УДК 343.1+004.5
DOI https://doi.org/10.32782/pdu.2024.1.17

Т. І. Панасюк
кандидат юридичних наук,
старший науковий співробітник
Національної академії Служби безпеки України

УЧАСНИКИ КРИМІНАЛЬНОГО ПРОВАДЖЕННЯ ЯК СУБ'ЄКТИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У статті розглянуто останні законодавчі зміни до Кримінального процесуального кодексу України. Впровадження положень щодо надання учасникам кримінального провадження права брати участь у судовому засіданні в режимі відеоконференції поза межами приміщення суду з використанням власних технічних засобів та кваліфікованого електронного підпису згідно з вимогами Положення про Єдину судову інформаційно-комунікаційну систему та/або положень, що визначають порядок функціонування окремих підсистем (модулів) Єдиної судової інформаційно-комунікаційної системи відповідає сучасним тенденціям у сприянні доступу до правосуддя, а також використання в умовах правового режиму воєнного стану технічних засобів у кримінальному процесі.

Надання такого права відповідно поклало на учасників кримінального провадження і відповідальність за ризики технічної неможливості участі у відеоконфернції та переривання зв'язку.

Водночас законодавцем наголошено, що застосовувані технічні засоби мають забезпечувати інформаційну безпеку, тому обов'язок забезпечення інформаційної безпеки під час такої відеоконференції покладено не тільки на державу в особі суду, а також і на учасника кримінального провадження, який використовує своє право.

У досліджені акцентовано увагу на можливості використання зловмисниками такого учасника кримінального провадження як слабкої ланки з метою вчинення впливу на нього особисто (шляхом дезінформації, отримання його персональних даних або пошкодження належних йому технічних пристроїв з метою перешкоджання його участі у судовому засіданні) або взагалі на судовий розгляд справи.

Виходячи з цього, учасник кримінального провадження має бути свідомим мінімальних базових вимог та правил з кібергігієни, знати про основні способи та методи впливу зловмисників як на технічні пристрої, так і на їх користувача.

У дослідженні проаналізовано основні способи впливу та узагальнено рекомендації, які мають бути впровадженні у життя кожної людини, а особливо часника кримінального провадження з метою недопущення будь-якого впливу та забезпечення інформаційної безпеки.

Ключові слова: *учасник кримінального провадження, відеоконференція, технічні засоби, кібербезпека, кібергігієна, інформаційна безпека.*

Постановка проблеми. Повномасштабне вторгнення в Україну, окупація значних територій держави спричинило зміну у житті людини і громадянина, діяльності органів державної влади та кримінальної юстиції. Це стало каталізатором тих процесів, думки про необхідність впровадження яких беруть початок з COVID-пандемії.

Цифровізація та діджиталізація наразі є актуальним напрямом державної політики. Ведуться дискусії щодо запровадження у кримінальній юстиції ШІ. Крім того, начальник Департаменту протидії злочинам, вчиненим в умовах збройного конфлікту Офісу Генерального прокурора Юрій Білоусов зазначив, що окремі елементи ШІ використовуються у роботі щодо опрацювання великих масивів інформації під час розслідування воєнних злочинів [1].

В умовах правового режиму воєнного стану до кримінального процесуаль-

ного кодексу України внесено численні зміни, які зокрема стосуються спрощення порядку використання технічних засобів (у тому числі можливості використання власних технічнх засобів із застосуванням мережі інтернет).

Аналіз останніх досліджень і публікацій. Проведене дослідження має комплексний характер, та обумовлено останніми змінами до кримінального процесуального законодавства, аналогічні дослідження наразі не проводилися. Водночас окремі питання були предметом досліджень науковців. Питання кібербезпеки виступали предметом досліджень О. Бакалінської, О. Бакалінського [2; 3], Д. Дубова [4], Д. Кисиленка, В. Столбового, [5]. Питання процесуального статусу учасників кримінального провадження виступали предметом наукових досліджень таких вчених, О. Кучинської, С. Стахівського, В. Шибіки та інших. Крім цього, наразі досліджувані питання виступають предметом обговорення на панельних дискусіях, семінарах, круглих столах.

