УДК 343.9
DOI https://doi.org/10.32782/2524-0374/2022-9/121

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ СПЕЦІАЛЬНИХ ЗНАНЬ ПІД ЧАС РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ

FEATURES OF THE USE OF SPECIAL KNOWLEDGE IN THE INVESTIGATION OF CYBERCRIMES

Колосов О.О., аспірант кафедри кримінальної юстиції
Навчально-науковий інститут права Державного податкового університету,
юрисконсульт
Товариство з обмеженою відповідальністю «Глобал Білгі»

Ковальчук О.А., студентка ІІ магістратури юридичного факультету
Навчально-науковий інститут права Державного податкового університету

У статті досліджуються особливості застосування спеціальних знань під час розслідування кіберзлочинів. З метою обгрунтування обраної теми дослідження наведено інформацію зі звітності Офісу Генерального прокурора України, а саме Єдиного звіту про осіб, які вчинили кримінальні правопорушення за 2020 та 2021 роки щодо різниці між кількістю осіб яким було повідомлено про підозру у вчиненні кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів) та кількістю осіб, відносно яких вироки та ухвали набрали законної сили.

Наведено інформацію Державної служби спеціального зв`язку та захисту інформації України щодо кібератак здійснених проти державних органів України.

Визначено роль спеціаліста та експерта у розслідуванні кіберзлочинів. Наведено перелік слідчих (розшукових) дій під час яких необхідне використання спеціальних знань при розслідуванні кіберзлочинів. Додаткова увага приділена комп`ютерно-технічній експертизі, її предмету, завданням та видам носіїв інформації, які може використовувати експерт під час проведення такої експертизи. Також визначено проблеми, ящо виникають під час проведення комп`ютерно-технічної експертизи.

Зокрема, наголошено на важливості володіння учасниками судочинства спеціальними знанням у сфері комп`ютерних технологій з метою уникнення труднощів під час формулювання коректних питань перед експертом, який буде проводити експертизу.

Визначено необхідність та важливість створення та оновлення наявних спеціальних рекомендацій та методичок для учасників судочинства щодо визначення правильних та точних питань до ексертів у питаннях проведення комп'ютерно-технічних експертиз. Також визначено необхідність у проведенні регулярних навчань (тренінгів) для працівників правоохоронних органів та судочинства щодо питань набуття спеціальних навичок у сфері комп`ютерних та інформаційних технологій, що, на думку авторів, сприятиме у майбутньому уникнення можливих труднощів та помилок під час визначення питань до експерта, які ставляться з метою проведення комп'ютерно-технічних експертиз.

Також нагаолошено на важливості міжнародного співробітництва України у сфері боротьби з кіберзлочинами. Зокрема, щодо обміну досвідом та інформацією про кіберінциденти, проведення спільних навчань, тренінгів, консультацій, заходів тощо з метою підсилення підсилити кіберспроможності України та її зарубіжних партнерів.

Ключові слова: кіберзлочин, розслідування, інформаційні технології, електронно-обчислювальних машини (комп`ютери), спеціаліст, експерт, комп`ютерно-технічна експертиза, спеціальні знання, судочинство, міжнародне співробітництво.

The article examines the features of the application of special knowledge in the investigation of cybercrimes. In order to substantiate the chosen research topic, information is provided on the reporting of the Office of the Prosecutor General of Ukraine, namely the Unified Report on Persons Who Committed Criminal Offenses for 2020 and 2021 on the difference between the number of persons who were informed of suspicion of committing criminal offenses in the field of using electronic computing machines (computers) and the number of persons in respect of which sentences and decisions have entered into force.

The information of the State Service of Special Communications and Information Protection of Ukraine regarding cyber attacks carried out against the state bodies of Ukraine is provided.

The role of a specialist and an expert in the investigation of cybercrimes is defined. A list of investigative (detective) actions is given during which the use of special knowledge in the investigation of cybercrimes is necessary. Additional attention is paid to computer-technical expertise, its subject, tasks and types of information carriers that an expert can use when conducting such an expertise. The problems that arise when conducting computer-technical expertise are also identified.

