**УДК351:343.85 (477)**
DOI: https://doi.org/10.32689/2617-2224-2019-17-2-300-310

***Островий Олексій Володимирович,***
*здобувач наукового ступеня кандидата наук з державного управління, Донецький державний університет управління, 87513, м. Маріуполь, вул. Карпинського, 58, тел.: (050) 426 07 70, e-mail: ostrovalexsey@icloud.com*
*ORCID: 0000-0002-7704-5149*

***Островой Алексей Владимирович,***
*соискатель ученой степени кандидата наук по государственному управлению, Донецкий государственный университет управления, 87513, г. Мариуполь, ул. Карпинского, 58, тел.: (050) 426 07 70, e-mail: ostrovalexsey@icloud.com*
*ORCID: 0000-0002-7704-5149*

***Ostrovoy Aleksey Vladimirovich,***
*Applicant of Ph.D. in Public Administration, Donetsk State University of Management, 87513, Mariupol, Str. Karpinsky, 58, tel.: (050) 426 07 70, e-mail: ostrovalexsey@icloud.com*
*ORCID: 0000-0002-7704-5149*

# АНАЛІЗ УМОВ ФОРМУВАННЯ ДЕРЖАВНОЇ ПОЛІТИКИ ЗАБЕЗПЕЧЕННЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ В УКРАЇНІ

**Анотація.** Узагальнюються основні тенденції, особливості та проблеми, які безпосередньо впливають на формування державної політики забезпечення кібернетичної безпеки. Проаналізовано сучасний стан кіберзлочинності у світі та доведено її глобальний характер розповсюдження. Досліджено потенціал кібератак в Україні та виявлено, що його підвищення обумовлено такими тенденціями у діяльності підприємств та бізнесу, як зростання кількості комп'ютерної техніки, підвищення доступу до мережі Інтернет, а також збільшення рівня використання інформаційно-комунікаційних технологій у своїй діяльності. Виявлено постійно зростаючу тенденцію до збільшення кількості злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку в Україні, а також збільшення їх питомої ваги у загальній кількості злочинів в Україні. Узагальнено основні фактори, які сприяли зростанню кількості кіберзлочинів в Україні, серед яких як технічна і струк-

турна неготовність існуючої системи управління правоохоронних органів, так і недосконаліть державної політики. На підставі аналізу злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів) (за закінченими розслідуваннями у кримінальних провадженнях) сформовано "портрет" кіберзлочинця та доведено, що основною його рисою є високий кваліфікаційний рівень. Виявлено, що серед позитивних тенденцій у сфері боротьби з кіберзлочинністю в Україні на сьогодні можна спостерігати впровадження у практичну діяльність сучасних методик виявлення, фіксації і дослідження цифрових доказів; підписання договорів про взаємодію у сфері боротьби з кіберзлочинністю з організаціями різних країн світу; налагодження ефективної взаємодії зі світовими соціальними мережами.

**Ключові слова:** державна політика, кібернетична безпека, кіберзлочин, кібератака, інформаційно-комунікаційні технології.

## АНАЛИЗ УСЛОВИЙ ФОРМИРОВАНИЯ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ ОБЕСПЕЧЕНИЯ КИБЕРНЕТИЧЕСКОЙ БЕЗОПАСНОСТИ В УКРАИНЕ

**Аннотация.** Обобщаются основные тенденции, особенности и проблемы, которые имеют непосредственное влияние на формирование государственной политики обеспечения кибернетической безопасности. Проанализировано современное состояние киберпреступности в мире и доказан глобальный характер ее распространения. Исследован потенциал кибератак в Украине и обнаружено, что его повышение обусловлено такими тенденциями в деятельности предприятий и бизнеса, как рост количества компьютерной техники, повышение доступа к сети Интернет, а также увеличение уровня использования информационно-коммуникационных технологий в своей деятельности. Выявлена постоянно растущая тенденция к увеличению количества преступлений в сфере использования электронно-вычислительных машин (компьютеров), систем и компьютерных сетей и сетей электросвязи в Украине, а также увеличение их удельного веса в общем количестве преступлений в Украине. Обобщены основные факторы, которые способствовали росту числа киберпреступлений в Украине, среди которых как техническая и структурная неготовность существующей системы управления правоохранительных органов, так и несовершенство государственной политики. На основании анализа преступлений в сфере использования электронно-вычислительных машин (компьютеров) (по законченным расследованиям в уголовных производствах) сформирован "портрет" киберпреступника и доказано, что основной его чертой является высокий квалификационный уровень. Выявлено, что среди положительных тенденций в сфере борьбы с киберпреступностью в Украине на сегодняшний день можно наблюдать внедрение в практическую деятельность современных методик выявления, фиксации и исследования цифровых доказательств; подписание договоров о взаимодействии в сфере борьбы с киберпреступностью с организациями разных стран мира; налажи-

