УДК 343:13
DOI https://doi.org/10.24144/2307-3322.2025.91.4.8

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

**Жевелєва І.С.,**
*кандидат юридичних наук, доцент,*
*доцент НА СБ України*

**Жевелєва І.С. Кримінально правова кваліфікація правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.**

Стаття присвячена кримінально-правовій кваліфікації злочинів, пов'язаних із використанням електронно-обчислювальних машин, комп'ютерних систем, мереж та засобів електрозв'язку. У статті здійснено комплексний аналіз положень розділу XVI Кримінального кодексу України, що встановлює кримінальну відповідальність за правопорушення вчиненні у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, зокрема: статті 361, 361[1], 361[2], 362, 363 та 363[1] КК України, з урахуванням практики їх застосування в умовах воєнного стану.

Розглянуто склад вищезгаданих кримінальних правопорушень, визначено їхній об'єкт, суб'єкт, об'єктивну та суб'єктивну сторони, а також особливості кваліфікації. Окрему увагу, приділено механізму незаконного втручання в роботу комп'ютерних систем, створенню та поширенню шкідливого програмного забезпечення, несанкціонованому розповсюдженню інформації з обмеженим доступом і порушенню правил експлуатації мереж.

Встановлено, що зазначені кримінальні правопорушення дедалі частіше використовуються країною-агресором як інструмент ведення гібридної війни, підготовки або прикриття більш тяжких злочинів проти основ національної безпеки – державної зради, шпигунства, диверсії, колабораційної діяльності, фінансування тероризму, пропаганди війни та посягання на територіальну цілісність України. Виявлено тенденції до зростання використання кіберзасобів у гібридних війнах, що потребує оновлення законодавчої бази та підходів до кримінально-правового реагування.

У статті висвітлено сучасні виклики у сфері протидії сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, серед яких недосконаліть методів розслідування, складність ідентифікації зловмисників, недостатність міжнародної співпраці та швидка адаптація злочинців до нових механізмів контролю.

У роботі зроблено висновок, що чинні норми КК України забезпечують лише базовий рівень кримінально-правового захисту кіберпростору. З огляду на зростання кількості кіберзагроз у період збройної агресії рф, автор наголошує на необхідності вдосконалення термінологічного апарату, гармонізації українського законодавства з європейськими стандартами, уточнення кваліфікаційних критеріїв і посилення відповідальності за використання новітніх технологій у злочинних цілях.

Обґрунтовано доцільність розвитку механізмів фіксації та верифікації цифрових доказів, удосконалення взаємодії органів досудового розс*лідування, підрозділів кібербезпеки правоохоронних органів та Збройних Сил України у межах єдиної концепції кібероборони держави. Підкреслено важливість інтеграції методів OSINT у кримінально-правову діяльність для ефективнішого виявлення, документування та попередження кіберзлочинів.

**Ключові слова:** кримінально-правова кваліфікація, злочини, комп'ютерні мережі, кримінальне правопорушення, національна безпека, OSINT, інформаційна безпека, кібербезпека, кібероборона.

**Zhevelieva I.S. Criminal legal qualification of offenses in the field of use of electronic computing machines (computers), systems and computer networks and electric communication networks.**

The article is devoted to the criminal law qualification of offences related to the use of electronic computing machines, computer systems, networks, and telecommunication means. It provides a comprehensive analysis of the provisions of Chapter XVI of the Criminal Code of Ukraine, which establishes criminal liability for offences committed in the field of using electronic computing machines (computers), systems, computer networks, and telecommunication networks – in particular, Articles 361, 361[1], 361[2], 362, 363, and 363[1] of the Criminal Code of Ukraine – taking into account the practice of their application under martial law.

The article examines the elements of the aforementioned criminal offences, defining their object, subject, objective and subjective aspects, as well as specific features of qualification. Particular attention is paid to the mechanisms of unlawful interference with computer systems, the creation and dissemination of malicious software, the unauthorized distribution of information with restricted access, and violations of network operation rules.

It is established that these criminal offences are increasingly used by the aggressor state as instruments of hybrid warfare, for the preparation or concealment of more serious crimes against the foundations of national security – including state treason, espionage, sabotage, collaboration activities, financing of terrorism, war propaganda, and encroachment on the territorial integrity of Ukraine. The study reveals a growing trend in the use of cyber tools in hybrid wars, which necessitates updating the legal framework and approaches to criminal law response.

