі реального часу та за демонстрування сексуальних дій здійснюють оплату грошовими коштами, котрі зараховуються на особистий рахунок на сайті, маючи корисливий мотив, з метою власного незаконного збагачення, організувала проведення видовищних заходів

[148] Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування. *Офіс Генерального прокурора.* URL : https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2.

[149] Кримінальний кодекс України : Закон України від 05.04.2001. URL : https://zakon.rada.gov.ua/laws/show/2341-14#Text.

сексуального характеру з використанням інформаційно-телекомунікаційних систем, задіявши до їх проведення неповнолітніх осіб. Неповнолітні «моделі» приходили у створений винною «Веб-інтим-колл центр», що за адресою: м. Вінниця, вул. Театральна, 1, де використовуючи інформаційно-телекомунікаційні системи – ноутбуки, обладнані веб-камерами, авторизувалися на сайтах і в режимі он-лайн спілкувалися з користувачами цих сайтів, на їх побажання оголялися, здійснювали маніпуляції зі статевими органами, тобто вчиняли сценічні дії, метою яких є втілення сексуальних дій. Дії винної були кваліфіковані судом за ч. 1 ст. 301-2 КК України[150].

Кримінальне правопорушення вважається закінченим з моменту проведення видовищного заходу сексуального характеру (формальний склад).

Суб'єктом кримінального правопорушення є фізична осудна особа з 16 років.

Суб'єктивна сторона кримінального правопорушення, передбаченого ст. 301-2 КК України, характеризується умисною формою вини у вигляді прямого умислу. Винний усвідомлює, що проводить видовищний захід сексуального характеру, і бажає цього.

Кримінальна відповідальність за ч. 2 ст. 301-2 КК України настає за відвідування видовищного заходу сексуального характеру з метою його перегляду.

Під відвідуванням розуміють присутність особи як глядача (спостерігача) на заході сексуального характеру з метою його перегляду чи сприйняття. Це може бути перебування у місці проведення такого заходу (клуб, приміщення тощо); перегляд у режимі онлайн (стримінг, трансляція) тощо. До того ж, цьому обов'язково відвідувач такого заходу повинен завідомо знати, що в ньому задіяно малолітню чи неповнолітню особу.

Кримінальна відповідальність за ч. 3 ст. 301-2 КК України настає за вчинення таких альтернативних дій:

1) втягнення неповнолітньої особи до участі у видовищному заході сексуального характеру;

2) примушування неповнолітньої особи до участі у такому заході з використанням обману, шантажу, уразливого стану особи або із застосуванням чи погрозою застосування насильства.

Обман – уведення неповнолітньої особи в оману шляхом повідомлення неправдивих відомостей або умисного приховування істини з метою спонукати її до певної поведінки.

[150] Вирок Вінницького міського суду Вінницької області у справі № 127/28630/22 від 30 грудня 2022 р. URL : https://reyestr.court.gov.ua/Review/108244485.

Шантаж – погроза розголошення відомостей (справжніх або вигаданих), які особа бажає зберегти в таємниці, з метою примусити її до певної поведінки

Під уразливим станом особи слід розуміти зумовлений фізичними чи психічними властивостями або зовнішніми обставинами стан неповнолітньої особи, який позбавляє або обмежує її здатність усвідомлювати свої дії (бездіяльність) або керувати ними, приймати за своєю волею самостійні рішення, чинити опір насильницьким чи іншим незаконним діям, збіг тяжких особистих, сімейних або інших обставин[151].

Кваліфікуючими ознаками передбаченими ч. 4 ст. 301-2 КК України є дії передбачені ч. 3 ст. 301-2 КК України вчинені стосовно малолітньої особи.

Контрольні питання до розділу 2:

1. Що означає імплементація норм міжнародного права у сфері запобігання кіберзлочинності?
2. Які міжнародно-правові акти є основою протидії кіберзлочинності?
3. Яке значення має Будапештська конвенція про кіберзлочинність?
4. Які суспільні відносини охороняються нормами розділу XVI Особливої частини КК України?
5. У чому полягає об’єктивна сторона кримінального правопорушення, передбаченого ст. 361 КК України?
6. Які форми несанкціонованого втручання охоплюються ст. 361-1 КК України?
7. листування (ст. 163 КК України)?
8. Які особливості кваліфікації порушення авторського права і суміжних прав у кіберпросторі (ст. 176 КК України)?
9. У чому полягає специфіка шахрайства, вчиненого з використанням електронно-обчислювальної техніки (ч. 4 ст. 190 КК України)?
10. Які особливості має розповсюдження порнографічного контенту через мережу Інтернет?

[151] Кримінальний кодекс України: Закон України від 05.04.2001. URL : https://zakon.rada.gov.ua/laws/show/2341-14#Text.

Розділ 3
ІНШІ ЗАХОДИ ЗАПОБІГАННЯ КІБЕРЗЛОЧИННОСТІ

3.1. Спеціально-кримінологічні заходи запобігання кіберзлочинності

Переходячи до розгляду спеціально-кримінологічних заходів запобігання кібірзлочинності, які мають антикриміногенну спрямованість, варто наголосити, що саме цілеспрямованість на виявлення та усунення (блокування, нейтралізацію) причин, умов, інших детермінант злочинів є їхньою профілюючою, констатуючою ознакою та головною особливістю[152].

У свою чергу, ефективність спеціально-кримінологічних заходів запобігання кіберзлочинності безпосередньо залежить від того, наскільки точно вони враховують специфічні особливості її детермінації.

Насамперед слід зауважити, що першим комплексним нормативно-правовим актом, який заклав правові та організаційні основи захисту життєво важливих інтересів людини і громадянина, суспільства та держави, а також національних інтересів України в кіберпросторі; ключові цілі, напрями й принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, посадових осіб і громадян у цій сфері та основи координації їхньої діяльності щодо забезпечення кібербезпеки, став Закон України «Про основні засади забезпечення кібербезпеки України» (2017 р.).

Зокрема, відповідно до ст. 4 цього Закону об’єктами кібербезпеки є:

1) конституційні права і свободи людини і громадянина;

2) суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища;

3) держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність;

4) національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави;

[152] Бандурка О. М., Литвинов О. М. Протидія злочинності та профілактика злочинів : монографія. Харків : ХНУВС, 2011. 308 с. С. 54.

5) об'єкти критичної інфраструктури[153].

У свою чергу, об'єктами кіберзахисту є:

1) інформаційні, електронні комунікаційні та інформаційно-комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону;

2) об'єкти критичної інформаційної інфраструктури;

3) інформаційні, електронні комунікаційні та інформаційно-комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу[154].

Також на законодавчому рівні було визначено національну систему суб'єктів забезпечення кібербезпеки та визначено їхні функції.

Координацію їхньої діяльності здійснює Президент України через очолювану ним Раду національної безпеки і оборони України.

Для здійснення координації та загального контролю за діяльністю суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку, а також загальної координації суб'єктів національної системи реагування на кіберінциденти, кібератаки, кіберзагрози було створено Національний координаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони України та системоутворюючий елемент всієї системи кібербезпеки та кіберзахисту України.

Зокрема, Національний координаційний центр кібербезпеки (далі – Центр) , який було утворено відповідно до рішення РНБО України від 27 січня 2016 року «Про Стратегію кібербезпеки України», уведеного в дію Указом Президента України від 15 березня 2016 року № 96, здійснює аналіз стану кібербезпеки, даних про кіберінциденти стосовно державних інформаційних ресурсів в інформаційно-телекомунікаційних системах; стану забезпечення кадрами національної системи кібербезпеки та підготовка пропозицій щодо її удосконалення; прогнозування та виявлення потенційних та реальних загроз у сфері кібербезпеки України.

До того ж, завданням Центру є розроблення концептуальних засад

---

[153] Про основні засади забезпечення кібербезпеки України : Закон України від 05 жовт. 2017р. Верховна Рада України : веб-сайт. URL : https://zakon.rada.gov.ua/laws/show/2163-19#Text.

[154] Про основні засади забезпечення кібербезпеки України : Закон України від 05 жовт. 2017р. Верховна Рада України : веб-сайт. URL : https://zakon.rada.gov.ua/laws/show/2163-19#Text.

та пропозицій щодо забезпечення кібербезпеки держави, спрямованих на підвищення ефективності заходів щодо виявлення і усунення чинників, які формують потенційні та реальні загрози у сфері кібербезпеки, підготовка проектів відповідних програм та планів щодо їх попередження та нейтралізації тощо[155].

Як позитив слід підкреслити впровадження стратегічного планування кримінологічної діяльності уповноважених суб'єктів щодо запобігання кіберзлочинності на загальнодержавному рівні. Зокрема, першу Стратегію кібербезпеки України, яка стала важливим етапом у розбудові ефективної системи кібербезпеки, було затверджено Указом Президента України 15 березня 2016 року[156]. За роки її реалізації докладено зусиль до становлення та розвитку національної системи кібербезпеки, а саме:

– удосконалено нормативне забезпечення з питань кіберзахисту об'єктів критичної інформаційної інфраструктури, ухвалено порядок її визначення та загальні вимоги до її кіберзахисту;

– утворено центри (підрозділи) забезпечення кібербезпеки або кіберзахисту в Державній службі спеціального зв'язку та захисту інформації України, Службі безпеки України, Національному банку України, Міністерстві інфраструктури України, Міністерстві оборони України, Збройних Силах України.

– розбудовується Національна телекомунікаційна мережа, утворюється Національний центр резервування державних інформаційних ресурсів, забезпечується функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки, діє урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA ;

– встановлено вимоги до захисту об'єктів критичної інфраструктури, включаючи запровадження системи аудиту інформаційної безпеки та ін.

Наразі відповідно до результатів експертних оцінок стан її практичної реалізації уповноваженими суб'єктами виявився недостатньо неефективним, оскільки не перевищував 40 відсотків. Таким чином, надзвичайно важливі для розвитку національної системи кібербезпеки завдання не були виконані, зокрема:

[155] Про Національний координаційний центр кібербезпеки Указ Президента України від 7 червня 2016 року №242/2016. URL : https://www.president.gov.ua/documents/2422016-20141.

[156] Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : Указ Президента України від 15.03.2016 р. № 96/2016. URL : https://www.president.gov.ua/documents/962016-19836.

– не сформовано перелік об'єктів критичної інформаційної інфраструктури;

– не створено модель державно-приватного партнерства;

– розвиток цифрової грамотності здійснювався без чіткої програми;

– кібернавчання проводились епізодично[157].

Проте отриманий досвід реалізації заходів попередньої Стратегії надав можливість виокремити низку системних проблем, скоординувати кримінологічну діяльність уповноважених суб'єктів і віповідні заходи запобігання кіберзлочинності у новому стратегічному документі.

Нова Стратегія кібербезпеки України враховує попередній досвід і проблеми, стан кібербезпекового середовища на національному та міжнародному рівні, а також положення Стратегії кібербезпеки ЄС на цифрове десятиліття, стратегій кібербезпеки окремих держав – членів ЄС та держав – членів НАТО[158].

У свою чергу, новими стратегічними цілями забезпечення кібербезпеки України стали:

– дієва кібероборона;

– ефективна протидія розвідувально-підривній діяльності у кіберпросторі та кібертероризму;

– ефективна протидія кіберзлочинності;

– розвиток асиметричних інструментів стримування[159].