вание эффективного взаимодействия с известными мировыми социальными сетями.

**Ключевые слова:** государственная политика, кибернетическая безопасность, киберпреступность, кибератака, информационно-коммуникационные технологии.

## ANALYSIS OF THE CONDITIONS FOR THE STATE POLICY FORMATION TO ENSURE KIBERNETIC SECURITY IN UKRAINE

**Abstract.** The article summarizes the main tendencies, features and problems that have a direct impact on the state policy formation for ensuring cybernetic security. The present state of cybercrime in the world has been analyzed and its global distribution has been proved. The potential of cyberattacks in Ukraine has been investigated and its increase was determined by such tendencies in the activity of enterprises and business as the growth of the number of computer equipment, increase of access to the Internet, and also increase of the level of use of information and communication technologies in their activity. The tendency to increase the number of crimes in the sphere of the use of electronic computers, systems and computer networks and telecommunication networks in Ukraine, as well as an increase in their share in the total number of crimes in Ukraine has been revealed. The main factors that contributed to the increase in the number of cybercrime in Ukraine, including technical and structural unwillingness of the existing system of management of law enforcement agencies, and imperfection of the state policy, have beend generalized. On the basis of the analysis of crimes in the field of the use of electronic computers (after the investigation by criminal proceedings) a "portrait" of a cybercriminator has been formed and it has been proved that its main feature is a high qualification level. It has been revealed that among the positive trends in the field of combating cybercrime in Ukraine today it is possible to observe the introduction of modern methods of detection, fixation and research of digital evidence into practical activity; signing agreements on cooperation in the field of combating cybercrime with organizations from different countries of the world; establishing effective interaction with the world's most famous social networks.

**Keywords**: state policy, cybernetic security, cybercrime, cyberattack, information and communication technologies.

---

**Постановка проблеми.** Стрімкий розвиток інформаційно-комунікаційних технологій сприяв зростанню світового показника кількості користувачів мережі Інтернет до 4,021 млрд осіб (55,6 %) від усього населення Землі, поряд з яким спостерігається активізація використання соціальних медіа, зростання кількості користувачів мережі Інтернет, зокрема, в Україні кількість користувачів становить понад 25 млн осіб або 60,7 % населення країни. Слід зауважити, що зростання рівня

проникнення, використання інтернету та соціальних медіа приватними особами та компаніями по всьому світу, у свою чергу, сприяє розвитку інтернет-бізнесу. Однак взаємозв'язок між бізнес-моделями й операційною діяльністю надає можливості не тільки освоїти нові сфери діяльності, а й створити загрозу через посилення вразливості в комп'ютерних мережах та підвищити ризик виникнення кіберінцидентів. Зазначені тенденції мають безпосередній вплив на формування та реалізацію державної політики забезпечення кібернетичної безпеки, тому їх відстеження та перманентний аналіз набуває ключового значення для забезпечення національної безпеки в умовах сьогодення.

**Аналіз останніх досліджень і публікацій.** Проблемі забезпечення кібернетичної безпеки присвячено ряд наукових досліджень таких авторів, як А. Бабенко, Ю. Батурін, П. Біленчук, В. Бутузов, В. Вєхов, В. Гавловский, В. Голубєв, Д. Дубов, О. Книженко, М. Кравцова [4], В. Номоконов, В. Петров, М. Погорецький, І. Рязанцева, Н. Савчук, В. Шеломенцев та ін. Також значний внесок у дослідження цієї проблеми зробили провідні міжнародні організації та компанії, як KPMG International [1], Norton by Symantec [2] та ін. Однак, на сьогодні існує нагальна потреба в інтеграції теоретичного доробку з актуальними аналітичними даними у цій сфері, яка стрімко розвивається та трансформується, з метою вироблення ефективної державної політики забезпечення кібернетичної безпеки.