The article highlights current challenges in combating crimes involving the use of electronic computing machines, computer systems, networks, and telecommunication infrastructures. These include the imperfection of investigation methods, difficulties in identifying offenders, insufficient international cooperation, and the rapid adaptation of criminals to new control mechanisms.

The research concludes that the existing provisions of the Criminal Code of Ukraine ensure only a basic level of criminal law protection of cyberspace. Given the growing number of cyber threats during the armed aggression of the Russian Federation, the author emphasizes the need to improve the legal terminology, harmonize Ukrainian legislation with European standards, refine qualification criteria, and strengthen criminal liability for the use of advanced technologies in criminal activities.

The article substantiates the importance of developing mechanisms for the recording and verification of digital evidence, enhancing cooperation between investigative bodies, cybersecurity units of law enforcement agencies, and the Armed Forces of Ukraine within a unified concept of the state's cyber defence. The integration of OSINT methods into criminal law activities is emphasized as a key element for improving the detection, documentation, and prevention of cybercrimes.

**Key words:** criminal law qualification, crimes, computer networks, criminal offence, national security, OSINT, information security, cybersecurity, cyber defence.

**Постановка проблеми.** У XXI столітті кіберзлочинність стала невидимим фронтом, на якому розгортається безперервна боротьба за безпеку даних, систем та цифрового простору. Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, передбачені розділом XVI Особливої частини Кримінального кодексу України (далі – КК України), не лише підривають інформаційну стабільність, а й можуть бути використані для готування до тяжчих злочинів – від шпигунства до диверсій.

Статистичні дані Генеральної прокуратури України свідчать про суттєве зростання кіберзлочинів починаючи з 2020 року, з піковими значеннями у 2022 році. Це пов'язано як із загальною цифровізацією, так і з військовою агресією, що активізувала використання кіберпростору у гібридних війнах. Водночас, після 2022 року спостерігається поступове зниження кількості реєстрацій злочинів, що пов'язано з адаптацією правоохоронних органів до ефективної протидії, також покращенням забезпечення кібербезпеки на рівні державних установ та приватного сектору [1].

Актуальність теми також можна аргументувати рядом труднощів, пов'язаних із правовою кваліфікацією кримінальних правопорушень у кіберпросторі. Особлива складність полягає в тому, що така злочинна діяльність зазвичай здійснюється конспіративно та негласно.

Попри зростаючу кількість розслідуваних кримінальних правопорушень, рівень латентної кіберзлочинності залишається високим. А основними викликами для правоохоронної системи

залишається відсутність достатньої кількості спеціалістів у сфері кібербезпеки та OSINT-розвідки, потреба у розширенні обсягу підготовки фахівці з OSINT розслідувань та правових питань кваліфікації відповідних правопорушень. В умовах відкритої повномасштабної агресії, Україна повинна активно впроваджувати новітні технології для забезпечення безпеки держави, бізнесу та громадян у кіберпросторі.

**Метою дослідження** є аналіз складу кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, виклад авторського тлумачення норм закону, визначення подальшого можливого вдосконалення змісту проаналізованих статей, а також можливості використання вказаних кримінальних правопорушень у якості готування до інших більш суспільного небезпечних.

**Стан опрацювання проблематики**. Питання відповідальності за вказаним кримінальними правопорушеннями розглядається таким вітчизняними науковцями, як Яценко С.С., Іншин М.І., Пєтков С.В., Журавльов Д.В., Соболь Є.Ю., Коломоєць Т.О., Бандурка О.М., Мельник М.І., Дрозд О.Ю., Григоренко Л.С., Григоренко А.В., Бесчастний В.М., Оніщенко Н.М., Назимко Є.С., Копотун І.М., Лошицький М.В., Чубенко А.Г., Колб О.Г., Вітвіцький С.С., Пєтков В.П., Золотарьова М.К., Ховпун О.С., Бортняк В.А., Микитюк М.А., Павлюк О.О., Приймаченко Д.В., Скриньковський Р.М., Костицький В.В., Хмиз М.В., Шамрай Б.М., Цюх С.І., Хомишин М.А., Костицький М.В., Соловей Ю.Д., Соловей Я.М.

Крім того, частина науковців, зокрема, Минько О.В., Іохов О.Ю., Оленченко В.Т., Власов К.В. розглядали питання пов'язанні з OSINT та ідеями отримання інформації виключно з відкритих джерел, не враховуючи правові аспекти.