Відповідно до Стратегії кібербезпеки України «Безпечний кіберпростір – запорука успішного розвитку країни» розбудова національної системи кібербезпеки на засадах стримування, кіберстійкості та взаємодії має здійснюватися шляхом виконання стратегічних завдань, спрямованих на досягнення визначених цілей, основними з яких є наступні:

– *утворення у системі Міністерства оборони України кібервійськ та забезпечення їх належними фінансовими, кадровими та технічними ресурсами для стримування збройної агресії у кіберпросторі та надання відсічі агресору*. На сьогодні Верховна Рада України прийняла за основу проєкт Закону «Про Кіберсили Збройних Сил України (реєстр. №12349)», метою якого є створення військової та технічної організаційної

[157] Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 р. № 447/2021. URL : https://zakon.rada.gov.ua/laws/show/447/2021#Tex.

[158] Там само

[159] Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 р. № 447/2021. URL : https://zakon.rada.gov.ua/laws/show/447/2021#Tex.

структури у складі Збройних Сил України за стандартами НАТО, яка відповідатиме за кібероборону України, захист її суверенітету та територіальної цілісності в кіберпросторі. Зокрема, основними завданнями цього нового органу військового управління будуть нарощування та ефективне застосування спроможностей кіберстримування, здобуття Збройними Силами України військової переваги над противником та послаблення його спроможностей шляхом проведення операцій в електромагнітному спектрі та кіберпросторі. Кіберсили Збройних Сил України діятимуть під безпосереднім керівництвом Головнокомандувача Збройних Сил України, а їхню політичну діяльність координуватиме Верховний Головнокомандувач – Президент України[160].

Відповідно до зазначеного законопроєкту Кіберсили Збройних Сил України пропонується створити як органом військового управління, який буде мати можливість залучати до свого складу цивільну складову (кіберрезервістів) на період проведення відповідних заходів з кіберстримування. Кіберрезервісти – це підготовлений людський ресурс, що утворений з громадян України, які мають необхідні знання, фахову підготовку та навички для планування і виконання окремих завдань кібероборони, готовий для оперативного залучення до складу Кіберсил Збройних Сил України. На відміну від призовників, військовозобов'язаних та резервістів, статус кіберрезервіста не передбачає обов'язкового набуття ним статуту військовослужбовця для залучення до лав Кіберсил Збройних Сил України, може носити періодичний та тимчасових характер, ґрунтується на певних особистих навичках особи в певній галузі та її мотивації для захисту Вітчизни, незалежності та територіальної цілісності України. Кіберсили Збройних Сил України будуть організовувати періодичне навчання та злагодженість кіберрезервістів для формування сталого кадрового інтелектуального потенціалу вмотивованих громадян України[161];

– *запровадження ефективних механізмів взаємодії основних суб'єктів національної системи кібербезпеки та сил оборони в частині спільного виконання завдань кібероборони*. Основним нормативно-правовим актом станом на початок 2026 року, що регулює зазначений механізм є Постанова Кабінету Міністрів України від 13 листопада

[160] Верховна Рада України підтримала створення нового органу військового управління – Кіберсили Збройних Сил України. URL : https://www.rada.gov.ua/news/razom/266780.html.

[161] Пояснювальна записка до проєкту Закону України «Про Кіберсили Збройних Сил України». С. 3. URL : https://itd.rada.gov.ua/7182191a-6958-4d49-a0ac-276d693dc8dd.

2025 р. № 1471 «Про затвердження Порядку взаємодії суб'єктів національної системи реагування на кіберінциденти, кібератаки, кіберзагрози із суб'єктами забезпечення кібербезпеки, правоохоронними, контррозвідувальними, розвідувальними органами та суб'єктами оперативно-розшукової діяльності»[162], відповідно до якої зазначені суб'єкти здійснюють взаємодію в межах функціонування міжвідомчих груп із реагування на кіберінциденти, кібератаки, кіберзагрози або кризову ситуацію у сфері кібербезпеки, зокрема в межах постійно діючої Об'єднаної групи реагування на кіберінциденти, кібератаки, кіберзагрози. Крім цього, зазначений документ регламентує спільні дії уповноважених суб'єктів забезпечення кібербезпеки щодо локалізації та нейтралізації кіберінцидентів. Встановлено чіткі процедури швидкого обміну інформацією про кіберзагрози між суб'єктами, що дозволяє силам оборони отримувати дані в реальному часі. Також зазначений Порядок охоплює організаційні, технічні та правові заходи щодо захисту критичної інфраструктури, що, відповідно до Закону України «Про основні засади забезпечення кібербезпеки України», є частиною кібероборони. Крім зазначеного, Постановою КМУ № 1533 від 26.11.2025 було затверджено Національний план реагування на кіберінциденти, кібератаки та кіберзагрози[163], що деталізував механізми взаємодії зазначених суб'єктів.

Зокрема, реагування на кіберінциденти, кібератаки та кіберзагрози розпочинається з етапу підготовки, під час якого суб'єктами національної системи реагування та суб'єктами забезпечення кібербезпеки проводяться заходи з вивчення та дослідження існуючих видів кіберінцидентів, кібератак та кіберзагроз, розроблення методів і механізму запобігання та протидії можливим кіберінцидентам та кібератакам.

На етапі виявлення, аналізу та інформування суб'єкти національної системи реагування та суб'єкти забезпечення кібербезпеки проводять постійний моніторинг систем, збір інформації про події кібербезпеки, що можуть свідчити про наявність кіберінциденту, кібератаки, проводять підтвердження та первинну обробку таких подій, виявлення індикаторів

[162] Про затвердження Порядку взаємодії суб'єктів національної системи реагування на кіберінциденти, кібератаки, кіберзагрози із суб'єктами забезпечення кібербезпеки, правоохоронними, контррозвідувальними, розвідувальними органами та суб'єктами оперативно-розшукової діяльності : Постанова Кабінету Міністрів України від 13 листопада 2025 р. № 1471. URL : https://zakon.rada.gov.ua/laws/show/1471-2025-%D0%BF#Text.

[163] Національний план реагування на кіберінциденти, кібератаки та кіберзагрози URL : https://zakon.rada.gov.ua/laws/show/1533-2025-%D0%BF#Text.

компрометації та підозрілої активності, ідентифікують та аналізують кіберзагрози, а також здійснюють інформування про кіберінциденти, кібератаки та кіберзагрози.

Наразі під час етапу стримування, усунення наслідків та відновлення суб'єкти забезпечення кібербезпеки самостійно або разом із суб'єктами національної системи реагування вживають заходів до зниження негативного впливу кіберінциденту, кібератаки, запобігання порушенню безпеки, несанкціонованому втручанню в їх роботу, забезпечення сталого, надійного та штатного режиму функціонування систем, захищеності (конфіденційності, цілісності і доступності) інформації та даних, що у них обробляються.

Під час етапу проведення аналізу ефективності реагування на кіберінциденти, кібератаки або кіберзагрози забезпечується документування інциденту шляхом формування звіту про реагування на кіберінцидент, кібератаку або кіберзагрозу, інформування національної команди реагування на кіберінциденти, кібератаки, кіберзагрози (CERT-UA) та Ситуаційного центру забезпечення кібербезпеки СБУ або відповідну галузеву/регіональну команду реагування на кіберінциденти, кібератаки, кіберзагрози (CSIRT) відповідно до порядку обміну інформацією, удосконалення захисних механізмів систем і мереж, перегляд внутрішньої документації та політик безпеки для запобігання подібним інцидентам у майбутньому, а також застосування набутого досвіду для покращення управління майбутніми кіберінцидентами, кібератаками або кіберзагрозами[164].

Таким чином, взаємодія в межах функціонування міжвідомчих груп передбачає: обмін інформацією, технічними даними та результатами досліджень щодо кіберінцидентів, кібератак, кіберзагроз; узгодження та координацію дій з локалізації та нейтралізації кіберінцидентів та кібератак, усунення їх наслідків; визначення необхідності залучення додаткових ресурсів (фінансових, матеріально-технічних, людських тощо) суб'єктів національної системи реагування або міжнародних партнерів та ін.

– *розроблення та виконання плану кібероборони як складової частини плану оборони України,* який є складовою загального плану оборони України, спрямованою на відбиття воєнної агресії у кіберпросторі. Цей процес передбачає координацію зусиль Генштабу, Міноборони, Держспецзв'язку та інших органів для захисту критичної інфраструктури, оцінку спроможностей та спільні навчання, зокрема за стандартами НАТО. Станом на кінець квітня 2026 р. уряд України активно реалізує заходи, передбачені Планом на 2025 рік з реалізації

[164] Національний план реагування на кіберінциденти, кібератаки та кіберзагрози. URL : https://zakon.rada.gov.ua/laws/show/1533-2025-%D0%BF#Text.

Стратегії кібербезпеки України, затверджені розпорядженням КМУ № 204-р від 7 березня 2025 року, що спрямовані на посилення кіберзахисту[165]. Цей план фокусується на зміцненні захисту критичної інфраструктури, підвищенні спроможностей СБУ, ЗСУ та інших держустанов протидіяти сучасним кіберзагрозам.

– *проведення щонайменше двічі на рік спільних тематичних навчань із відповідними підрозділами держав – членів НАТО задля досягнення оперативної сумісності*;. Так, наприклад, Україна стала однією з 7 країн-партнерів (разом із Грузією, Ірландією, Японією, Південною Кореєю, Швейцарією та Австрією), що брали участь у навчаннях «Кіберкоаліція 2025», які проходили з 28 листопада по 4 грудня 2025 року в Таллінні (Естонія) для захисту мереж від складних кібератак. Навчання «Кіберкоаліція» – це флагманські навчання НАТО з кіберзахисту та одні з найбільших у своєму роді[166].

– *створення MIL.CERT-UA в інтересах Міністерства оборони України та Збройних Сил України*, налагодивши на постійній основі співпрацю із європейською військовою CERT-мережею. Принагідно зауважимо, що «MIL.CERT-UA» – Центр кіберзахисту – спеціалізований підрозділ реагування на комп'ютерні інциденти вже створено в системі Міністерства оборони України у 2024 році. Діяльність Центру спрямована на забезпечення належного рівня кіберзахисту, своєчасне виявлення, аналіз та реагування на кіберінциденти в інформаційно-комунікаційних системах Міністерства оборони України. Головними завданнями Центру реагування на кіберінциденти є: реагування на кіберінциденти і кібератаки, усунення їхніх наслідків; вжиття заходів кіберзахисту інформаційно-комунікаційних систем Міністерства оборони; впровадження й використання систем управління інцидентами кібербезпеки і обміну інформацією про кіберзагрози; взаємодія з підрозділами суб'єктів національної системи кібербезпеки і Сил оборони в частині спільного виконання завдань; організація і проведення практичних навчань у сфері кібербезпеки; співпраця із НАТО та іншими суб'єктами оборонної сфери щодо безпеки кіберпростору і спільного захисту від кіберзагроз[167].

---

[165] План заходів на 2025 рік з реалізації Стратегії кібербезпеки України, затвердж. розпорядженням КМУ № 204-р від 7 березня 2025 року URL : https://zakon.rada.gov.ua/laws/show/204-2025-%D1%80#Text.

[166] Exercise Cyber Coalition, NATO's flagship Cyber Defence exercise, concludes in Estonia. URL : https://shape.nato.int/news-archive/2025/exercise-cyber-coalition--natos-flagship-cyber-defence-exercise--concludes-in-estonia.