In particular, the importance of the possession of special knowledge in the field of computer technology by the participants in the proceedings in order to avoid difficulties in formulating the correct questions to the expert who will conduct the expertise was noted.

The necessity and importance of creating and updating of existing special recommendations and methods for participants in proceedings to determine the correct and accurate questions to experts in matters of conducting computer-technical expertises are determined. The need to conduct regular exercises (trainings) for law enforcement officials and judiciary on the acquisition of special skills in the field of computer and information technology is defined which according to the authors will help avoid possible difficulties and errors in determining questions to the expert put in order to conduct computer-technical expertises.

The importance of international cooperation of Ukraine in the field of combating cybercrime is also outlined. In particular, on the exchange of experience and information on cyber incidents, holding joint exercises, trainings, consultations, events, etc. in order to strengthen the cyber capability of Ukraine and its foreign partners.

Key words: cybercrime, investigation, information technology, electronic computing machines (computers), specialist, expert, computer-technical expertise, special knowledge, proceedings, international cooperation.

На сьогоднішній день з урахуванням розвитку інформаційних технологій в Україні та у світі захист кіберпростору є одним з ключових завдань забезпечення національної та соціально-економічної безпеки. Таким чином, враховуючи теперішні безпекові виклики вкрай актуальним є проблема підвищення ефективності розслідування кіберзлочинів.

Проблематкою дослідження забезпечення інформаційної безпеки займалися такі українські вчені як Арістова І. В., Березовська І. Р., Дзьобаня О. П., Калюжний Р. А., Кормич Б. А., Ліпкан В. А., Марущак А. І., Цимбалюк В. С., Юдін О. К. та інші. Проблематиці протидії кіберзлочинності присвячено роботи таких вітчизнаних вчених як Азарова Д.С., Біленчука П. Д., Бутузова В. М., Вєхова В. Б., Гавловського В. Д., Голубєва В. О., Іванченко О. Ю., Карчевського М. В., Музики А. А., Пашнєва Д. В., Цимбалюка В. С., Шеломенцева В. П. та ін..

Мета статті полягає у дослідженні особливостей застосування спеціальних знань під час розслідування кіберзлочинів.

Згідно звітності Офісу Генерального прокурора України (Єдиний звіт про осіб, які вчинили кримінальні правопорушення) за 2020 рік кількість осіб яким було повідомлено про підозру у вчиненні кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (р. XVI Кримінального кодексу України), зокрема серед яких були: несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361 ККУ); створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст. 361-1 ККУ); 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 ККУ); 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 ККУ); інші, складала 1243 осіб. Кількість осіб, відносно яких вироки та ухвали набрали законної сили щодо таких кримнальних правопорушень у 2020 році становила 0 осіб [1].

За 2021 рік кількість осіб, яким було повідомлено про підозру у вчиненні таких кримінальних правопорушень складала 1732 особи. Кількість осіб, відносно яких вироки та ухвали набрали законної сили щодо таких кримнальних правопорушень у 2021 році становила 0 осіб [1].

Тож виходячи із наявної статистичної інформації, можна зробити висновок, що така різниця між кількістю осіб яким було повідомлено про підозру у вчиненні кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів) та кількістю осіб, відносно яких вироки та ухвали набрали законної сили свідчить про складність доказування, в тому числі як свідчить практика, в частині роботи із електронними доказами та їх носіями.