На сьогодні в науковій спільноті існують різні підходи до визначення поняття OSINT (Open Source Intelligence). Зокрема, Н.Ф. Ржевська та О.О. Кожушко, узагальнюючи праці зарубіжних дослідників, розглядають OSINT як форму процесу організації та управління збором розвідувальних даних, що охоплює пошук, відбір, добування та аналіз інформації з метою формування розвідувального документа для прийняття рішень [2]. Проте у наукових роботах цих авторів не в повній мірі розкриті питання правового регулювання.

Аналіз вітчизняної наукової літератури свідчить про недостатню увагу дослідників до питань кримінально-правової кваліфікації злочинів сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Натомість основний фокус таких досліджень зосереджено на алгоритмах пошуку інформації, методах її аналізу та процесах ухвалення управлінських рішень на основі отриманих даних.

**Виклад основного матеріалу**. Чинним КК України [3] у розділі «Злочини, вчинені у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» виділено 6 видів злочинів, що посягають на кібербезпеку. Сама назва розділу змінювалась двічі: Законом № 908-IV від 05.06.2003 та № 2617-VIII від № 22.11.2018.

Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку використовуються країною агресором, окупантами рф, для вчинення більш тяжких кримінальних правопорушень проти України.

Аналізуючи типологію злочинів у цій сфері, можна виділити кілька основних напрямків:

За характером дій: *несанкціоноване втручання* – несанкціонований доступ до інформаційних систем (ст. 361 КК України); *створення та розповсюдження шкідливих програм* – написання, продаж або використання програм для злому систем (ст. 361-1 КК України); *несанкціоноване розповсюдження інформації* – продаж або поширення даних з обмеженим доступом (ст. 361-2 КК України); *порушення правил експлуатації* – дії, що призводять до шкоди через неналежне використання техніки (ст. 363 КК України); *перешкоджання роботі мереж* – DDoS-атаки або масова розсилка спаму (ст. 363-1 КК України).

За способом вчинення: *індивідуальні* – вчинені окремою особою (наприклад, злом комп'ютера); *групові* – вчинені за попередньою змовою групою осіб (організовані кібератаки); *автоматизовані* – використання ботів або шкідливих програм без прямої участі людини.

За наслідками: *легкі* – незначне втручання, що не призвело до суттєвих збитків; *середні* – втручання, яке призвело до втрати або зміни інформації; *тяжкі* – атаки, що спричинили великі збитки, техногенні аварії чи загрозу життю людей.

За мотивами: *кримінальні* – з метою збагачення або шантажу; *ідеологічні* – хактивізм, політичні мотиви; *хуліганські* – задля розваги чи демонстрації навичок.

Аналіз статистичних даних вказує на певну кореляцію між кількістю зареєстрованих кіберзлочинів та числом справ, скерованих до суду. У періоди зростання кількості кіберзлочинів (2021-2022 роки) число направлених до суду справ також збільшувалася, однак із запізненням у кілька місяців, що свідчить про затримку в процесах розслідування та збору доказів. Водночас значна частина кримінальних правопорушень залишається нерозкритою через складність ідентифікації зловмисників, які часто використовують анонімізацію та інструменти приховування слідів у мережі [4].

Автор пропонує проводити аналіз кримінальних правопорушень, вказаних у розділі XVI КК України за наступною схемою: об'єктивна сторона; суб'єкт; суб'єктивна сторона; об'єкт.

Ст. 361 КК України «Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку».

Об'єктивна сторона правопорушення, передбаченого частиною першою цієї статті, може полягати у незламному втручанні в роботу вказаних систем або мереж. Вказане втручання полягає у будь-яких діях суб'єкту правопорушення, які впливають на сукупність операцій, що здійснюються з використанням вказаних систем або мереж. Таке втручання може приводити до перекручення або знищення інформації або її носіїв. Цей злочин слід рахувати закінченим у тому разі, коли перекручення чи знищення інформації мали місце.

Частина друга ст. 361 КК України передбачає відповідальність за ті самі дії, вчинені повторно або за попередньою змовою групою осіб.

Повторність кримінальних правопорушень визначена частиною першою ст. 32 КК України і полягає у вчиненні двох або більше кримінальних правопорушень, передбачених тією самою статтею або частиною статті Особливої частини КК України.