Мета статті є дослідження питання та формулювання висновків щодо застосування методів та правил кібербезпеки учасниками кримінального провадження, з метою забезпечення реалізації наданого їм права брати участь у судовому засіданні в режимі відеоконференції поза межами приміщення суду з використанням власних технічних засобів та технологій та кваліфікованого електронного підпису згідно з вимогами Положення про Єдину судову інформаційно-комунікаційну систему.

Виклад основного матеріалу. Правовий режим воєнного стану покладає обмеження прав і особливості участі учасників кримінального провадження у досудовому розслідуванні та під час судового розгляду кримінального провадження. Такі особливості можуть обумовлюватися неможливістю доступу особи до приміщення суду (перебування в іншому місті через евакуацію, або навіть перебування в іншій країні, а також питому вагу неможливості участі у судовому засіданні складає небажання особи. Однією з причин такого небажання є страх, страх зустрітися з кривдником, страх стигматизації, страх помсти за надані показання собі або членам сім'ї, які проживають на окупованих територіях.

Відповідно до принципу компліментарності кримінальні провадження щодо воєнних злочинів можуть розслідуватися як на національному рівні, так і міжнародному. Україна докладає значних зусиль з метою дотримання прав людини та громадянина та відновлення порушених прав. 80% кримінальних проваджень розслідуються на національному рівні. За інформацією Офісу генерального прокурора у період повномасштабного вторгнення рф станом на 06.04.2024 року зареєстровано 16949 злочинів проти основ національної безпеки та 123353 злочинів агресії та воєнних злочинів [6].

Відповідно до статті 216 Кримінального процесуального кодексу (далі –КПК) України досудове розслідування таких кримінальних правопорушень здійснюють слідчі органів безпеки України. Належить відмітити, що відповідно до положень КПК України у передбачених випадках розслідування таких злочинів здійснюють також слідчі Національної поліції, Державного бюро розслідувань, Національного антикорупційного бюро. Процесуальне керівництво під час розслідування здійснює Офіс Генерального прокурора.

Звільнення окупованих територій викрило велику кількість злочинів відносно цивільних осіб, злочинів у формі сексуального насильства, пов'язаного з конфліктом (далі – СНПК).

Слід зауважти, що науковці, правозахисники, слідчі, прокурори, адвокати та законодавці розглядають різні підходи з метою надання можливості учасникам кримінального провадження (особливо в особі потерпілих та свідків воєнних злочинів) реалізувати свої процесуальні права та взяти участь у судовому засіданні без страху.

Одним зі шляхів вирішення цього питання є норми проєкту закону № 9351 від 05.06.2023 року [7]. Цей проєкт закону пропонує внести зміни до статей 27, 232 і 278 КПК, які можна об'єднати у такі групи:

- закриті слухання за замовчуванням у справах СНПК (стаття 27 КПК України);
- можливість проведення допиту дистанційно у режимі відеоконферен-

ції (частина 6 статті 232 КПК України) з використанням власних технічних засобів (стаття 336 КПК України);

• зміна змісту повідомлення про підозру (стаття 278 КПК України), що підлягає опублікуванню у засобах масової та на офіційному веб-сайті Офісу Генерального прокурора відповідно до частини 8 статті 135 КПК України.

Виходячи з предмета нашого дослідження заслуговує уваги питання надання права застосувати власні технічні засоби особам у кримінальному провадженні.