**Мета статті** полягає в обґрунтуванні основних умов, які прямо впливають на формування державної політики забезпечення кібербезпеки в Україні.

**Виклад основного матеріалу.** Кіберзлочинність вже давно стала глобальним явищем та проблемою, про що свідчить дослідження американської компанії Norton [2], за даними якого у 2017 р. 978 млн дорослих людей у 20 країнах (де проводилось дослідження) стикалися з глобальною кіберзлочинністю, що складає 44 % онлайн-користувачів. У результаті, споживачі, які стали жертвами кіберзлочинності, сумарно втратили 172 млрд доларів (в середньому 142 долари на жертву). Серед найбільш розповсюджених кіберзлочинів, які було відзначено, слід зазначити такі:

• наявність пристрою, зараженого вірусом чи іншою загрозою безпеці (53 %);

• проблеми з дебетовими або кредитними картами (38 %);

• усунення пароля облікового запису (34 %);

• несанкціонований доступ або хакерство електронної пошти чи облікового запису соціальних медіа (34 %);

• придбання онлайн, яке виявилося шахрайським (33 %);

• натискання на шахрайську електронну пошту або надання конфіденційної (особистої/фінансової) інформації у відповідь на шахрайство з електронною поштою (32 %).

За даними іншого дослідження, проведеного компанією KPMG International серед керівників компаній у різних країнах [1], близько половини керівників компаній (49 %) наголошують на можливості кібер-

атаки, не з точки зору "якщо", а саме "коли". При цьому у трійці лідерів, за оцінкою кібератаки як неминучої загрози для бізнесу, здійсненого за географічною ознакою, знаходяться США, Австралія та Німеччина (рис. 1). У галузевому розрізі найбільш підготовленою до кібератак стала сфера інфраструктури (67 %). Показово, що лише близько половини керівників підприємств (51 %) визначають значну підготовленість до кібератак.

Якщо окремо аналізувати потенціал кібератак в Україні, то насамперед слід звернути увагу на те, що на сьогодні за даними Державного комітету статистики України [3] на підприємствах можна констатувати зростання кількості комп'ютерної техніки (+2 % у 2017 р. порівняно з 2016 р.), підвищення доступу до мережі Інтернет (+2 % у 2017 р.) та збільшення рівня використання інформаційно-комунікаційних технологій у своїй діяльності, зокрема у 2017 р.:

+4 % підприємств, що мали вебсайт, який функціонував у мережі Інтернет;

+8 % підприємств, які використовували соціальні медіа (соціальні мережі, блоги чи мікроблоги підприємства, веб-сайти з мультимедійним вмістом, засоби обміну знаннями);

+13,6 % підприємств, що купували послуги хмарних обчислень упродовж року;

+4,5 % підприємств, які надавали рахунки-фактури в електронному/паперовому вигляді;

+3,7 % підприємств, що отримували замовлення через комп'ютерні мережі на продаж товарів або послуг (за винятком замовлень, отриманих електронною поштою);

+14 % підприємств, що здійснювали закупівлі через комп'ютерні мережі товарів або послуг (за винятком замовлень, отриманих електронною поштою).

Серед підприємств, які мали доступ до мережі Інтернет найбільша частка належить до сфери оптової та роздрібної торгівлі; ремонту автотранспортних засобів і мотоциклів, переробної промисловості та будівництва.