Попередня змова групи осіб визначена частиною другою ст. 28 КК України, як вчинення кримінального правопорушення групою осіб (дві або більше), які заздалегідь, тобто до початку кримінальних правопорушень, домовилися про спільне його вчинення.

Частина третя ст. 361 КК України передбачає відповідальність за дії, передбачені частиною першою або другою цієї статті, якщо вони призвели до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації.

Частина четверта статті 361 КК України передбачає відповідальність за дії, передбачені частиною першою або другою цієї статті, якщо вони заподіяли значну шкоду чи створили небезпеку тяжких технологічних аварій або екологічних катастроф, загибелі або масового захворювання населення чи інших тяжких наслідків. Значна шкода визначена приміткою до ст. 361 КК України, як така, яка в триста і більше разів перевищує неоподаткований мінімум доходів громадян.

Факт створення небезпеки тяжких технологічних аварій або екологічних катастроф, загибелі або масово захворювання населення чи інших тяжких наслідків у кожному разі встановлює слідство та суд за допомогою відповідної експертизи.

Частина п'ята ст. 361 КК України передбачає відповідальність за неї, передбачені частиною третьою або четвертою цієї статті, вчинені під час дії воєнного стану.

Воєнний стан – це особливий правовий режим, що вводиться в Україні або в окремих її місцевостях у разі збройної агресії чи загрози нападу, небезпеки державній незалежності України, її територіальній цілісності та передбачає надання відповідним органам державної влади, військовому командуванню, військовим адміністраціям та органам місцевого самоврядування повноважень, необхідних для відвернення загрози, відсічі збройної агресії та забезпечення національної безпеки, усунення загрози небезпеки державній незалежності України, її територіальній цілісності, а також тимчасове, зумовлене загрозою, обмеження конституційних прав і свобод людини й громадянина та прав і законних інтересів юридичних осіб із зазначенням строку дії цих обмежень [5].

Частина шоста ст. 361 КК України відзначає, що дії, передбачені частинами першою - четвертою цієї статті, не вважаються несанкціонованим втручанням в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, якщо вони були вчинені відповідно до порядку пошуку та виявлення потенційних вразливостей таких систем чи мереж.

Ст. $361^1$ КК України «Створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут» у першій частині передбачає відповідальність за частиною першою ст. $361^1$, створення з метою протиправ-

ного використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж.

Шкідливі програми чи технічні засоби – це такі, що завдають шкоди, тобто матеріальних витрат, збитків кому- або чому-небудь [6, с. 220]. Вони є предметом кримінального правопорушення.

Об'єктивна сторона цього кримінального правопорушення може полягати у створенні шкідливих програм або технічних засобів, метою чого є їх подальше використання, розповсюдження або збут.

Частина друга ст. $361^{1}$ КК України передбачає відповідальність за ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду,.

Ст. $361^{2}$ КК України «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», у першій частині передбачає відповідальність за 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, створеної та захищеної відповідно до чинного законодавства.

Будь-яка інформація, якщо вона створена на законних підставах та захищена законодавством, є предметом даного кримінального правопорушення.

Об'єктивна сторона цього кримінального правопорушення полягає в несанкціонованому збуті або розповсюдженні комп'ютерної інформації з обмеженим доступом.

Збут вказаної комп'ютерної інформації є її оплатна або безоплатна передача іншій особі або іншим особам, які не мають права офіційного доступу до неї.

Розповсюдження – розміщення в АС чи комп'ютерній мережі з наданням вільного доступу до неї – це можуть бути також інші будь-які діяння, що створюють можливість вільного доступу до неї невизначеного кола осіб.

Кримінальне правопорушення може бути вчинено як особою, що мала офіційний доступ до цієї інформації, так і такою, що такого доступу не мала.

Частина друга ст. $361^{2}$ КК України передбачає відповідальність за ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду.

Ст. 362 КК України передбачає відповідальність за несанкціоновані зміну, знищення або блокування інформації, яка обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах, або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї.

Предметом даного кримінального правопорушення є інформація цього кримінального правопорушення, що обробляється у вказаних системах або мережах та зберігається на відповідних носіях. Це може бути інформація з обмеженим доступом або комп'ютерна інформація, доступ до якої є платним.

Об'єктивна сторона цього кримінального правопорушення – вчинення до відповідної комп'ютерної інформації будь-який з вказаних у її диспозиції дій, а саме: зміни; знищення, перехоплення, копіювання інформації, яка обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, якщо це призвело до її витоку, вчинені особою, яка має право доступу до такої інформації. Обов'язковою ознакою закінченого кримінального правопорушення є така його ознака як суспільно небезпечні наслідки – витік інформації.