Метою іншого проєкту закону № 8219 від 23.11.2022 «Про внесення змін до Кримінального процесуального кодексу України щодо забезпечення поетапного впровадження Єдиної судової інформаційно-телекомунікаційної системи» [8] як зазначено у пояснювальній записці до нього, є створення законодавчих умов задля поетапного впровадження ЄСІТС, першими етапом чого передбачено забезпечення обміну документами (надсилання та отримання документів) в електронній формі між судом та учасниками судового процесу, та забезпечення участі осіб у судових засіданнях дистанційно [9]. Законом України «Про внесення змін до Кримінального процесуального кодексу України щодо забезпечення поетапного впровадження Єдиної судової інформаційно-комунікаційної системи» від 23.02.2024 року № 3604-IX зазначений проєкт прийнято [10]. Таким чином КПК України надав право учасникам кримінального провадження брати участь у судовому засіданні в режимі відеоконференції поза межами приміщення суду з використанням власних технічних засобів та кваліфікованого електронного підпису згідно з вимогами Положення про ЄСІТС. При цьому ризики технічної неможливості участі у відеоконференції у таких випадках, переривання зв'язку тощо несе учасник кримінального провадження, який подав відповідне клопотання (частини п'ята та шоста статті 336 КПК України).

Згідно з нормами КПК України (частина 3 статті 336) застосовувані у дистанційному судовому провадженні технічні засоби і технології мають забезпечувати належну якість зображення і звуку, дотримання принципу гласності та відкритості судового провадження, а також інформаційну безпеку.

Забезпечення такої інформаційної безпеки безпосередньо покладається на учасника кримінального провадження.

Стратегією інформаційної безпеки визначено, що інформаційна безпека України – складова частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом [11].

В аспекті нашого дослідження з метою використання наданого права брати участь у судових засіданнях з використанням власних технічних засобів та технологій, та виконання покладеного обов'язку забезпечення інформаційної безпеки, кожен учасник кримінального провадження має бути свідомим питань кібербезпеки.

Чинне законодавство України не покладає обов'язку або відповідальності особи у сфері захисту своїх технічних засобів у мережі інтернет. Водночас відомо, що до механізму отримання, зберігання та обробки даних дотичні три елементи: люди, технології і процеси. Найслабшим елементом у цьому виступає саме людина, оскільки може неусвідомлено повідомити свої персональні дані чи відкрити сумнівне покликання, переслати таке покликання іншій особі або організації, проігнорувати подвійну аутентифікацію, а отже, створити загрозу для безпеки усім пов'язаним з нею суб'єктам. Кібератака у грудні 2023 року на одного із національних опе-

раторів мобільного зв'язку «Київстар», за фактом якого СБ України відкрито кримінальне провадження за статтями 361, 361-1, 110, 111, 113, 437, 438, 255 Кримінального кодексу України [12] сталася через скомпрометований обліковий запис одного з працівників [13].

Слід зазначити, що у національних нормативно-правових актах на сьогодні відсутнє безпосереднє згадування такої категорії як «кібергігієна».

Як зазначають фахівці ESET, кібергігієна – це заходи безпеки, розроблені для захисту пристроїв користувача від інфікування шкідливим програмним забезпеченням та можливого викрадення конфіденційної інформації [14].

Аналіз кращих світових практик та здійснених кібератак дозволяють сформулювати базові вимоги та рекомендації з питань кібербезпеки, кібергігієни та цифрової грамотності, яких повинні бути свідомі учасники кримінального провадження під час участі у судовому розгляді справ з використанням власних технічних засобів.

• Застосування спеціально визначених програм, додатків, веб-сайтів, так званого «білого списку», при цьому здійснюється блокування усіх інших, включаючи шкідливе програмне забезпечення.

• Використання двофакторної аутентифікації для забезпечення додаткового рівня захисту при вході до облікових записів. Крім імені користувача та пароля, або особистого ідентифікаційного номера (PIN) чи шаблону, для двофакторної аутентифікації іноді потрібен додатковий токен безпеки: фізичний об'єкт – кредитна картка, телефон; біометричне сканування – відбиток пальця, розпізнавання обличчя або голосу.

• Система шифрування – це процес перетворення інформації в секретний код, що забезпечить захист даних шляхом обмеження доступу до конфіденційної інформації користувачів, а також дозволить зменшити завдану шкоду від її втрати у разі успішної атаки.

• Моніторинг безпеки. Регулярний, безперервний і часто автоматизований процес моніторингу систем, мереж та програм на наявність загроз і вразливостей значно покращує кібергігієну, визначаючи як потенційно активні загрози, так і слабкі місця, до яких зловмисники можуть отримати доступ.