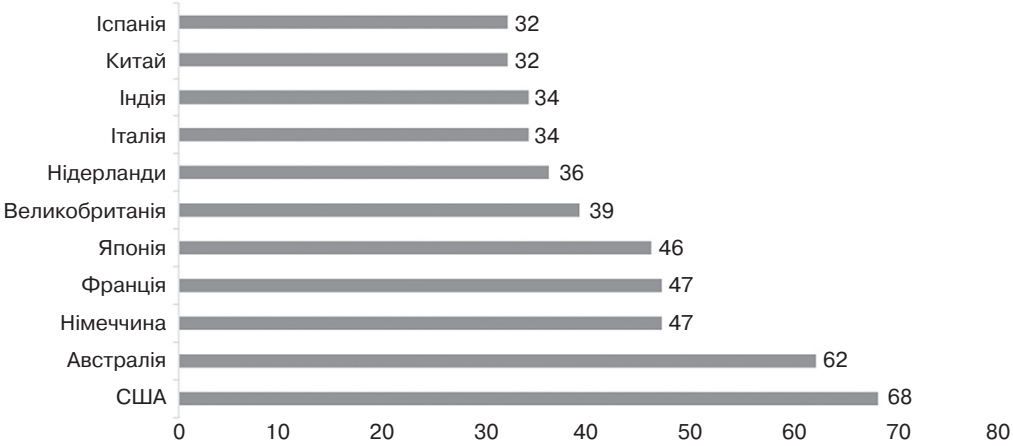


*Рис. 1.* **Оцінка кібератак як неминучої загрози для бізнесу,** %
*Джерело*: складено за даними [1].

Мережу Інтернет використовують у таких напрямах: надсилання чи отримання повідомлень електронною поштою; здійснення телефонних дзвінків за допомогою Інтернет/VoIP-зв'язку або відео-конференцій; отримання інформації про товари та послуги; користування миттєвим обміном повідомленнями та електронною дошкою оголошень; отримання інформації від органів державної влади; здійснення різноманітних операцій з органами державної влади (за винятком отримання інформації); здійснення банківських операцій; доступ до інших фінансових послуг.

Такі тенденції створили не лише передумови для розвитку підприємств та національної економіки в цілому, але й спричинили підвищення рівня злочинності у сфері інформаційно-комунікаційних технологій.

Відомості про зареєстровані кримінальні порушення (провадження) та результати їх розслідування узагальнюються у звітності за формою № 1 "Єдиний звіт про кримінальні правопорушення", яка формується щомісяця накопичувальним підсумком із початку звітного періоду (року) за регіоном вчинення злочину на підставі даних, внесених до Єдиного реєстру досудових розслідувань користувачами інформаційної системи, у розрізі розділів та статей Кримінального кодексу України, а про осіб, які їх вчинили — у звітності за формою № 2 "Єдиний звіт про осіб, які вчинили кримінальні правопорушення", за закінченими розслідуванням кримінальними провадженнями.

Так, зазначимо, що кількість злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, починаючи з 2014 р. постійно зростала, сягнувши у 2017 р. цифри 2573 злочини. Темп зростання за 2014–2017 рр. становив 480,8 %. За 8 місяців 2018 р. цей показник перевищив рівень 2016 р. на 117,9 %.

Випереджаюче зростання зареєстрованих кіберзлочинів вплинуло на збільшення їх питомої ваги у загальній кількості злочинів в Україні, зберігаючи тенденції підвищення від 0,08 % у 2014 р. до 0,51 у 2018, що є найвищим показником, починаючи з 2009 р.

Такі тенденції склалися під впливом ряду факторів. Серед основних з них слід зазначити такі: значні темпи інформатизації суспільства, технічне відставання правоохоронної системи та необхідність її реформування, недостатній рівень фінансування заходів з кіберзахисту.

Слід констатувати, що у 2018 р. увагу працівників кіберполіції було зосереджено на розслідуванні злочинів, вчинених у сфері високих інформаційних технологій. Так, протягом року працівники Департаменту кіберполіції були залучені до розслідування понад 11 тис. кримінальних проваджень. Їх структура наведена на рис. 2.

При цьому, необхідно вказати на той факт, що за територіями найбільша кількість злочинів у 2017 р. була зосереджена у місті Києві, Київській, Чернівецькій, Львівській областях. За результатами 2018 р. найвища кримінальна активність спостеріга-