[167] Атаки хакерів на Міноборони відбиватиме новостворений Центр реагування на кіберінциденти URL : https://mod.gov.ua/news/ataki-hakeriv-na-minoboroni-vidbivatime-novostvorenij-czentr-reaguvannya-na-kiberinczidenti.

– *запровадження у системі військово-патріотичного виховання та системі територіальної оборони навчальних програм підготовки та проведення практичних навчань у сфері кібербезпеки*. Зокрема, наприклад, запроваджуються Проєкт CyberTeens (спеціалізований онлайн-проєкт для школярів, спрямований на підвищення цифрової обізнаності); інтерактивних інструментів (квест «Гієна Гігієна й МереЖах») для моделювання реальних кіберзагроз у школах; безкоштовне навчання з кібербезпеки для людей з інвалідністю «CyberBee» та ін.

– *удосконалення аналітичного і криміналістичного забезпечення контррозвідувального захисту кібербезпеки держави за рахунок впровадження інноваційних методик обробки та оцінки цифрових даних, формування електронних доказів*. Наприклад, Державна служба спецзв'язку затвердила рекомендації з кіберзахисту інформаційно-комунікаційних систем (ІКС), які використовують технології штучного інтелекту (ШІ). В рекомендаціях розглядаються такі ключові вектори загроз: атаки на ланцюги постачання технологій ШІ (компрометація ПЗ, апаратного забезпечення або API); «отруєння» даних та моделей ШІ (навмисне внесення спотворених даних до навчальної вибірки для погіршення роботи системи); змагальні атаки (створення спеціальних вхідних даних для провокування помилкових рішень ШІ); атаки типу «промпт-ін'єкція» (введення маніпулятивних запитів для обходу механізмів захисту та витоку даних); інверсія та крадіжка моделі ШІ (отримання несанкціонованого доступу до внутрішньої структури, навчальних даних або створення копій моделі). Також в рекомендаціях наголошується на необхідності інтеграції управління ризиками ШІ у загальну систему кібербезпеки організацій з використанням передових міжнародних стандартів, таких як ISO/IEC 23894:2023, ISO/IEC 42001:2023 та профільних фреймворків NIST. Використання цих рекомендацій допоможе українським установам та організаціям безпечно інтегрувати інноваційні технології, уникаючи специфічних вразливостей та захищаючи критично важливі дані від новітніх векторів кібератак[168]. У сфері криміналістичного забезпечення кібербезпеки Україна впровадила нові методики роботи з цифровими слідами, які відповідають стандартам ЄС (зокрема директиві NIS2) та фокусуються на швидкості реагування, хмарних технологіях та автоматизації.

– *створення технологічних можливостей для автоматичного*

[168] Держспецзв'язку затвердила рекомендації з кіберзахисту систем, які використовують штучний інтелект. URL : https://www.kmu.gov.ua/news/derzhspetszviazku-zatverdyla-rekomendatsii-z-kiberzakhystu-system-iaki-vykorystovuiut-shtuchnyi-intelekt.

виявлення кібератак у режимі реального часу в потоках даних загальнодержавних інформаційно-комунікаційних систем та на окремих об'єктах критичної інфраструктури, їх блокування та визначення пріоритетності. На виконання цього завдання в Україні було впроваджено комплекс технічних та нормативних рішень, які відповідають логіці «активного кіберзахисту» та вимогам NIS2 щодо автоматизації безпеки. Зокрема, впроваджується Національної системи сенсорів (IDS/IPS), яка є ключовим компонентом ешелонованої системи кіберзахисту України, що активно розвивається Держспецзв'язку разом із СБУ та іншими суб'єктами. Ця система забезпечує цілодобовий моніторинг підозрілої активності у мережах державних органів та критичної інфраструктури та ін.

– *запровадження практики проведення загальнонаціональної інформаційної роз'яснювальної кампанії щодо дій громадян у випадку, коли вони стикаються із кібершахрайством та іншими кіберзлочинами, а також роз'яснення процедур звернення до правоохоронних органів*[169]. Як приклад, Щорічна ініціатива «Місяць цифрової грамотності», спрямована на вдосконалення цифрових навичок українців, яку проводить Міністерство цифрової трансформації України. Ця кампанія спрямована на підвищення рівня цифрової освіченості населення та впровадження актуальних технологічних компетенцій у повсякденну та професійну діяльність.

– *розроблення методики збору кіберстатистики та щорічного оприлюднення статистичної інформації щодо кібератак, кіберінцидентів та заходів протидії за сферами відповідальності основних суб'єктів національної системи кібербезпеки на їх офіційних вебсайтах*. Зокрема, наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 5 серпня 2025 року № 482 затверджено Методичні рекомендації щодо збору та обробки статистичних даних щодо кібератак, кіберінцидентів і заходів протидії у Державній службі спеціального зв'язку та захисту інформації України, який мають інформаційний та рекомендаційний характер. Зокрема, до звітів Державної служби спеціального зв'язку та захисту інформації України вносяться відомості про кіберінциденти (кібератаки) або заходи протидії з підтвердженою реєстрацією. Узагальнення даних кіберстатистики здійснюється Державним центром кіберзахисту Державної служби спеціального зв'язку та захисту інформації України,

[169] Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 р. № 447/2021. URL : https://zakon.rada.gov.ua/laws/show/447/2021#Tex.

звіт якого за результатами узагальнення даних кіберстатистики за календарний рік може подаватися користувачам із цільової групи користувачів даних кіберстатистики раз на рік. Звіт за результатами узагальнення даних кіберстатистики (для оприлюднення даних кіберстатистики за календарний рік) оприлюднюється Державною службою спеціального зв'язку та захисту інформації України на своєму вебсайті щороку[170]. Основні суб'єкти національної системи кібербезпеки публікують щорічні та квартальні звіти на своїх офіційних ресурсах, а саме: РНБО (НКЦК) – координує загальний збір даних та оприлюднює узагальнену статистику. За 2025 рік зафіксовано майже 6000 кібератак (на 37 % більше, ніж у 2024 році)[171]; Держспецзв'язку (CERT-UA) – публікує детальні річні звіти про роботу Системи виявлення вразливостей. У першому кварталі 2026 року фахівці опрацювали 117 складних кіберінцидентів[172]; Служба безпеки України – регулярно звітує про нейтралізацію атак на критичну інфраструктуру. За перший квартал 2026 року СБУ зупинила понад 530 атак. Як вбачається зі Звіту, здебільшого кібератаки спрямовані на органи державної влади та оборонні підприємства[173]; Департамент кіберполіції – оприлюднює щорічні звіти, фокусуючись на протидії кіберзлочинності, зокрема фінансовому шахрайству та незаконному використанню криптовалют[174].

– розроблення методики проведення щорічних соціологічних досліджень щодо кіберзагроз, з якими стикається населення України, з оцінками ефективності діяльності державних органів у протидії ним і

---

[170] Методичні рекомендації щодо збору та обробки статистичних даних щодо кібератак, кіберінцидентів і заходів протидії у Державній службі спеціального зв'язку та захисту інформації України: затв. Наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 5 серпня 2025 року № 482. URL : https://cip.gov.ua/ua/docs/nakaz-administraciyi-derzhspeczv-yazku-vid-05-08-2025-482-pro-zatverdzhennya-metodichnikh-rekomendacii-shodo-zboru-ta-obrobki-statistichnikh-danikh-stosovno-kiberatak-kiberincidentiv-i-zakhodiv-protidiyi-u-derzhavnii-sluzhbi-specialnogo-zv-yazku-ta-zakhistu-informaciyi-ukrayini.

[171] Український досвід змінює світову кібербезпеку. Рада національної безпеки і оборони: веб-сайт. URL : https://www.rnbo.gov.ua/ua/Diialnist/7376.html.

[172] Оперативний центр реагування на кіберінциденти ДЦКЗ прозвітував за І квартал 2026 року. URL : https://cip.gov.ua/ua/news/operativnii-centr-reaguvannya-na-kiberincidenti-dckz-prozvituvav-za-i-kvartal-2026-roku.

[173] Кузьменко Ю. СБУ з початку року нейтралізувала понад 530 кібератак, більшість – справа російських спецслужб. URL : https://news.liga.net/ua/war/news/sbu-z-pochatku-roku-neytralizuvaly-ponad-530-kiberatak-bilshist-sprava-rosiyskykh-spetssluzhb?utm_source=fb&utm_medium=cpc&utm_campaign=social.

[174] Щорічний звіт Департаменту кіберполіції Національної поліції України за 2025 рік : Кіберполіція Уряїни : веб-сайт. URL : https://cyberpolice.gov.ua/news/shhorichnyj-zvit-7096/.

забезпечення проведення таких досліджень;

– *розроблення методики комунікації між державою та суспільством щодо протидії масштабним кібератакам і кіберінцидентам, створення необхідних умов для її практичної реалізації*. Наприклад, у системі Національної поліції, з метою покращення взаємодії з громадянами та надання їм кваліфікованої допомоги, забезпечено диференційовані канали зв'язку, зокрема, особисті та електронні звернення, телефонну інформаційну підтримку, функціонування офіційного вебресурсу з каналами зворотного зв'язку. Відповідно до оприлюдненого Щорічного звіту Департаменту кіберполіції Національної поліції України за 2025 р. розпочато окремі загальнодержавні інформаційні кампанії для підвищення кіберграмотності українців, протидії насиллю над дітьми, кібербуллінгу та для розвитку безбар'єрного простору на підтримку визначеного керівництвом держави курсу євроінтеграції. Враховуючи те, що однією з детермінант учинення кіберзлочинів є кіберграмотність та рівень усвідомлення цінності персональних даних, з метою запобігання їх витоку поліцією здійснювалася підготовка та розміщення матеріалів Всеукраїнської інформаційної кампанії «КібербезпекаФінансів» (спільно з Національним банком України та Держспецзв'язку), яка має за мету поширення знань про правила платіжної безпеки та формування в споживачів фінансових послуг навичок захисту фінансових даних у віртуальному просторі та є продовженням інформаційної кампанії «ШахрайГудбай». Запроваджено також спільну рубрику Департаменту кіберполіці та ранкового шоу «Сніданок з 1+1», яка спрямована на підвищення цифрової грамотності громадян, де фахівці інформують про найпоширеніші шахрайські схеми, надаючи дієві поради щодо захисту особистих даних тощо[175].

– *налагодження систематичного обміну інформацією про деструктивну діяльність у кіберпросторі з міжнародними партнерами, насамперед Сполученими Штатами Америки, державами – членами ЄС та державами – членами НАТО, створення платформи такого обміну*. Наприклад, державна команда реагування на комп'ютерні надзвичайні події України (CERT-UA), що діє при Держспецзв'язку, використовує MISP (відкриту open-source платформу для збору, зберігання, аналізу та обміну інформацією про кіберзагрози) для обміну інформацією про кіберзагрози з міжнародними партнерами. Наразі під час атак на

[175] Щорічний звіт Департаменту кіберполіції Національної поліції України за 2025 рік : Кіберполіція Уряїни : веб-сайт. URL : https://cyberpolice.gov.ua/news/shhorichnyj-zvit-7096/.

українські урядові сайти у 2022 році CERT-UA застосовувала MISP для швидкого поширення IoC, пов'язаних із шкідливим ПЗ (наприклад, WhisperGate), серед інших CERT та CSIRT. Це дозволило організаціям оперативно оновити свої системи захисту[176].