• Керування виправленнями. Програмне забезпечення для керування виправленнями – це інструмент, який дає змогу підтримувати свої комп'ютерні системи в актуальному стані, інсталюючи останні оновлення безпеки. Більшість рішень для керування виправленнями автоматично перевіряють наявність оновлень і повідомляють користувача про них [15].

• Використання ліцензійного програмного забезпечення та увімкнення автоматичного оновлення. Через короткострокову економію витрат споживачі часто обирають неліцензійне програмне забезпечення, що може призвести до ризику втрати конфіденційної інформації. Неможливість оновлення до останньої версії неліцензійного програмного забезпечення, створює додаткові ризики.

• Дотримання політики паролів. Велика кількість облікових записів на різних платформах або додатках, ускладнює їх запам'ятовування, тому управляти паролями стає все складніше. Водночас необхідно дотримуватися політики паролів: наявність великих і малих літер, цифр та спеціальних символів; обмеження мінімальної довжини коду допуску – щонайменше 12 символів, а краще від 16; обмеження щодо максимального терміну дії коду допуску; час очікування автоматичного замикання тощо. При цьому важливо уникати використання словникових слів, відомих фраз чи передбачуваних шаблонів, оскільки автоматизовані програми швидко вгадують поширені слова або фрази. Окремо слід звернути увагу на необхідності регулярної зміни паролів, інтервалом три-шість місяців та уникненні повторного використання своїх паролів. Для генерування та збереження у безпеці унікальних паролів до кожного облікового запису доцільним є використання менеджерів паролів.

• Використання безпечного Інтернету та віддаленого доступу. Наразі Інтернет – це не лише місце для роботи, спілкування та розваг, а й місце, де існує безліч загроз. Можуть бути використані

уразливості браузерів та встановлених плагінів, які виникають внаслідок нехтування оновленням. Хакери зламують легітимні сайти та розміщують на них шкідливий код та програми, а також захоплюють публічні точки доступу до мережі Інтернет для викрадення конфіденційних даних користувачів.

• Регулярне оновлення браузеру та встановлені плагіни; коректно налаштувати вимоги до приватності даних у браузері, щоб запобігти відстеженню та заблокувати сторонні файли cookie і спливаючі вікна; встановити додаткові плагіни безпеки, наприклад, HTTPS Everywhere,перевагою якого є попередження про незахищене з'єднання і ризик перехоплення даних: логінів, паролів тощо, або AdBlock для блокувальник реклами [16]. Деякі сайти використовують протоколи, які не мають шифрування HTTPS. У свою чергу, це є прямим шляхом до викрадення персональних даних. Протокол HTTPS є більш безпечний, ніж HTTP, шифрує всю інформацію та захищає від атак. Крім цього, під час під'єднання до публічної точки Wi-Fi може відбутися переадресація на іншу сторінку.

• Використання віртуальних приватних мереж (VPN) із шифруванням. Існує велика кількість комерційних та безкоштовних рішень. Одним із найпопулярніших є OpenVPN. Організація такого типу віддаленого доступу передбачає наявність серверу, до якого приєднуються клієнти за допомогою спеціально згенерованих сертифікатів, після чого їх трафік перенаправляється до внутрішніх інформаційних систем [17].

• Безпечне користування Wi-Fi. З метою забезпечення безпеки необхідно: вимкнути функцію автоматичного виявлення та підключення до доступних мереж; використовувати безпечний протокол з'єднання HTTPS та перевіряти його наявність у браузері; не робити жодних грошових операцій у публічних мережах; не вимикати програми, що захищають пристрій від мережевих атак; вимкнути загальний доступ до файлів і папок в операційній системі.

• Оновлення мобільного програмного забезпечення гарантуватиме захист від зловмисних програм. Подібно до атаки на ПК або корпоративний сервер, зловмисники використовують уразливості на мобільному програмному забезпеченні. Хакери розробляють шкідливі програми, які можна завантажити безкоштовно або навіть придбати. Після встановлення, ці програми можуть викрадати дані з пристроїв.