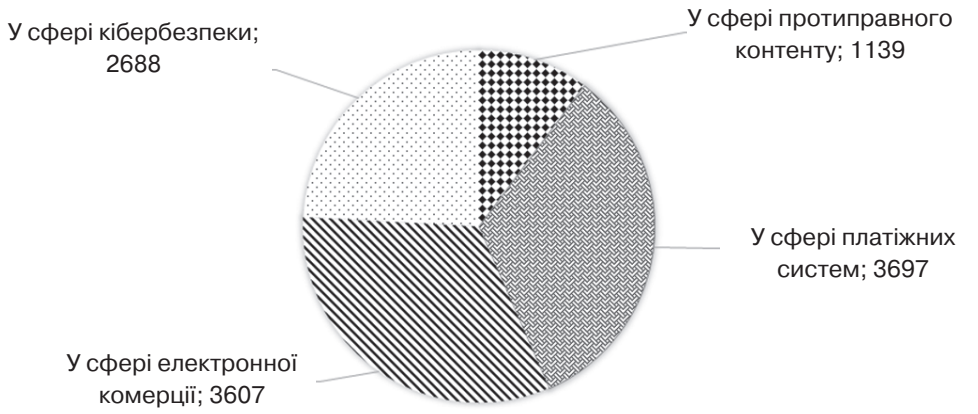


*Рис. 2.* **Структура кримінальних проваджень, які знаходяться на розслідуванні кіберполіції (2018 р.),** од.

*Джерело*: складено за даними [5].

лась у м. Києві, а також на території Черкаської, Одеської, Миколаївської та Львівської областей.

Аналіз структури кіберзлочинів в динаміці дозволив констатувати протягом 2013–2017 рр. найбільшу частку злочинів, які скоєно за ст. 361 Кримінального Кодексу України: несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (від 50 до 77 %) (табл. 1). Крім того, саме за рахунок цих злочинів спостерігається загальний приріст кіберзлочинів в динаміці.

Більш докладний аналіз структури злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж, який здійснено на основі статистичної звітності за 2017 р., констатує, що, у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку найбільшу частку складають ті, відповідальність за які передбачено ст. 361 Кримінального кодексу України — несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (69,8 %). На останньому місці — злочини, передбачені 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 (0,1 %).

Упродовж 2018 р. було виявлено 6 тис. злочинів, вчинених у сфері використання високих інформаційних технологій. При цьому найбільше з них — у сфері електронної комерції (див. рис. 3).

Аналіз відомостей про осіб, які вчинили злочини у сфері використання електронно-обчислювальних машин (комп'ютерів) (за закінченими розслідуваннями у кримінальних провадженнях), на основі даних 2017 р., дав можливість сформувати "портрет" кіберзлочинця. Основна

*Таблиця 1*

**Структура кіберзлочинності за кримінально-правовою ознакою за 2013–2017 рр.** [4]

| Обліковано кримінальних правопорушень у звітному періоді | Рік | | | | |
|---|---|---|---|---|---|
| | 2013 | 2014 | 2015 | 2016 | 2017 |
| Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361 КК України) | 408 | 344 | 432 | 494 | 1795 |
| Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст. 361-1 КК України) | 12 | 10 | 21 | 15 | 35 |
| 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) | 20 | 11 | 59 | 28 | 64 |
| Несанкціоновані дії з інформацією, яка обробляється 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) | 152 | 73 | 75 | 311 | 670 |
| 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 обробляється (ст. 363 КК України) | 2 | 4 | 9 | 15 | 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) | 1 | 1 | 2 | 2 | 3 |
| Разом | 595 | 443 | 598 | 865 | 2573 |

частка — це особи у віці від 18 до 39 років, які мають повну вищу і базову вищу освіту, що підтверджує їх високий кваліфікаційний рівень.

За даними 2018 р. було викрито понад 800 осіб, причетних до вчинення злочинів у сфері високих інформаційних технологій. Згідно зі статистикою, більша частина підозрюваних — чоловіки у віці від 25 до 40 років (табл. 2).

Дослідження викритих кіберзлочинів за статтями констатує, що основна їх частка скоєна за ст. 190

Кримінального кодексу України (табл. 3).

Аналіз структури кіберзлочинів за видами свідчить, що водночас, у сфері кібербезпеки найбільше виявлено користувачів шкідливого програмного забезпечення, які вчиняли злочини, використовуючи придбані віруси у DarkNet (рис. 4).