– врегулювання на законодавчому рівні питання щодо всебічного залучення приватного сектору та громадянського суспільства до здійснення заходів зі стримування деструктивної діяльності в кіберпросторі. Наприклад, у ст.ст. 7.1.e, 9.4.e, 11.4 Директиви NIS2, п.п. 31, 49 преамбули Акту про кібербезпеку згадується про можливість взаємодії з приватним сектором. У результаті внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури було надано можливість делегувати приватним командам реагування виконання завдань галузевих або регіональних команд реагування (зміни до ст. 14 Закону України «Про Державну службу спеціального зв'язку та захисту інформації України», до п. 2 ч. 3 ст. 9 Закону України «Про основні засади забезпечення кібербезпеки України») та залучати їх для надання послуг з управління інцидентами кібербезпеки, кібератаками, кіберзагрозами власникам/розпорядникам[177].

– упровадження ризик-орієнтованого підходу в частині заходів забезпечення кібербезпеки об'єктів критичної інфраструктури та державних органів, зокрема, розроблення методики ідентифікації та оцінки кіберризиків на національному рівні та для секторів критичної інфраструктури держави, врегулювання на законодавчому рівні обов'язковості здійснення періодичної оцінки ризиків на підставі розроблених методик тощо[178]. Україна переходить на ризикоорієнтований підхід. Затверджено каталог заходів та нові вимоги для держорганів і критичної інфраструктури, що діятимуть у 2026 році. Адміністрація Держспецзв'язку затвердила пакет нормативних документів, які впроваджують сучасний ризикоорієнтований підхід до кібербезпеки в Україні. Нові заходи розроблені з урахуванням міжнародного стандарту NIST Cybersecurity Framework 2.0 та спрямовані

[176] MISP: Платформа для обміну інформацією про кіберзагрози та її значення для України. URL : https://cybersec.net.ua/statti/907-misp-platforma-dlia-obminu-informatsiieiu-pro-kiberzahrozy-ta-ii-znachennia-dlia-ukrainy.html.

[177] Висновок на проект Закону України «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури». URL : https://itd.rada.gov.ua/4b8097e0-3ba8-4310-a984-850d62932d7a.

[178] Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 р. № 447/2021. URL : https://zakon.rada.gov.ua/laws/show/447/2021#Tex.

на захист критичної інфраструктури та державних інформаційних ресурсів. Зокрема, з метою посилення стійкості національного кіберпростору, Адміністрація Державної служби спеціального зв'язку та захисту інформації України оприлюднила ключові документи, що визначають оновлені правила гри для суб'єктів кіберзахисту у 2026 році. Основною зміною став перехід від формального виконання вимог до активного управління ризиками. Зокрема, нова архітектура заходів базується на таких функціях, як ідентифікація, захист, виявлення, реагування та відновлення.

– Затверджений пакет включає чотири основні компоненти:

1. *Каталог заходів з кіберзахисту* – повний перелік організаційних та технічних дій, структурований за міжнародними стандартами;
2. *Базові заходи з кіберзахисту* – мінімально необхідний набір дій для різних категорій організацій, що дозволяє швидко налаштувати базовий рівень безпеки;
3. Уніфікована форма Плану кіберзахисту – чіткий шаблон, який допоможе керівникам установ структурувати заходи, призначити відповідальних та визначити терміни виконання;
4. Методичні рекомендації – детальні роз’яснення та приклади впровадження заходів (із посиланнями на NIST SP 800-53, COBIT та НД ТЗІ), що робить процес реалізації зрозумілим для технічних фахівців[179].

Оновлені вимоги є обов'язковими для: операторів критичної інфраструктури (I-IV категорій критичності); органів державної влади та місцевого самоврядування; державних підприємств та установ, які працюють з державними інформаційними ресурсами або інформацією з обмеженим доступом.

Особлива увага в документах приділяється забезпеченню безперервності бізнес-процесів та здатності швидко відновлюватися після інцидентів. Зокрема, нові норми деталізують процедури інформування про кіберінциденти через механізм «єдиного вікна» та платформу обміну інформацією в режимі реального часу. Впровадження цих стандартів – це не просто виконання нормативних вимог, а крок до створення єдиної екосистеми кіберзахисту, де кожна організація розуміє

[179] Наказ Адміністрації Держспецзв’язку від 30.01.2026 № 75 «Про затвердження Каталогу заходів з кіберзахисту, базових заходів з кіберзахисту, форми плану кіберзахисту та методичних рекомендацій щодо здійснення заходів з кіберзахисту». URL : https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-30-01-2026-75-pro-zatverdzhennya-katalogu-zakhodiv-z-kiberzakhistu-bazovikh-zakhodiv-z-kiberzakhistu-formi-planu-kiberzakhistu-ta-metodichnikh-rekomendacii-shodo-zdiisnennya-zakhodiv-z-kiberzakhistu.

свої активи, ризики та має чіткий алгоритм дій у разі атаки[180].

Відтак, з метою дотримання встановлених норм суб'єктам слід здійснити інвентаризацію активів (ID.AM) та оцінити ризики, керуючись оновленими методичними рекомендаціями.

Таким чином, у порівнянні з першою вітчизняною Стратегією з кібербезпеки основні спеціально-кримінологічні заходи запобігання кіберзлочинності, які передбачені на період 2021–2025 рр, виконані (на 86 %[181]), що свідчить про значне покращення ефективності координації між державним, військовим та приватним секторами в умовах воєнного стану, стійкість та гнучкість державної архітектури кіберзахисту в умовах кризового реагування.

3.2. Індивідуальні заходи запобігання кіберзлочинності

Стрімкий розвиток цифрового середовища, збільшення кількості користувачів мережі Інтернет і активне впровадження електронних сервісів обумовлюють не лише розширення можливостей для комунікації та економічної діяльності, але й створюють нові ризики для безпеки особи, суспільства та держави. З огляду на зазначене кіберзлочинність залишається однією із найбільш небезпечних форм протиправної поведінки. До її основних ознак на думку Дзюндзюк В. Б. та Дзюндзюк Б. В. належать: 1) вчиняється у віртуальному просторі або в межах комп'ютерних мереж; 2) вчинення кіберзлочинів, на відміну від інших, є більш доступним для людей із невисокими соціальними і віковими можливостями; 3) його вчинення у віртуальному просторі вимагає застосування певного комплексу знань, крім того, в суспільстві активно пропагується ідея «інтелектуальності» хакерів, роблячи цю субкультуру ще більш популярною; 4) кіберзлочини є анонімними та неперсоніфікованими; 5) цьому виду злочинності властивий високий рівень латентності[182].

---

[180] Держспецзв'язку оновлює вимоги до кіберзахисту: затверджено нові стандарти на основі NIST CSF 2.0. URL : https://ips.ligazakon.net/lawnews/doc/EN260244-derzhspetszvyazku-onovlyuye-vymohy-do-kiberzakhystu-zatverdzheno-novi-standarty-na-osnovi-2-0.

[181] Адміністрація Держспецзв'язку оприлюднила звіт про виконання Стратегії кібербезпеки України у 2025 році: рівень реалізації заходів сягнув 86 %. URL : https://cip.gov.ua/ua/news/derzhspeczv-yazku-oprilyudnila-zvit-pro-vikonannya-strategiyi-kiberbezpeki-ukrayini-u-2025-roci-riven-realizaciyi-zakhodiv-syagnuv-86.

[182] Дзюндзюк В. Б., Дзюндзюк Б. В. Поява і розвиток кіберзлочинності. *Державне будівництво*. 2013. № 1. С. 8-9.

Враховуючи зазначене, провідне місце у системі запобігання кіберзлочинності посідають індивідуальні заходи. Під ними доцільно розуміти сукупність дій, правил поведінки та технічних рішень, що застосовуються окремою особою з метою захисту власних персональних даних, електронних пристроїв і фінансових ресурсів від кіберзагроз. На відміну від загальних заходів, які реалізуються на державному чи організаційному рівнях, індивідуальні заходи мають персоніфікований характер і безпосередньо пов'язані з рівнем цифрової культури та обізнаності користувача[183].

Практика свідчить, що значна частина кіберзлочинів, зокрема фішинг, шахрайство з платіжними картками, атаки на банкомати тощо, здійснюється безпосередньо через поведінку людей, а саме у зв’язку з їх необізнаністю, неуважністю або недотриманням базових правил кібербезпеки[184]. Як наслідок, підвищення рівня цифрової грамотності населення є головною частиною віктимологічної профілактики кіберзлочинності, що сприятиме формуванню ефективних моделей безпечної поведінки в цифровому середовищі та зменшенню рівня віктимності населення.

Наразі Джужа О. М. визначає індивідуальну профілактику як своєчасний вплив на тих осіб, від яких першочергово надходить загроза ймовірності вчинення злочину. У цьому разі йдеться про чітку дію уповноважених органів на конкретну особу та її оточення після появи сигналу щодо можливої криміналізації зазначеної особи. За такого підходу до визначення індивідуальної профілактики об’єктом профілактичних дій визнається певна людина та її спосіб життя, який свідчить про можливість вдатися до злочинних дій[185].

Водночас Бандурка О. М. наголошує на тому, що індивідуальна профілактика проявляється у низці виховних дій, які проводяться уповноваженими органами заради формування певного імунітету в особи стосовно певної злочинної спокуси[186]. Разом із цим індивідуальну профілактику можна визначити як певну систему з декількома рівнями

---

[183] Сміян Л. С., Нікітін Ю. В. Кримінологія: підручник / за заг. ред. Л. С. Сміяна, Ю. В. Нікітіна. Київ : Національна академія управління, 2010. С. 116.

[184] Борисенко В. О. Класифікація та типологія кіберзлочинів у банківській сфері. *Ірпінський юридичний часопис*. 2025. № 2(19). С. 145-153.

[185] Профілактика злочинів : підручник / О.М. Джужа, В.В. Василевич, О.Ф. Гіда та ін.; за заг. ред. д-ра юрид. наук, проф. О. М. Джужі. Київ : Атіка, 2011. С. 52-53.

[186] Бандурка О.М. Профілактика злочинності. *Вісник Південного регіонального центру Національної академії правових наук України*. 2014. № 1. С. 116.

взаємодії різних елементів суспільства, метою діяльності якої є загальна боротьба зі злочинністю[187].

Вбачається, що зміст індивідуальної профілактики не обмежується виключно виявленням потенційних ризиків, а передбачає комплексне впровадження превентивних заходів, спрямованих на трансформацію мотиваційних установок, рівня правосвідомості та поведінкових моделей особи. Значною складовою такої діяльності є цілеспрямований вплив на оточення особи, як у реальному соціальному середовищі, так і в цифровому просторі, який у сучасних умовах набуває дедалі більшого значення під час формування девіантної поведінки.

Попередження кіберзлочинів передбачає, перш за все, цільовий вплив на осіб, які схильні до вчинення таких правопорушень. Заходи такого впливу охоплюють не лише індивідуальну профілактичну роботу з конкретними особами, але й моніторинг та корекцію соціального середовища. До цього належить аналіз діяльності онлайн-спільнот, спеціалізованих форумів, месенджерів та сегментів так званих «темних мереж»[188].

Під формами профілактичної діяльності у сфері протидії кіберзлочинності доцільно розуміти науково обґрунтовану систему найбільш ефективних засобів, спрямованих на розв'язання завдань профілактики кіберзлочинів. Такі форми відображають організаційно та функціонально впорядковану діяльність уповноважених суб'єктів, орієнтовану на запобігання правопорушенням у цифровому середовищі[189].