• Зазвичай смартфони підключають щонайменше до двох мереж, а іноді й більше. До них належать мобільний зв'язок, Wi-Fi, Bluetooth і GPS. Кожна з цих точок підключення може бути використана хакерами з метою заволодіння пристроєм або проникнення до корпоративної мережі. Тому слід вимикати програми, які не використовуються і переконатися, чи налаштовані на ґаджеті параметри безпеки та конфіденційності. Отримавши доступ до мобільного пристрою, можна швидко авторизуватись в месенджерах, поштових сервісах, системі онлайн-банкінгу. Ці дії можуть спричинити негативні наслідки у формі не лише втрати конфіденційних даних, а й фінансів. У разі захоплення мобільного пристрою слід заблокувати банківські та службові електронні кабінет; повідомити відповідальну особу про компрометацію облікових записів; завершити усі активні сеанси в облікових записах та змінити всі паролі [16].

• Обираючи безпечний месенджер слід звернути увагу на такі аспекти, які можуть гарантувати безпечний обмін повідомленнями: наскрізне шифрування, яке передбачає, що повідомлення в процесі надсилання будуть зашифровані; наявність політики конфіденційності; регулярні оновлення протоколів для оперативного усунення вразливостей.

• З метою з'ясування персональних даних особи, інформації про неї з подальшою компрометацією, дезінформацією або навіть залякуванням, або з метою здійснення кібератаки на державний орган чи організацію, в якій людина працює, хакери можуть збирати дані з акаунтів соціальних мереж.

• Тому важливо контролювати, хто саме має доступ до облікових записів та не розміщувати конфіденційну інформацію; не переходити за підозрілими посиланнями;

ділитися лише перевіреною інформацією; налаштувати параметри конфіденційності.

• Розповсюдженим способом отримання конфіденційної інформації та віддаленого доступу, а також зараження системи або мережі організації є розсилка фішингрових листів. При надходженні неочікуваного листа на e-mail слід провести аналіз змісту для встановлення індикаторів, які можуть бути характерними для фішингових листів: заклик вчинити швидку дію або прийняти швидке рішення, підмінені літери або символи в домені відправника з метою маскування під авторитетне джерело; наявність граматичних або орфографічних помилок; файл у додатку та пароль для відкриття його [16]. Фахівці CERT-UA рекомендують не переходити за невідомими посиланнями та не завантажувати файли, що мають потенційно небезпечне розширення (наприклад: .exe, .bin, .ini, .dll, .com, .sys, .bat, .js тощо) та навіть безпечне (наприклад: .docx, .zip, .pdf), адже можуть використовуватися вразливості, макроси та інші небезпеки [18].

• З метою захисту електронної скриньки необхідно використовувати такі правила: чітко розмежовувати особисту та службову пошти; використовувати багатофакторну аутентифікацію та системи аутентифікації, які перевіряють справжність відправників; впровадити спам-фільтри для фільтрації такої небажаної пошти.

• Забезпечення фізичної безпеки своїх пристроїв. Фізичний доступ до комп'ютера, ноутбука, планшета з метою встановлення шкідливого програмного забезпечення. Належить довіряти лише власним пристроям та бути обережними з пристроями, які отримуються від інших людей по роботі або в інших цілях; при підключенні пристроїв забезпечувати їх автоматичну перевірку на наявність шкідливого програмного забезпечення; відключати автоматичний запуск змінних носіїв інформації [18].

• Уміння розпізнавати дезінформацію та пропаганду як елементи інформаційної війни. Інфоманіпуляції часто є системними та масштабними, характеризуються багатоканальністю та повторюваністю наративів. Найбільш розповсюдженими методами пропаганди є спотворення та констатація фактів, гра з емоціями та почуттями людей, поширення чуток, нав'язування ярликів і стереотипів, звертання до авторитетних джерел [19]. Фейки у більшості випадків поширюються через веб-сайти новин, соціальні мережі, блоги, розсилки електронною поштою. Мета фейкової інформації полягає у введенні людей в оману. Навчитися протидіяти їм також можна [20]. Критичне осмислення будь-якої інформації, перевірка та уточнення відомостей через інші джерела, вміння більше керуватися розумом, аніж емоціями під час сприйняття інформації та обізнаність у сфері методів пропагандистського впливу, дають змогу виявити маніпулятивні прийоми та технології.