Частина друга ст. 362 КК України передбачає відповідальність за несанкціоновані перехоплення або копіювання інформації, яка обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, якщо це призвело до її витоку, вчинені особою, яка має право доступу до такої інформації.

Частина третя ст. 362 КК України передбачає відповідальність за неї, передбачені частиною першою або другою цієї статті, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду.

Ст. 363 КК України «Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або поряд-

ку, чи правил захисту інформації, яка в них обробляється». У першій частині передбачає відповідальність за 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, якщо це заподіяло значну шкоду, вчинені особою, яка відповідає за їх експлуатацію.

Як бачимо, об'єктивна сторона цього кримінального правопорушення характеризується порушенням вказаних правил, що можуть вчинятись як шляхом дій, так і бездіяльності. Обов'язковою ознакою закінчення цього кримінального правопорушення спричинення злочинної шкоди.

Ст. 363[1] КК України «Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку» у частині передбачає кримінальну відповідальність за умисне масове розповсюдження повідомлень електрозв'язку, здійснене без попередньої згоди адресатів, що призвело до порушення або припинення роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

Об'єктивна сторона кримінального правопорушення характеризується масовим розповсюдженням повідомлень електронного зв'язку без попередньої згоди адресатів. Обов'язковим наслідком таких дій для визнання кримінальної відповідальності закінченим актом вказує порушення або припинення роботи вказаних ЕОМ, систем або мереж.

Масовими такі розповсюдження слід вважати, якщо вони утворюються з використанням можливостей комп'ютера та розміщуються автоматично на різних адресатах. У будь-якому разі масовість є поняттям оцінювальним і встановлюється слідчим і судом. Попередня згода адресата на отримання цієї інформації при цьому відсутня.

Порушенням роботи ЕОМ, систем або мереж є зміна параметрів процесу обробки інформації. Це може бути прискорення, уповільнення цього процесу, припинення обробки інформації у будь-якій її частині або в цілому, перекручення результатів її обробки тощо. Припинення роботи ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку – це зупинка не деякий час обробки інформації, що в них знаходиться.

Частина 2 ст. 363[1] КК України передбачає відповідальність за дії, вчинені повторно або за попередньою змовою групою осіб, якщо вони заподіяли значну шкоду.

Суб'єкт кримінальних правопорушень передбачених розділом XVI Особливої частини КК України фізична осудна особа, що досягла віку 16 років.

У кримінальних правопорушеннях, передбачених ст. 362 КК України, ст. 363 КК України суб'єкт кримінального правопорушення – це особа, яка має право доступу до такої інформації або відповідає за експлуатацію автоматизованої системи, комунікативних мереж чи мереж електрозв'язку.

Суб'єктивна сторона кримінального правопорушення передбаченого ст.ст. 361, 361[1], 362[2], 362, 363 КК України – прямий умисел.

Передбачене ст. 363 КК України, може вчинятися як умисно, так і з необережності. Об'єкт цих кримінальних правопорушень – встановлений порядок використання електронно-обчислюваних машин (комп'ютерів) систем та комп'ютерних мереж електрозв'язку.

У разі розслідування кримінальних правопорушень, пов'язаних з використанням електронно обчислюваних машин (комп'ютерів) систем та комп'ютерних мереж і мереж електрозв'язку, які можуть використовуватись для вчинення найбільш тяжких злочинів, особливу увагу слід приділяти змісту суб'єктивної сторони, аналізуючи не лише умисел, а і мету.

Так, несанкціоноване втручання в роботу інформаційних (автоматизованих), електричних комунікаційних систем, електронних комунікаційних мереж (ст. 361 КК України, 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) можуть вчинятись з метою поширення публічних закликів до насильницької зміни чи повалення конституційного ладу або до захоплення державної влади, а також розповсюдження матеріалів із закликами до вчинення таких дій (ч. 2 та ч. 3 ст. 109 КК України).

Дії, передбачені ст. 361 та ст. 362 КК України, можуть також вчиняти з метою пропаганди війни (ст. 436 КК України), пропаганди комуністичної або нацистської символіки та пропаганди комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів, виправдування,

визнання правомірною, заперечення збройної агресії рф проти України, глорифікація її учасників, створення для групи життєвих умов, спрямованих на повне чи часткове її фізичне знищення.