Принагідно відзначити, що залежно від стадії формування у особи девіантної поведінки, індивідуальна профілактика поділяється на чотири види.

Перший вид стосується осіб, які перебувають на початковому етапі криміналізації (рання індивідуальна профілактика кримінальних правопорушень)[190].

Другий вид стосується осіб, які вчинили або вчиняють кримінальні правопорушення (судово-слідчий)[191].

---

[187] Цимбал П. В., Кимлик Н. В., Ляшенко М. М. Попередження корупційних злочинів. *Науковий вісник Національного університету державної податкової служби України (економіка, право)*. 2012. № 4. С. 213-214.

[188] Михайлов В. О., Романенко О. В. Темна мережа (darknet) як динамічне середовище кіберпростору та інструмент для вчинення кримінальних правопорушень. DICTUM FACTUM. 2024. № 2(16). С. 267.

[189] Didkivska H. V., Elshad R.I. Topical issues of counteracting cybercrime in Ukraine. *Ірпінський юридичний часопис*. 2025. № 1(18). С. 182-188.

[190] Сміян Л. С., Нікітін Ю. В. Кримінологія: підручник / за заг. ред. Л. С. Сміяна, Ю. В. Нікітіна. Київ : Національна академія управління, 2010. С. 118-119.

[191] Так само.

Третій вид охоплює осіб, які вчинили кримінальні правопорушення і стосовно них суд прийняв рішення про застосування різних заходів кримінально-правового впливу (пенітенціарний)[192].

Четвертий вид стосується осіб, що відбули кримінальне покарання, але перебувають під наглядом з метою запобігання рецидиву (постпенітенціарний)[193].

Заходи індивідуального попередження кіберзлочинності, що реалізуються стосовно конкретної особи, мають на меті нейтралізацію або усунення внутрішніх негативних характеристик її особистості та поведінки. Йдеться, зокрема, про корекцію використання знань і навичок, які можуть застосовуватися у протиправних цілях, подолання мотивації до отримання швидкого незаконного прибутку, а також формування належного рівня кібергігієни. Важливе значення має також урахування кримінологічно значущих психофізіологічних особливостей особи, що можуть впливати на її схильність до вчинення кіберзлочинів[194].

У випадках, коли профілактичний вплив спрямовується на соціальне мікросередовище особи, пріоритетом стає усунення або мінімізація зовнішніх негативних чинників. До таких чинників належать, зокрема, участь у деструктивних онлайн-спільнотах, доступ до протиправного контенту в сегментах даркнету, а також несприятливі міжособистісні відносини у реальному середовищі. Вплив на мікросередовище дозволяє змінити соціальний контекст, у якому формується поведінка особи, що, сприяє зниженню ризику девіантної та протиправної діяльності.

Вибір конкретних заходів індивідуальної профілактики визначається сукупністю факторів, серед яких ключовими є ступінь антисоціальності мікросередовища, можливості його трансформації, інтенсивність негативного впливу, а також індивідуальні характеристики особи. До того ж, особливої уваги набуває принцип своєчасності, адже найбільш ефективними є превентивні заходи, застосовані на ранніх стадіях формування протиправної поведінки коли у особи з’являється мотивація[195].

---

[192] Так само.

[193] Так само.

[194] Агапова К. В. Індивідуально-профілактичні заходи запобігання кримінальним правопорушенням, що вчиняються молодіжними угрупованнями. *Південноукраїнський правничий часопис*. № 4. 2021. С. 88-89.

[195] Нікіфорова Т. І. Теорія і практика застосування заходів кримінально-правового характеру: навчальний посібник. Хмельницький : Хмельницький університет управління та права імені Леоніда Юзькова, 2020. 175 с.

Рання індивідуальна профілактика є не лише найбільш людиноцентричним заходом, але й результативною формою запобігання кіберзлочинності, оскільки останній дозволяє протидіяти вчиненню більш тяжких кримінальних правопорушень[196]. Такий підхід відповідає сучасним засадам державної політики у сфері кібербезпеки, зокрема положенням Закону України «Про основні засади забезпечення кібербезпеки України», який орієнтований на пріоритет превентивних заходів, підвищення рівня обізнаності населення та зміцнення індивідуальної відповідальності за безпечну поведінку в цифровому середовищі[197].

Досягнення цієї мети вимагає реалізації низки конкретних завдань:

а) виявлення осіб, поведінка яких свідчить про реальну можливість вчинення кримінальних правопорушень;

б) виявлення джерел протиправного впливу на них;

в) прогнозування індивідуальної поведінки;

г) планування заходів індивідуальної профілактики;

д) позитивно керуючий вплив.

Важливою частиною індивідуальної профілактики кіберзлочинності у діяльності правоохоронних органів, зокрема Департаменту кіберполіції Національної поліції України, є виконання спеціальних превентивних завдань, передбачених чинним законодавством. До таких завдань належать, зокрема, реалізація державної політики в сфері протидії кіберзлочинності; своєчасне інформування населення про появу нових осіб, які вчиняють кримінальні правопорушення; впровадження програмних засобів для систематизації фактів вчинення кримінальних правопорушень у досліджуваній сфері; реагування на запити закордонних партнерів[198]. Зазначені заходи мають превентивний характер і спрямовані на недопущення вчинення нових або повторних кіберзлочинів.

Наразі реалізація таких заходів пов’язана з певним втручанням у сферу приватного життя особи, що обумовлює необхідність їх здійснення виключно з дотриманням конституційних гарантій прав та свобод

---

[196] Павлова Т. О. Механізм формування кримінально протиправної поведінки. Матеріали 77-ї наук. конф. професорсько-викладацького складу і наукових працівників економіко-правового факультету Одеського національного університету імені І. І. Мечникова (23–25 листоп. 2022 р., м. Одеса) / відп. ред. О. В. Побережець ; ред. кол.: А. Л. Святошнюк, Т. В. Степанова та ін. Одеса : Олді+, 2022. С. 104.

[197] Закон України «Про основні засади забезпечення кібербезпеки України». № 2163-VIII від 24 жовтня 2020 р. URL : https://zakon.rada.gov.ua/laws/show/2163-19#Text.

[198] Білобров Т. В. Адміністративно-правовий статус Департаменту кіберполіції Національної поліції України : дис. ... канд. юрид. наук : 12.00.07. Київ, 2020. С. 4.

людини і громадянина. Зокрема, така діяльність повинна відповідати положенням Конституції України, законодавству у сфері кібербезпеки, а також нормам, що регулюють захист персональних даних. Це забезпечує баланс між інтересами суспільної безпеки та правами окремої особи.

З метою підвищення ефективності індивідуального попередження кіберзлочинності у науковій та практичній сферах виокремлюються основні вимоги, яких необхідно дотримуватися при реалізації відповідних заходів. Наразі законність є підґрунтям здійснення будь-якої превентивної діяльності у сфері кібербезпеки. Відповідно до цього усі заходи мають реалізовуватися виключно на підставі, в межах повноважень та у спосіб, що передбачені чинним законодавством України.

Своєчасність полягає у здійсненні раннього виявлення осіб, схильних до формування суспільно-небезпечних установок у кіберпросторі, з метою запобігання вчиненню кіберзлочинів. Несвоєчасне реагування уповноважених органів істотно підвищує ризик реалізації протиправної поведінки, що зумовлено швидкістю поширення інформації та значним рівнем анонімності в мережі Інтернет. У зв’язку з цим особливого значення набуває забезпечення оперативності та безперервності моніторингу кіберпростору, а також належної оцінки потенційних загроз.

Послідовність характеризується системним та безперервним здійсненням профілактичного впливу. Також інтенсивність заходів варіюється залежно від ефективності їх реалізації, поведінки особи та рівня ризику вчинення правопорушення. Зазначений підхід забезпечує своєчасне коригування профілактичних заходів і підвищує їх результативність. Водночас це дозволяє уникнути як надмірного, так і недостатнього втручання у поведінку особи. Крім того, дотримання принципу послідовності сприяє зниженню ймовірності рецидиву правопорушень.

Матеріально-технічне забезпечення полягає у визначенні відповідності запланованих заходів фактичним можливостям їх практичної реалізації. Зазначене передбачає обов'язкове урахування наявних матеріальних, технічних та кадрових ресурсів, якими володіють відповідні підрозділи. Його дотримання забезпечує досяжність поставлених цілей і запобігає формальному характеру управлінських рішень. Водночас це дозволяє оптимізувати використання ресурсного потенціалу та забезпечити належний рівень виконання покладених завдань.

Разом із цим, ефективність індивідуальної профілактики кіберзлочинності значною мірою залежить від комплексного дотримання зазначених вимог, що забезпечує не лише результативність превентивних заходів, але й правомірності їх застосування. Така діяльність передбачає не одноразовий вплив, а тривалий, систематичний і цілеспрямований

процес роботи з особою, що ґрунтується на поєднанні правових, соціально-психологічних та організаційних засобів. Важливо, що така діяльність має здійснюватися з дотриманням прав і свобод людини, а також із урахуванням індивідуальних особливостей особи, її поведінки та оточення. У юридичній науці та правозастосовній практиці традиційно виокремлюють три основні методи індивідуального попередження кіберзлочинності: переконання, надання допомоги та примус[199].

Зі змісту вбачається, що метод переконання є пріоритетним у системі запобігання, оскільки спрямований на формування внутрішньої мотивації особи до правомірної поведінки. Він охоплює комплекс інформаційно-просвітницьких заходів, метою яких є нівелювання будь-яких девіантних установок, підвищення рівня правової культури та усвідомлення наслідків протиправної діяльності у кіберпросторі[200]. До основних форм реалізації цього методу належать індивідуальні профілактичні бесіди з працівниками кіберполіції, проведення роз'яснювальної роботи у закладах освіти, запровадження інституту менторства, а також інформування про положення кримінального законодавства, зокрема ст. 361-363-1 Кримінального кодексу України, що передбачають відповідальність за кіберзлочини. Важливу роль відіграє офіційне попередження про неприпустимість протиправної поведінки та можливість постановки на облік як превентивного заходу.

Метод надання допомоги вважається одним із найбільш ефективних, оскільки дозволяє не лише усунути передумови протиправної поведінки, але й сприяти соціально корисній реалізації потенціалу особи. Його сутність полягає у створенні умов, за яких особа може застосовувати свої знання та навички у правомірній діяльності. Зокрема, йдеться про сприяння працевлаштуванню у сфері кібербезпеки, надання можливостей для підвищення кваліфікації, участі в освітніх програмах або професійній підготовці. До того ж, цей метод передбачає покращення соціально-побутових умов, психологічну підтримку, а також вплив на мікросередовище особи з метою усунення негативного впливу, зокрема обмеження контактів із деструктивними онлайн-спільнотами[201].

Метод примусу є допоміжним і застосовується лише у випадках, коли інші заходи не дали належного результату або коли поведінка особи становить

---

[199] Сміян Л. С., Нікітін Ю. В. Кримінологія: підручник / за заг. ред. Л. С. Сміяна, Ю. В. Нікітіна. Київ : Національна академія управління, 2010. С. 117-118.

[200] Бесчастний В. М. Кримінологічне забезпечення протидії злочинності в Україні: монографія. Харків : В справі, 2017. 360 с.