• Постійне навчання з кібербезпеки. Наразі підготовлено та розміщено на навчальних платформах навчальні курси з кібергігієни, які може пройти кожен бажаючий [16; 21]. Підвищення загальної обізнаності за допомогою практичного навчання дозволить зменшити кількість кіберінцидентів.

Висновки і пропозиції. Чинне законодавство йде шляхом його відповідності сучасним запитам та потребам, цифровізації та використання сучасних технічних засобів та технологій. Водночас кожне надане право обумовлює і покладання відповідного обов'язку.

Так, можливість використання власних технічних засобів у кримінальному провадженні поділяє обов'язок забезпечення інформаційної безпеки між державою та учасником провадження, який буде використовувати власні технічні засоби. Тільки спільна їх діяльність дозволить виконати покладений обов'язок. У цьому випадку дотримуючись наведених у статті рекомендацій з кібербезпеки та кібергігієни, особа (учасник кримінального провадження) не буде слабкою ланкою забезпечення інформаційної безпеки процесу.

Список використаної літератури:

1. Штучний інтелект і розслідування воєнних злочинів: досвід України. URL: https://justtalk.com.ua/post/shtuchnij-intelekt-i-rozsliduvannya-voennih-zlochiniv-dosvid-ukraini (дата звернення: 05.04.2024).

2. Бакалінська О. Бакалінський О. Правове забезпечення кібербезпеки в Україні URL: Адміністративне право і процес. К., 2019. №9. С. 100-108. URL: http://pgp-journal.kiev.ua/archive/2019/9/18.pdf (дата звернення: 22.03.2024).
3. Бакалінська О. Сучасні тенденції правового регулювання кібербезпеки та інтелектуальна власність // Теорія і практика інтелектуальної власності. 2022. № 5. С.82-92.
4. Дубов Д. Формуючи нову стратегію кібербезпеки України: чи можемо уникнути помилок першої спроби стратегування. URL: https://niss.gov.ua/sites/default/files/2021-01/tezy-dubov-2.pdf (дата звернення: 31.03.2024).
5. Заходи з підвищення кібербзпеки на державному та корпоративному рівнях в умовах діджеталізації суспільства / В. Столбовий, Д. Кисиленко // Наукові записки Львівського університету бізнесу та права. Серія економічна. Серія юридична. Випуск 37/2023. URL: https://nzlubp.org.ua/index.php/journal/article/download/802/729 (дата звернення: 01.04.2024).
6. Злочини, вчинені в період повномасштабного вторгнення рф. URL: https://www.gp.gov.ua/ (дата звернення 06.04.2024).
7. Проект Закону про внесення змін до Кримінального процесуального кодексу України щодо удосконалення порядку здійснення досудового розслідування та судового розгляду у кримінальних провадженнях щодо злочинів, які пов'язані із сексуальним насильством, яке вчинене в умовах збройного конфлікту. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/41960 (дата звернення: 06.04.2024).
8. Проект закону «Про внесення змін до Кримінального процесуального кодексу України щодо забезпечення поетапного впровадження Єдиної судової інформаційнотелекомунікаційної системи». URL: https://itd.rada.gov.ua/billInfo/Bills/Card/40876 (дата звернення: 06.04.2024).
9. Пояснювальна записка до проекту Закону «Про внесення змін до Кримінального процесуального кодексу України щодо забезпечення поетапного впровадження Єдиної судової інформаційно-телекомунікаційної системи». URL: blob:https://itd.rada.gov.ua/1e22dbd0-bad5-4f5c-8fe6-fb1a0acbeaeb (дата звернення: 06.04.2024).
10. Про внесення змін до Кримінального процесуального кодексу України щодо забезпечення поетапного впровадження Єдиної судової інформаційно-комунікаційної системи : Закон України від 23.02.2024 року № 3604-IX. URL: https://zakon.rada.gov.ua/laws/show/3604-IX#Text (дата звернення: 06.04.2024).
11. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» : Указ президента України від 28 грудня 2021 року № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text (дата звернення 06.04.2024).
12. СБУ відкрила кримінальне провадження за фактом кібератаки на «Київстар» URL: https://ssu.gov.ua/novyny/sbu-vidkryla-kryminalne-provadzhennia-za-faktom-kiberataky-na-kyivstar (дата звернення 03.03.2024).
13. Хакери зламали захист Київстар через обліковий запис працівника – Президент компанії URL: https://www.ukrinform.ua/rubric-technology/3799815-hakeri-zlamali-zahist-kiivstar-cerez-oblikovij-zapis-pracivnika-prezident-kompanii.html (дата звернення 03.03.2024).
14. ESET. Основні правила захисту даних – кібергігієна для активного Інтернет-користувача. URL: https://www.eset.com/ua/about/newsroom/blog/data-protection/osnovnyye-pravila-zashchity-dannykh-kibergigiyena-dlya-aktivnogo-internet-polzovatelya/ (дата звернення: 29.03.2024).
15. Microsoft. Що таке керування вразливостями. URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-vulnerability-management (дата звернення: 29.03.2024).
16. Основи кібергігієни. Цифрова освіта. URL: https://osvita.diia.gov.ua/courses/cyber-hygiene (дата звернення: 29.03.2024).
17. Рекомендації щодо віддаленої роботи. CERT-UA. URL: https://cert.gov.ua/recommendation/11388 (дата звернення 25.03.2024).
18. Основні правила кібергігієни. CERT-UA. URL: https://cert.gov.ua/recommendation/31 (дата звернення: 29.03.2024).
19. Основні методи пропаганди в російському інтернет-змі pravda.ru / Б. Іванницька, С. Гусєва. URL: https://science.lpnu.ua/sites/default/files/journal-paper/2019/apr/16167/ivanytska3.pdf.