Зазначимо, що з метою виявлення кіберзлочинів, українська кіберполіція розробляє і впроваджує у практичну діяльність сучасні методики виявлення, фіксації і дослідження цифрових доказів. Зокрема, упродовж 2018 р. спеціалістами з кіберполіції оглянуто та проаналізовано 5,5 петабайтів інформації, яка у по-

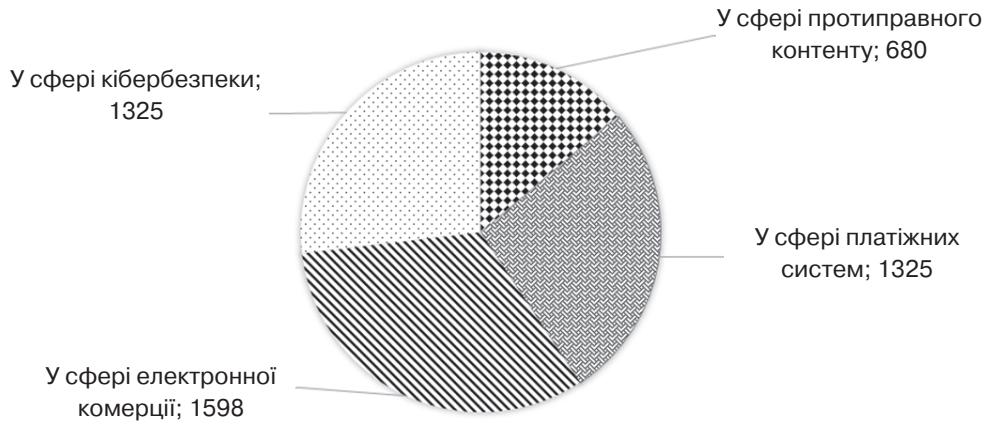


*Рис. 3.* **Структура виявлених злочинів у сфері високих інформаційних технологій (2018 р.),** од.

*Джерело*: складено за даними [5].

*Таблиця 2*

**Розподіл кіберзлочинців за статтю**, % (за даними 2018 р.) [5]

| Вік | Чоловіки | Жінки |
|---|---|---|
| Разом, з них: | 67 | 33 |
| До 25 років | 13 | 6 |
| 25–40 років | 39 | 20 |
| 40 і більше | 15 | 7 |

*Таблиця 3*

**Розподіл кіберзлочинців за статтю та статтями** [5]

| Стать | Стаття Кримінального кодексу України | | | |
|---|---|---|---|---|
| | 176 | 190 | 361 | 361-1 |
| Разом, осіб, з них: | 37 | 1019 | 505 | 55 |
| чоловіки, % | 97 | 67 | 92 | 95 |
| жінки, % | 3 | 33 | 8 | 5 |

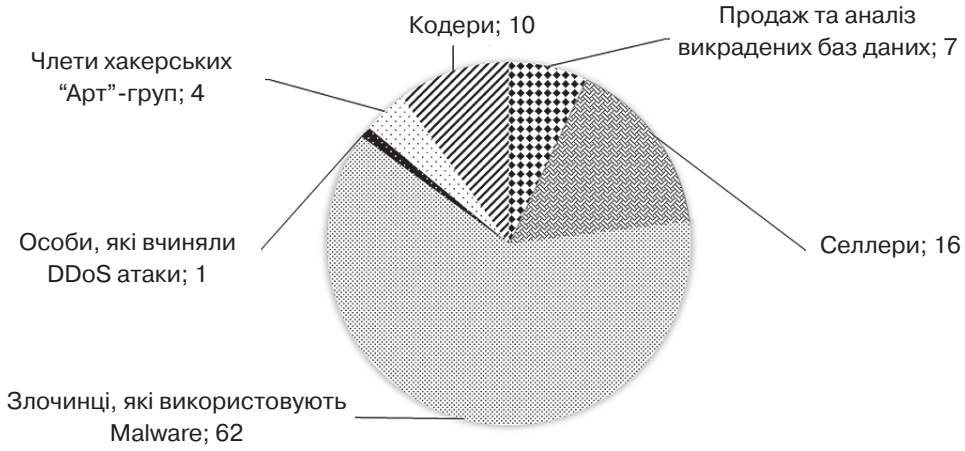


*Рис. 4.* **Структура виявлених кіберзлочинів за видами** (за даними 2018 р.), %
*Джерело*: складено за даними [5].