[201] Кримінологія: академічний підручник: [Богатирьов І. Г., Колб О. Г., Топчій В. В. та ін.] за. заг. ред. доктора юридичних наук, професора, заслуженого діяча науки і техніки України Богатирьова І. Г. Чернівці: Технодрук, 2020. С. 108.

реальну загрозу. Його використання можливе виключно на підставі закону та в межах повноважень правоохоронних органів[202]. До основних форм примусу належать такі: примусові заходи медичного характеру (статті 92–95 КК України), примусове лікування (ст. 96 КК України), спеціальна конфіскація (статті 96^1–96^2 КК України), заходи кримінально-правового характеру щодо юридичних осіб (статті 96^3–96^{11} КК України), примусові заходи виховного характеру (статті 97, 105 КК України) та інші[203].

Тобто, ефективна індивідуальна профілактика кіберзлочинності передбачає комплексне поєднання зазначених методів із пріоритетом переконання та надання допомоги, а також обмеженим і правомірним застосуванням примусу. Саме сукупність цих підходів забезпечує не лише запобігання правопорушенням, але й сприяє формуванню відповідальної поведінки людини у цифровому середовищі.

Застосування заходів індивідуального попередження кіберзлочинності передбачає безперервний, системний процес вивчення особистості, що охоплює аналіз її поведінки як у реальному, так і у віртуальному середовищі. Особлива увага приділяється дослідженню онлайн-активності особи, характеру її цифрових зв'язків, участі в інтернет-спільнотах, а також можливих намірів щодо використання інформаційних технологій у протиправних цілях. Зібрана та узагальнена інформація є підґрунтям для формування індивідуального плану профілактичної роботи, що підлягає постійному коригуванню залежно від змін у поведінці особи, ступеня ризику та ефективності застосованих заходів. Зазначена діяльність реалізується Департаментом кіберполіції Національної поліції України відповідно до положень Закону України «Про основні засади забезпечення кібербезпеки України», Закону України «Про Національну поліцію», а також стратегічних документів державної політики у сфері кібербезпеки, зокрема Стратегія кібербезпеки України.

Водночас, із урахуванням вищезгаданого людиноцентричного підходу, доцільним є виокремлення пріоритетних напрямів дотримання кібергігієни, які мають комплексний та взаємопов'язаний характер. До таких напрямів, зокрема, належать: захист персональних даних і забезпечення конфіденційності інформації, протидія кібератакам та шкідливому програмному забезпеченню, а також формування цифрової культури як важливої складової безпечного функціонування особи у кіберпросторі.

---

[202] Коломієць Ю. Ю. Невідворотність кримінальної відповідальності: правова природа та зміст : автореф. дис. ... канд. юрид. наук : 12.00.08. Одеса, 2005. 17 с.

[203] Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III. URL : https://zakon.rada.gov.ua/laws/show/2341-14#Text.

Отже, індивідуальна профілактика кіберзлочинності є одним із визначальних напрямів сучасної системи протидії кіберзагрозам. Вона поєднує комплекс правових, організаційних і соціально-психологічних заходів впливу як на особу, так і на її найближче оточення. Своєю чергою, її ефективність безпосередньо залежить від своєчасного виявлення ризиків, системності та послідовності здійснення профілактичної роботи, а також неухильного дотримання принципу законності та поваги до прав і свобод людини. Це сприяє не лише запобіганню відповідним правопорушенням, але й формуванню відповідальної, правосвідомої поведінки особи у цифровому середовищі.

Контрольні питання до розділу 3:

1. Що слід розуміти під спеціально-кримінологічними заходами запобігання кіберзлочинності?
2. Яке місце спеціально-кримінологічних заходів у системі запобігання кіберзлочинності?
3. Які основні напрями спеціально-кримінологічного запобігання кіберзлочинності?
4. Яка роль державних органів у реалізації спеціально-кримінологічних заходів?
5. Яке значення має діяльність підрозділів кіберполіції у запобіганні кіберзлочинності?
6. Що слід розуміти під індивідуальними заходами запобігання кіберзлочинності?
7. У чому полягає відмінність індивідуального запобігання від загального та спеціального?
8. Які категорії осіб потребують індивідуального запобіжного впливу у сфері кіберзлочинності?
9. Які основні форми індивідуальної профілактики кіберзлочинів?
10. Яке значення має раннє виявлення осіб, схильних до вчинення кіберзлочинів?

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Агапова К. В. Індивідуально-профілактичні заходи запобігання кримінальним правопорушенням, що вчиняються молодіжними угрупованнями. *Південноукраїнський правничий часопис.* № 4. 2021. С. 86–91.

2. Адміністрація Держспецзв'язку оприлюднила звіт про виконання Стратегії кібербезпеки України у 2025 році: рівень реалізації заходів сягнув 86 %. URL : https://cip.gov.ua/ua/news/derzhspeczv-yazku-oprilyudnila-zvit-pro-vikonannya-strategiyi-kiberbezpeki-ukrayini-u-2025-roci-riven-realizaciyi-zakhodiv-syagnuv-86.

3. Атаки хакерів на Міноборони відбиватиме новостворений Центр реагування на кіберінциденти. URL : https://mod.gov.ua/news/ataki-hakeriv-na-minoboroni-vidbivatime-novostvorenij-czentr-reaguvannya-na-kiberinczidenti.

4. Бандурка О. М., Литвинов О. М. Протидія злочинності та профілактика злочинів : монографія. Харків : ХНУВС, 2011. 308 с.

5. Бандурка О. М. Профілактика злочинності. Вісник Південного регіонального центру Національної академії правових наук України. 2014. № 1. С. 115–124.

6. Беккарія Ч. Про злочини і покарання / Ч. Беккарія. Київ : Юрінком Інтер, 2005.

7. Бесчастний В. М. Кримінологічне забезпечення протидії злочинності в Україні: монографія. Харків : В справі, 2017. 360 с.

8. Білобров Т. В. Адміністративно-правовий статус Департаменту кіберполіції Національної поліції України : дис. ... канд. юрид. наук : 12.00.07. Київ, 2020. 209 с.

9. Борисенко В. О. Класифікація та типологія кіберзлочинів у банківській сфері. *Ірпінський юридичний часопис.* 2025. № 2(19). С. 145-153.

10. Борисов В. І. Кримінально-правова охорона інформаційної безпеки в Україні. Харків : Право, 2024. 328 с.

11. Верховна Рада України підтримала створення нового органу військового управління – Кіберсили Збройних Сил України. URL : https://www.rada.gov.ua/news/razom/266780.html.

12. Вирок Вінницького міського суду Вінницької області у справі № 127/28630/22 від 30 грудня 2022 р. URL : https://reyestr.court.gov.ua/Review/108244485.

13. Вирок Залізничного районного суду м Львова у справі № 462/2974/22 від 20 жовтня 2022 р. URL : https://reyestr.court.gov.ua/Review/106857880.

14. Вирок Збаразького районного суду Тернопільської області у справі № 598/584/24 від 13 березня 2024 р. URL : https://reyestr.court.gov.ua/Review/117633776.

15. Вирок Орджонікідзевського районного суду м. Запоріжжя у справі № 335/14157/14-к від 17 грудня 2014 р. URL : https://reyestr.court.gov.ua/Review/41961833.

16. Вирок Печерського районного суду м. Києва у справі № 757/35881/15-к від 12.10.2015 р. URL : https://zakononline.ua/court-decisions/show/52901355.

17. Вирок Радомишльського районного суду Житомирської області у справі № 289/2502/22-к від 15.02.2023 р. URL : https://reyestr.court.gov.ua/Review/108997544.

18. Вирок Святошинського районного суду м. Києва у справі № 759/4752/22 від 15 червня 2023 р. URL : https://reyestr.court.gov.ua/Review/111561448.

19. Вирок Тячівського районного суду Закарпатської області у справі № 307/838/20 від 01 жовтня 2020 р. URL : https://reyestr.court.gov.ua/Review/91922391.

20. Вирок Франківського районного суду м. Львова у справі № 465/5121/20 від 11.10.2021 р. URL : https://reyestr.court.gov.ua/ Review/100341888.

21. Вирок Центрального районного суду м. Миколаєва у справі № 490/7762/21 від 28 жовтня 2021 р. URL : https://reyestr.court.gov.ua/Review/100745826.

22. Висновок на проект Закону України «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об’єктів критичної інформаційної інфраструктури» URL : https://itd.rada.gov.ua/4b8097e0-3ba8-4310-a984-850d62932d7a.

23. Галушко П. П. Кіберзлочинність: поняття та соціально-правова природа. *Вісник кримінологічної асоціації України*. 2025. № 1 (34). С. 808-815. с. 815.

24. Група реагування на комп'ютерні надзвичайні події України CERT-UA. Звіт за 2025 рік. Київ, 2026.

25. Давидова Т. О. Система кількісних та якісних показників як основа дослідження кримінологічної характеристики корупції. *Юридичний науковий електронний журнал.* 2014. №5. С. 107-110.

26. Дем'янов В. Кримінологічна характеристика порушення правил екологічної безпеки у промисловому регіоні України. *Юридичний вісник*. 2022. № 5. С. 335-343.

27. Державна служба спеціального зв'язку та захисту інформації України. Звіт про стан кібербезпеки 2025. Київ, 2026.

28. Держспецзв'язку затвердила рекомендації з кіберзахисту систем, які використовують штучний інтелект. URL : https://www.kmu.gov.ua/news/derzhspetszviazku-zatverdyla-rekomendatsii-z-kiberzakhystu-system-iaki-vykorystovuiut-shtuchnyi-intelekt.

29. Держспецзв'язку оновлює вимоги до кіберзахисту: затверджено нові стандарти на основі NIST CSF 2.0. URL : https://ips.ligazakon.net/lawnews/doc/EN260244-derzhspetszvyazku-onovlyuye-vymohy-do-kiberzakhystu-zatverdzheno-novi-standarty-na-osnovi-2-0.

30. Деякі питання щодо спеціальних технічних засобів для зняття інформації з каналів зв'язку та інших технічних засобів негласного отримання інформації: Постанова КМУ від 22 вересня 2016 р. № 669. URL : https://zakon.rada.gov.ua/laws/show/669-2016-%D0%BF#Text.

31. Дзюндзюк В. Б., Дзюндзюк Б. В. Поява і розвиток кіберзлочинності. *Державне будівництво.* 2013. № 1. С. 4–12.

32. Дмитренко Н. А. Віктимологічні аспекти кібершахрайства в умовах війни. *Вісник Ужгородського національного університету*. Серія: Право. 2025. № 48. С. 145-160.

33. Дручек О. В. Посттравматичний стресовий розлад як фактор кіберзлочинної поведінки ветеранів. *Психологічний журнал*. 2025. № 4. С. 101-115.

34. Дудоров О. О. Шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки. URL : http://dudorov.com.ua/images/download/tezy-st-190kk-eom.pdf.

35. Думчиков М. О. Концептуальні засади кримінально-правової охорони кіберпростору в Україні : дис. ... д-ра юрид. наук : 12.00.08 / Дніпров. держ. ун-т внутр. справ. Дніпро, 2024. 450 с.

36. Думчиков М. О. Процеси диджиталізації і криміналістика: ретроспективний аналіз. Криміналістика і судова експертиза. 2020. Вип. 65. С. 100–108.

37. Еверт О. В. Міжнародна співпраця у протидії кіберзлочинності: досвід України 2022-2025. *Міжнародне право*. 2025. № 4. С. 112-128.