Ті ж кримінальні правопорушення, передбачені ст. 361[1] КК України, можуть використовуватись для вчинення державної зради у формі шпигунства (ч. 1 та ч. 2 ст. 111 КК України) або шпигунства (ст. 114 КК України), деяких форм колаборaційної діяльності ч. 1, 3, 6 ст. 111[1] КК України), перешкоджання законної діяльності Збройних сил України та інших військових формувань (ст. 114[1] КК України), а також 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).

Крім того, кримінальні правопорушення, передбачені розділом XVI КК України можуть використовувати для фінансування дій, вчинених з метою насильницької зміни чи повалення конституційного ладу або захоплення державної влади, зміни меж території або державного кордону України (ст. 110[2] КК України), пособництва державі агресору (ст. 111[2] КК України).

Також ці ж кримінальні правопорушення можуть використовуватись при вчиненні диверсії (ст. 113 КК України) з метою дистанційного керування вчинення вибухів, підпалів або інших дій, спрямованих (ч. 1 або ч. 2 ст. 113 КК України), як і при посяганні на життя державного чи громадського діяча (ст. 112 КК України).

**Висновки.** Проведений аналіз положень розділу XVI Кримінального кодексу України дає підстави стверджувати, що система норм, спрямованих на забезпечення кібербезпеки держави, становить комплексний механізм правового захисту інформаційних ресурсів, електронно-обчислювальних машин, систем і мереж електрозв'язку. Водночас трансформація сучасних загроз, обумовлена збройною агресією російської федерації, свідчить про необхідність оновлення підходів до кримінально-правової охорони інформаційного простору.

Кримінальні правопорушення, передбачені у цьому розділі, дедалі частіше використовуються як інструмент для вчинення більш тяжких злочинів проти основ національної безпеки – державної зради, диверсій, шпигунства, колаборaційної діяльності та інформаційно-психологічних операцій, спрямованих на підрив суверенітету України. Це свідчить про інтеграцію кіберзлочинів у структуру сучасних інформаційних воєн, де комп'ютерні технології виступають не лише засобом злочину, але й зброєю у гібридному протиборстві.

Існуючі положення КК України охоплюють базові види протиправних діянь у сфері використання інформаційних систем, однак потребують подальшого уточнення термінологічного апарату, гармонізації з європейським законодавством та врахування нових форм злочинної активності.

З метою підвищення ефективності протидії таким посяганням доцільним є подальше вдосконалення кримінально-правових норм у частині уточнення термінологічного апарату, посилення відповідальності за використання новітніх технологій у злочинних цілях, а також розвиток механізмів фіксації та верифікації цифрових доказів. Важливим напрямом є налагодження системної взаємодії органів досудового розслідування, підрозділів кібербезпеки правоохоронних органів, а також військ зв'язку та кібербезпеки Збройних Сил України у межах єдиної концепції кібероборони держави.

**СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:**

1. Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування: веб-сайт Генеральної прокуратури України. URL: https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2 (дата звернення 14.10.2025).
2. Ржевська Н.Ф., Кожушко О.О. Розвідка відкритих джерел (OPEN SOURCE INTELLIGENCE). Україна в системі глобального інформаційного обміну: теоретико-методологічні аспекти дослідження і підготовки фахівців : всеукраїнська наукова конференція, Львів, 27 травня 2021 р. Львів :Видавництво Львівської політехніки, 2011. С. 257–261 URL: https://ena.lpnu.ua:8443/server/api/core/bitstreams/a964dfbb-a16d-4e8a-b621-9aa6cb277197/content.
3. Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14/print (дата звернення 14.10.2025).

4. Статистика розслідування і розгляду в судах кримінальних правопорушень, які пов'язані із здійсненням господарської та інвестиційної діяльності. URL: https://dashboard.gp.gov.ua (дата звернення 14.10.2025).
5. Про правовий режим воєнного стану: Закон України від 12.05.2015 № 389-VIII. URL: https://zakon.rada.gov.ua/laws/show/389-19/print (дата звернення 14.10.2025).
6. Волков О.О. Поняття шкідливого програмного засобу, призначеного для несанкціонованого втручання в роботу електронно-обчислювальної техніки. *Науковий вісник Національної академії внутрішніх справ,* 2018. № 1 (106). С. 217-231.