20. Як захиститися від фейків і дезінформації. Базові навички з фактчекігну та протидії дезінформації. URL: https://osvita.diia.gov.ua/courses/how-to-protect-yourself-from-fakes-and-disinformation (дата звернення: 05.04.2024).
21. Персональна кібергігієна. URL: https://osvita.diia.gov.ua/courses/personal-cyberhygiene (дата звернення: 05.04.2024); Кіберняні. URL: https://osvita.diia.gov.ua/courses/cybernanny (дата звернення: 05.04.2024).

Panasiuk T. Participants in the criminal proceedings as subjects ensuring information security

This article examines the recent legislative changes to the Criminal Procedure Code of Ukraine. The implementation of provisions granting participants in criminal proceedings the right to participate in court hearings via video conferencing outside the courtroom, using their own technical means and a qualified electronic signature, aligns with modern trends in facilitating access to justice and accounts for the use of technical tools during a state of war.

The conferment of this right places responsibility on participants in criminal proceedings, and they bear the risks associated with technical difficulties in participating in video conferences and potential disruptions in communication.

Legislators emphasize that the technical tools employed must ensure information security. Therefore, the duty to ensure information security during such video conferences lies not only with the state (represented by the court) but also with the participants in criminal proceedings exercising this right.

The study highlights the possibility of malicious actors targeting vulnerable participants in criminal proceedings. This may involve disinformation, obtaining personal data, or damaging their technical devices to hinder their participation in court hearings or affect the overall judicial process.

In light of this, participants in criminal proceedings should be aware of basic cybersecurity requirements and rules. They should understand the fundamental methods and techniques used by malevolent actors to influence both technical devices and their users. In the research, the main methods of influence have been analyzed and recommendations have been summarized, which should be implemented in the life of every person, especially a participant in criminal proceedings, in order to prevent any influence and ensure information security.

Key words: *participant in criminal proceedings, video conferencing, technical means, cybersecurity, cyber hygiene, information security.*