дальшому була визначена як цифрові докази. За результатами міжнародної співпраці у 2018 р. було викрито 8 транснаціональних хакерських угруповань та взято участь у понад 30 міжнародних операціях. У 2018 р. було підписано договори про взаємодію у сфері боротьби з кіберзлочинністю з організаціями як державного, так і приватного секторів. Серед них — представники міжнародних кампаній у сфері інформаційної безпеки та IT-компанії, поліція Австралії, Сінгапуру, Катару та інших країн. Налагоджено ефективну взаємодію з найвідомішими світовими соціальними мережами.

**Висновки та перспективи подальших досліджень.** Зростання інформатизації у світі відкриває як нові шляхи для подальшого світового розвитку, так і сприяє виникненню нових загроз, таких, як кібератаки. При цьому роль держави та відповідного державного регулювання у вирішенні зазначеної проблеми також зростає, враховуючи те, що саме держава визначає політику національної безпеки, сталого розвитку, цифровізації економіки і т. д. Проведений аналіз показав, що кількість кіберзлочинів в Україні зростає випереджальними темпами, тоді як правоохоронна система виявилася технічно не готовою до їх запобігання. Отже, проблема залучення та оптимізації технічних, фінансових та організаційно-управлінських ресурсів, необхідних для ефективного подолання кіберзлочинності в Україні на сьогодні стає одним з головних завдань державної політики забезпечення кібернетичної безпеки та є невід'ємною складовою політики національної безпеки. У подальших дослідженнях доцільно обґрунтувати відповідні механізми державної політики забезпечення кібернетичної безпеки в Україні.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Growing pains 2018 Global CEO Outlook, KPMG International. URL: kpmg.com/CEOoutlook

2. Norton Cyber Security Insights Report 2017 Global Results 2017. URL: https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf
3. Використання інформаційно-комунікаційних технологій на підприємствах України: статистичний бюлетень / відп. за вип. О. О. Кармазіна. — Київ : Держ. служба статистики України, 2015–2018. URL: http://www.ukrstat.gov.ua/
4. *Кравцова М. О.* Сучасний стан і напрями протидії кіберзлочинності в Україні // Вісн. кримінологічної асоціації України. — 2018. — № 2 (19). — С. 155–166. URL: http://dspace.univd.edu.ua/xmlui/bitstream/handle/ 123456789/3848/Suchasnyi%20stan%20i%20napriamy%20protydii%20kiberzlochynnosti%20v%20Ukraini%20_Kravtsova_2018.pdf?sequence=1&isAllowed=y
5. Офіційний сайт кіберполіції України. URL: https://cyberpolice.gov.ua/results/2018/

## REFERENCES

1. Growing pains: 2018 Global CEO Outlook. (2019). kpmg.com. Retrieved from https://home.kpmg/qm/en/home/insights/2018/05/growing-pains-2018-global-ceo-outlook.html [in English].
2. Norton Cyber Security Insights Report. Global Results 2017. (2018). www.symantec.com. Retrieved from https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf [in English].
3. *Karmazina O. O.* (Eds.). (2016). Vykorystannia informatsiino-komunikatsiinykh tekhnolohii na pidpryiemstvakh Ukrainy [Use of information and communication technologies in Ukraine]. Kyiv : Derzhavna sluzhba statystyky Ukrainy. Retrieved from https://ukrstat.org/uk/druk/publicat/kat_u/2016/bl/07/bl_vikt_15pdf.zip [in Ukrainian].
4. *Kravtsova M. O.* (2018). Suchasnyi stan i napriamy protydii kiberzlochynnosti v Ukraini [The current state and strain the counteraction to cybercrime in Ukraine]. Visnyk kryminolohichnoi asotsiatsii Ukrainy – Bulletin of the Criminological Association of Ukraine, 2(19), 155-166. Retrieved from http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/3848/Suchasnyi%20stan%20i%20napriamy%20protydii%20kiberzlochynnosti%20v%20Ukraini%20_Kravtsova_2018.pdf?sequence=1&isAllowed=y [in Ukrainian].
5. Pidsumky 2018 roku v tsyfrakh [Summary of the Year 2018 In Figures]. cyberpolice.gov.ua. Retrieved from https://cyberpolice.gov.ua/results/2018/ [in Ukrainian].