38. Закалюк А. П. Курс сучасної української кримінології: теорія і практика: У 3 кн. Київ : Видавничий Дім «ІнЮре», 2007. Кн. 1: Теоретичні засади та історія української кримінологічної науки. 424 с.

39. Звіт про діяльність Департаменту кіберполіції Національної поліції України у 2024 році : офіційний сайт кіберполіції Украйни. URL : https://cyberpolice.gov.ua/news/zvitpro-diyalnist-departamentu-kiberpolicziyi-naczionalnoyi-policziyi-ukrayiny-u--roczi-7074/.

40. Зінченко О. І. Протидія кібертероризму як загрозі сучасній національній безпеці держав Європейського регіону : дис. ... д-ра філос. наук : 052 / Харків. нац. ун-т ім. В. Н. Каразіна. Харків, 2025. 275 с.

41. Зінченко С. С. Фішинг та deepfake: нові виклики для кібербезпеки України. *Вісник Національної академії правових наук України*. 2025. № 3. С. 78-92.

42. Інформація про стан кіберзлочинності в Україні : щорічний звіт Департаменту кіберполіції Національної поліції України за 2025 рік. URL : https://cyberpolice.gov.ua/ (дата звернення: 19.02.2026).

43. Казначеєва Д. В. Кібершахрайство як соціальна інженерія в умовах воєнного стану. *Аналітично-порівняльне правознавство*. 2025. № 1. С. 56-71.

44. Кальман О. Г., Христич І. О. Злочинність в Україні: основні тенденції. URL : http://dspace.nlu.edu.ua/bitstream/123456789/10141/1/Kalman_Xristich_41-56.pdf. 12 с.

45. Калюга К. В. Кримінологічна типологія кіберзлочинців: оновлений підхід. *Кримінологія та кримінально-виконавче право*. 2025. № 3. С. 45-60.

46. Кіберполіція України. Аналітичний огляд кіберзлочинності за 2024-2025 рр. Київ, 2026.

47. Кіберполіція України. Щорічний звіт про стан протидії кіберзлочинам за 2025 рік. Київ, 2026.

48. Кодекс України про адміністративні правопорушення від 7 грудня 1984 р. URL : https://zakon.rada.gov.ua/laws/show/8073-10#Text.

49. Коломієць Ю. Ю. Невідворотність кримінальної відповідальності: правова природа та зміст : автореф. дис. ... канд. юрид. наук : 12.00.08. Одеса, 2005. 17 с.

50. Конвенція про кіберзлочинність від 23.11.2001 р. URL : https://zakon.rada.gov.ua/laws/show/994_575#Text.

51. Конституція України. URL : https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text.

52. Корж І. Ф. Роль Telegram-каналів у поширенні кіберзлочинних інструментів. *Інформаційне право*. 2025. № 1. С. 67-82.

53. Кравцова М. О. Сусаний стан і напрями протидії кіберзлочинності в Україні. *Вісник кримінології асоціації України*. 2018. № 2(19). URL : https://dspace.univd.edu.ua/server/api/core/bitstreams/c451d2ca-1ebe-4be3-a50d-f86ca1b0e37f/content.

54. Кримінальна справа № 127/28630/22 // Архів Вінницького міського суду Вінницької області.

55. Кримінальна справа № 161/1717/15-к // Архів Луцького міськрайонного суду Волинської області.

56. Кримінальна справа № 201/10744/22 // Архів Жовтневого районного суду м. Дніпропетровська.

57. Кримінальна справа № 201/8123/25 // Архів Соборного районного суду м. Дніпра.

58. Кримінальна справа № 401/512/24 // Архів Світловодського міськрайонного суду Кіровоградської області.

59. Кримінальна справа № 404/10931/24 // Архів Фортечного районного суду м. Кропивницького.

60. Кримінальна справа № 444/3821/23 // Архів Жовківського районного суду Львівської області.

61. Кримінальна справа № 521/21166/25 // Архів Хаджибейського районного суду м. Одеси.

62. Кримінальна справа № 599/1222/25 // Архів Зборівського районного суду Тернопільської області.

63. Кримінальна справа №607/1658/15-к // Архів Тернопільського міськрайонного суду Тернопільської області.

64. Кримінальне право України: Особлива частина : підручник / Ю. В. Баулін, В. І. Борисов, В. І. Тютюгін та ін. ; за ред. В. В. Сташиса, В. Я. Тація. 4-те вид., переробл. і допов. Харків : Право, 2010. 608 с.

65. Кримінальний кодекс України: Закон України від 05 квітня 2001 р. / Верховна Рада України. URL : https://zakon.rada.gov.ua/laws/show/2341-14#Text.

66. Кримінологія : підручник / А. М. Бабенко, О. Ю. Бусол, О. М. Костенко та ін. ; за заг. ред. Ю. В. Нікітіна, С. Ф. Денисова, Є. Л. Стрельцова. – 2-ге вид., перероб. та допов. Харків : Право, 2018. 416 с.

67. Кримінологія : підручник / В. В. Голіна, Б. М. Головкін, М. Ю. Валуська та ін. ; за ред. В. В. Голіни, Б. М. Головкіна. Харків : Право, 2014. 440 с.

68. Кримінологія : підручник / О. М. Джужа, В. В. Василевич, В. В. Чернєй, С. С. Чернявський та ін. ; за заг. ред. д-ра юрид. наук, проф. В. В. Чернєя ; за наук. ред. д-ра юрид. наук, проф. О. М. Джужі. Київ : Нац. акад. внутр. справ, 2020. 612 с.

69. Кримінологія: академічний підручник: [Богатирьов І. Г., Колб О. Г., Топчій В. В. та ін.] за. заг. ред. доктора юридичних наук, професора, заслуженого діяча науки і техніки України Богатирьова І. Г. Чернівці: Технодрук, 2020. 336 с.

70. Кримінологія: Загальна та Особлива частини : підручник / І. М. Даньшин, В. В. Голіна, М. Ю. Валуйська та ін.; за ред. В. В. Голіни. 2-ге вид., переробл. і допов. Харків : Право, 2015. 440 с.

71. Кузьменко Ю. СБУ з початку року нейтралізувала понад 530 кібератак, більшість – справа російських спецслужб. URL : https://news.liga.net/ua/war/news/sbu-z-pochatku-roku-neytralizuvaly-ponad-530-kiberatak-bilshist-sprava-rosiyskykh-spetssluzhb?utm_source=fb&utm_medium=cpc&utm_campaign=social.

72. Кунтій А. І. Профілактика кіберзлочинності серед молоді в умовах воєнного стану. *Порівняльно-аналітичне право*. 2025. № 4. С. 112-125.

73. Лазаренко А. М. Кіберзлочинність в умовах воєнного стану. *Вісник кримінологічної асоціації України*. 2025. № 1. С. 89-104.

74. Ломброзо Ч. Злочинець / Ч. Ломброзо. Київ : Право, 2010.

75. Лугіна Н. А., Лучук А. М. Порівняльний аналіз вітчизняного та європейського законодавства з питань запобігання кіберзлочинності. *Ірпінський юридичний часопис:* науковий журнал. 2023. Вип. 1 (10). С. 180-187. с. 183.

76. Максименко М. І. Роль штучного інтелекту в еволюції кіберзлочинності. *Інформаційна безпека*. 2025. № 2. С. 34-47.

77. Мельник М. І., Хавронюк М. І. Науково-практичний коментар Кримінального кодексу України. 12-те вид., переробл. і допов. Київ : Дакор, 2025. 1350 с.

78. Методичні рекомендації щодо збору та обробки статистичних даних щодо кібератак, кіберінцидентів і заходів протидії у Державній службі спеціального зв'язку та захисту інформації України: затв. Наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 5 серпня 2025 року № 482. URL : https://cip.gov.ua/ua/docs/nakaz-administraciyi-derzhspeczv-yazku-vid-05-08-2025-482-pro-zatverdzhennya-metodichnikh-rekomendacii-shodo-zboru-ta-obrobki-statistichnikh-danikh-stosovno-kiberatak-kiberincidentiv-i-zakhodiv-protidiyi-u-derzhavnii-sluzhbi-specialnogo-zv-yazku-ta-zakhistu-informaciyi-ukrayini.

79. Михайлов В. О., Романенко О. В. Темна мережа (darknet) як динамічне середовище кіберпростору та інструмент для вчинення кримінальних правопорушень. DICTUM FACTUM. 2024. № 2(16). С. 265-275.

80. Морщавка Є. І. Кримінологічна характеристика кіберзлочинців: нові тенденції. *Кримінологія*. 2025. № 2. С. 67-82.

81. Наказ Адміністрації Держспецзв'язку від 30.01.2026 № 75 «Про затвердження Каталогу заходів з кіберзахисту, базових заходів з кіберзахисту, форми плану кіберзахисту та методичних рекомендацій щодо здійснення заходів з кіберзахисту» URL : https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-30-01-2026-75-pro-zatverdzhennya-katalogu-zakhodiv-z-kiberzakhistu-bazovikh-zakhodiv-z-kiberzakhistu-formi-planu-kiberzakhistu-ta-metodichnikh-rekomendacii-shodo-zdiisnennya-zakhodiv-z-kiberzakhistu.

82. Науково-практичний коментар Кримінального кодексу України/ за ред. М. І. Мельника, М. І. Хавронюка. 10-те вид., переробл. та допов. Київ : ВД «Дакор». 950 с.

83. Національний план реагування на кіберінциденти, кібератаки та кіберзагрози URL : https://zakon.rada.gov.ua/laws/show/1533-2025-%D0%BF#Text.

84. Нестерова І. А. Психологічний портрет кіберзлочинця: сучасні підходи. *Психологія і право*. 2024. № 3. С. 45-58.

85. Оперативний центр реагування на кіберінциденти ДЦКЗ прозвітував за І квартал 2026 року. URL : https://cip.gov.ua/ua/news/operativnii-centr-reaguvannya-na-kiberincidenti-dckz-prozvituvav-za-i-kvartal-2026-roku.

86. Орлюк О. П. Кібербезпека: правові та кримінологічні аспекти : монографія. Київ : Наукова думка, 2024. 368 с.

87. Павлова Т. О. Механізм формування кримінально протиправної поведінки. Матеріали 77-ї наук. конф. професорсько-викладацького складу і наукових працівників економіко-правового факультету Одеського національного університету імені І. І. Мечникова (23–25 листоп. 2022 р., м. Одеса) / відп. ред. О. В. Побережець ; ред. кол.: А. Л. Святошнюк, Т. В. Степанова та ін. Одеса : Олді+, 2022. С. 103-105.

88. Піцик Ю. М. Кіберзлочини проти власності: кримінально-правова та кримінологічна характеристика : автореф. дис. ... канд. юрид. наук : 12.00.08. Київ, 2019. 20 с.

89. План заходів на 2025 рік з реалізації Стратегії кібербезпеки України, затвердж. розпорядженням КМУ № 204-р від 7 березня 2025 року URL : https://zakon.rada.gov.ua/laws/show/204-2025-%D1%80#Text.

90. Подільчак О. М. Особа кіберзлочинця: кримінологічний портрет. *Право і суспільство*. 2024. № 3. С. 145-158.

91. Постанова Другої судової палати Касаційного кримінального суду у справі № 752/8994/22 від 04 липня 2024 р. URL : https://iplex.com.ua/doc.php?regnum=120244099.

92. Постанова Пленуму Верховного Суду від 06.11.2009 № 10 «Про судову практику у справах про злочини проти власності». URL : https://zakon.rada.gov.ua/laws/show/v0010700-09#Text.

93. Пояснювальна записка до проєкту Закону України “Про Кіберсили Збройних Сил України” С. 3. URL : https://itd.rada.gov.ua/7182191a-6958-4d49-a0ac-276d693dc8dd

94. Про авторське право і суміжні права: Закон України від 1 грудня 2022 р.. URL : https://zakon.rada.gov.ua/laws/show/2811-20#Text.

95. Про державну підтримку медіа, гарантії професійної діяльності та соціальний захист журналіста: Закон України від 05.04.2001. URL : https://zakon.rada.gov.ua/laws/show/540/97-%D0%B2%D1%80#Text.

96. Про державну таємницю : Закон України від 21.01.1994 № 3855-XII (зі змінами). URL : https://zakon.rada.gov.ua/laws/show/3855-12.

97. Про електронні комунікації : Закон України від 16.12.2020 № 1089-IX. URL : https://zakon.rada.gov.ua/laws/show/1089-20.

98. Про затвердження Порядку взаємодії суб’єктів національної системи реагування на кіберінциденти, кібератаки, кіберзагрози із суб’єктами забезпечення кібербезпеки, правоохоронними, контррозвідувальними, розвідувальними органами та суб’єктами оперативно-розшукової діяльності : Постанова Кабінету Міністрів України від 13 листопада 2025 р. № 1471. URL : https://zakon.rada.gov.ua/laws/show/1471-2025-%D0%BF#Text.

99. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 5 липня 1994 р. URL : https://zakon.rada.gov.ua/laws/show/uk-sq/80/94-%D0%B2%D1%80#Text.

100. Про інформацію : Закон України від 02.10.1992 № 2657-XII (зі змінами). URL : https://zakon.rada.gov.ua/laws/show/2657-12.

101. Про кінематографію: Закон України від 13 січня 1998 р. URL : https://zakon.rada.gov.ua/laws/show/9/98-%D0%B2%D1%80#Text.

102. Про Національний координаційний центр кібербезпекиказ Президента України від 7 червня 2016 року №242/2016. URL : https://www.president.gov.ua/documents/2422016-20141.

103. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 р. URL : https://zakon.rada.gov.ua/laws/show/2163-19#Text.

104. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України від 26 серпня 2021 р. № 447/2021. URL : https://zakon.rada.gov.ua/laws/show/447/2021#n12.

105. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : Указ Президента України від 15.03.2016 р. № 96/2016. URL : https://www.president.gov.ua/documents/962016-19836.

106. Профілактика злочинів : підручник / О. М. Джужа, В. В. Василевич, О. Ф. Гіда та ін.; за заг. ред. д-ра юрид. наук, проф. О. М. Джужі. Київ : Атіка, 2011. 720 с.

107. Пузиревський М. В. Інсайдерські загрози в умовах гібридної війни. *Національна безпека: право, політика, економіка*. 2025. № 1. С. 89-102.

108. Регламент комісії (ЄС) № 617/2013 від 26 червня 2013 року про імплементацію Директиви Європейського Парламенту і Ради 2009/125/ЄС стосовно вимог до екодизайну для комп'ютерів і комп'ютерних серверів. URL : https://zakon.rada.gov.ua/laws/show/984_010-13/ed20130626#n31.

109. Русецький А. А., Куцолабський Д. А. Теоретико-правовий аналіз понять «кіберзлочин» і «кіберзлочинність». *Право і безпека*. 2017. № 1 (64). С. 74-78. с. 75.

110. Сміян Л. С., Нікітін Ю. В. Кримінологія: підручник / за заг. ред. Л. С. Сміяна, Ю. В. Нікітіна. Київ : Національна академія управління, 2010. 496 с.

111. Статистичні звіти «Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування» за 2013 – 2025 р.р., підготовлені Генеральною прокуратурою України. URL : https://new.gp.gov.ua/ua/posts/statistika.

112. Телейчук В. Г. Хактивізм як форма кіберзлочинності: кримінологічний аналіз. *Право України*. 2025. № 5. С. 123-138.

113. Український досвід змінює світову кібербезпеку. Рада національної безпеки і оборони: веб-сайт. URL : https://www.rnbo.gov.ua/ua /Diialnist/7376.html.

114. Фіалка М. І. Показники злочинності. *Вісник Асоціації кримінального права України*, 2016, № 2(7). С.361-367.

115. Хавронюк М. І. Кримінальне право України. Особлива частина : підручник. Київ : Ваіте, 2023. 512 с.

116. Черниш М. О. Теоретико-прикладні засади запобігання кримінальним правопорушенням проти довкілля: дис. на здобуття наукового ступеня доктора наук за спеціальністю 12.00.08 – кримінальне

право та кримінологія; кримінально-виконавче право. Дніпровський державний університет внутрішніх справ, Дніпро, 2025. 374 с.

117. Шкута О. О. Профілактика кіберзлочинності серед студентів технічних вишів. *Освіта і право*. 2025. № 2. С. 89-104.

118. Щорічний звіт Департаменту кіберполіції Національної поліції України за 2025 рік : Кіберполіція Уряїни : веб-сайт. URL : https://cyberpolice.gov.ua/news/shhorichnyj-zvit-7096/.

119. Ягунов Д. В. Кіберзлочинність в Україні: стан, структура, динаміка (2018-2025) : монографія. Київ : НАВС, 2025. 248 с.

120. Akyazi U., van Eeten M. J. G., & Hernandez Ganan, C. *Measuring Cybercrime-as-a-Service Offerings in a Cibercrime forum*. *Workshop on the Economics of Information Security* (28-29 jun. 2021). URL : https://pure.tudelft.nl/ws/portalfiles/portal/94649359/WEIS2021_Measuring_CaaS_Offerings_in_a_Cybercrime_Forum.pdf.

121. Baezner M. Synthesis 2017: Cyber-conflicts in perspective (Hotspot Analysis). Zürich: Center for Security Studies (CSS), ETH Zürich, 2018. URL : https://ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2018-06.pdf.

122. CrowdStrike. 2025 Global Threat Report. Sunnyvale : CrowdStrike, 2025.

123. CrowdStrike. Adversary Pursuit Report: Russia-Ukraine Cyber Conflict 2025. Sunnyvale, 2025.

124. Cybersecurity Ventures. *Cybercrime To Cost The World $10.5 Trillion Annually By 2025*. URL : https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021.

125. D. Abraham, S. Hilde Houmb, L. Erdodi Cyber-Attacks on Energy Infrastructure – A. Literature Overview and Perspectives on the Current Situation. *Applied Sciences* (2025). URL : https://www.mdpi.com/2076-3417/15/17/9233 (p. 19).

126. DataReportal. Digital 2021: Global Overview Report. Singapore: We Are Social & Hootsuite, – January 2021. 299 p. (p. 15-18). URL : https://datareportal.com/reports/digital-2021-global-overview-report?utm_source=chatgpt.com.

127. DataReportal. Digital 2025: Ukraine. Singapore: We Are Social & Hootsuite, February 2025. 45 p.

128. Didkivska H. V., Elshad R.I. Topical issues of counteracting cybercrime in Ukraine. *Ірпінський юридичний часопис.* 2025. № 1(18). С. 182-188.

129. ENISA THREAT LANDSCAPE 2024. European Union Agency for Cybersecurity (ENISA), 2024. 131 p. (p. 17-18). DOI: 10.2824/0710888. URL : https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf.

130. Europol. Internet Organised Crime Threat Assessment (IOCTA) 2025. – The Hague : Europol, 2025. 112 p.

131. Europol. Internet Organised Crime Threat Assessment (IOCTA). 2025. Luxembourg: Publications Office of the European Union, 2025. URL : https://ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2018-06.pdf.

132. Exercise Cyber Coalition, NATO's flagship Cyber Defence exercise, concludes in Estonia. URL : https://shape.nato.int/news-archive/2025/exercise-cyber-coalition--natos-flagship-cyber-defence-exercise--concludes-in-estonia.

133. Federal Bureau of Investigation. 2024 Internet Crime Report. Washington, D.C.: Internet Crime Complaint Center (IC3), 2025. 28 с. (с. 4–5, 6, 8, 12). URL : https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.

134. Google Threat Analysis Group. Adversarial Threat Landscape Report 2025. Mountain View : Google, 2025.

135. Grabosky P. Cybercrime and Security. Cheltenham : Edward Elgar, 2010.

136. Holt T. J., Bossler A. M. Cybercrime in Progress. London : Routledge, 2016.

137. INTERPOL. Global Cybercrime Strategy 2024-2026. Lyon : INTERPOL, 2025.

138. Kshetri N. The Global Cybercrime Industry. Berlin : Springer, 2010.

139. Leukfeldt E. R., Holt T. J. (eds.). Cybercrime: An Introduction to an Emerging Phenomenon. New York : McGraw-Hill, 2021.

140. Mandiant (Google Cloud). M-Trends 2025: Ukraine-Russia Cyber Warfare Insights. 2025.

141. McGuire M. Into the Web of Profit: The Cybercrime Threat. Bromium Report, 2019.

142. Merton R. K. Social Structure and Anomie. *American Sociological Review*. 1938. Vol. 3, No. 5. P. 672–682. URL : https://www.csun.edu/~snk1966/Robert%20K%20Merton%20-%20Social%20Structure%20and%20Anomie%20Original%201938%20Version.pdf.

143. Microsoft Digital Defense Report 2025 Lighting the path to a secure future/ A Microsoft Threat Intelligence report October 2025. 85 p. (p.11). URL : https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/Microsoft-Digital-Defense-Report-2025.pdf.

144. MISP: Платформа для обміну інформацією про кіберзагрози та її значення для України. URL : https://cybersec.net.ua/statti/907-misp-platforma-dlia-obminu-informatsiieiu-pro-kiberzahrozy-ta-ii-znachennia-dlia-ukrainy.html.

145. No More Ransom Project. Annual Report 2025.

146. Palo Alto Networks Unit 42. 2025 Cloud Threat Report. Santa Clara, 2025.

147. Turner A. B., McCombie S., & Uhlmann A. J. (2020). *Analysis Techniques for Illicit Bitcoin Transactions*. *Frontiers in Computer Science*, 2:600596. URL : https://www.frontiersin.org/journals/computer-science/articles/10.3389 /fcomp.2020.600596/full.

148. Wall D. Cybercrime: The Transformation of Crime in the Information Age. Cambridge : Polity Press, 2007. 272 p.

149. Yar M. Cybercrime and Society. London : SAGE, 2013.

Навчальне видання

ЗАПОБІГАННЯ КІБЕРЗЛОЧИННОСТІ

Навчальний посібник

Колектив авторів

Редактор, оригінал-макет – *Самотуга А. В.*
Редактор *Н. В. Леонова*

Підп. до друку 01.06.2026. Формат 60×84/16. Гарнітура – Times New Roman.
Папір офісний. Друк – цифровий. Ум.-друк. арк. 10,46. Обл.-вид. арк. 11,25.
Наклад – 20 прим. Зам. № 05/26-нп

Надруковано у Дніпровському державному університеті внутрішніх справ
49005, м. Дніпро, просп. Науки, 26, sed@dduvs.edu.ua
Свідоцтво про внесення до Державного реєстру видавців ДК № 8112 від 13.06.2024