Також питання забезпечення кібербезпеки є як ніколи актуальним в умовах воєнного стану в Україні. Були повідомлення від Держспецзв'язку про отримання українськими користувачами нових небезпечних електронних листів з темою «№ 1275 від 07.04.2022». Листи містили HTML-файл, відкриття якого призводило до створення на комп'ютері архіву з файлом під назвою «Щодо фактів переслідування та вбивства працівників Прокуратури з боку російських військових на тимчасово окупованих територіях.lnk». Його відкриття, у свою чергу, призведило до можливості хакерів отримати повний контроль над комп'ютером користувача і загрожувало крадіжкою конфіденційної інформації, пошкодженням даних та комп'ютерних систем. Таку активність було асоційовано з діяльністю групи UAC-0010 (Armageddon), яка вже неодноразово здійснювала кібертаратаки як державні органи України, так і на країни ЄС [2].

Держспецзв'язку попереджувало про розповсюдження електронних листів, що містять HTML-файл «Військові злочинці РФ.htm», відкриття якого призведить до створення на комп'ютері RAR-архіву «Viyskovi_zlochinci_RU.rar». Згаданий архів містить файл-ярлик «Військові-злочинці що знищують Україну (домашні адреси, фото, номера телефонів, сторінки у соціальних сетях).lnk». Його відкриття призведить до того, що зловмисники отримують віддалений доступ до комп'ютера жертви. Активність асоційовано з діяльністю групи UAC-0010 (Armageddon) [3].

Під криміналістичною методикою розкриття і розслідування комп'ютерних злочинів розуміється сукупність наукових положень і рекомендацій, розроблених на їх основі, тобто, науково обґрунтованих і апробованих на практиці порад щодо розкриття і розслідування даних злочинів [4, 296].

Організація і проведення слідчих (розшукових) дій під час розслідування кримінальних правопорушень у сфері використання комп'ютерів, систем та комп'ютерних мереж має певні особливості, що вимагає від слідчого як особистого володіння спеціальними знаннями та навичками, так і використання допомоги осіб, що на високому рівні володіють такими знаннями [5, с. 113]. Таким чином, розслідування кіберзлочинів вимагає спеціальних знань у сфері комп`ютерів та інофрмаційних технологій, необхідність у застосуванні яких виникає в процесі провадження слідчих (розшукових) дій під час розслідування таких злочинів. Особою, яка володіє спеціальними знаннями та навичками у кримінальномиу провадженні є спеціаліст.

Відповідно до ст. 71 КПК України спеціаліст може надавати консультації, пояснення, довідки та висновки під час досудового розслідування і судового розгляду з питань, що потребують відповідних спеціальних знань і навичок, та може бути залучений для надання безпосередньої технічної допомоги [6]. Особливого значення використання спеціальних знань набуває під час проведення таких слідчих (розшукових) дій як слідчий огляд та обшук, оскільки вони пов'язані безпосередньо з виявленням, дослідженням та вилученням комп'ютерного обладнання і його програмного забезпечення [5, с. 113].

Відповідно до КПК України спеціаліст має право: 1) ставити запитання учасникам процесуальної дії з дозволу сторони кримінального провадження, яка його залучила, чи суду; 2) користуватися технічними засобами, приладами та спеціальним обладнанням; 3) звертати увагу сторони кримінального провадження, яка його залучила, або суду на характерні обставини чи особливості речей і документів; 3-1) викладати у висновку відомості, що мають значення для кримінального провадження і щодо яких йому не були поставлені запитання; 4) знайомитися з протоколами процесуальних дій, в яких він брав участь, і подавати до них зауваження; 5) одержувати винагороду за виконану роботу та відшкодування витрат, пов'язаних із його залученням до кримінального провадження; 6) заявляти клопотання про забезпечення безпеки у випадках, передбачених законом; 7) надавати висновки з питань, що належать до сфери його знань, під час досудового розслідування кримінальних проступків, у тому числі у випадках, передбачених частиною третьою статті 214 цього Кодексу; 8) надавати довідки з питань, що належать до сфери його знань, у випадках, передбачених частиною третьою статті 245-1 цього Кодексу [6].

Таким чином, залучення спеціалістів під час розслідування кіберзлочинів має важливе значення, оскільки завдяки допомозі спеціаліста можливо визначити індивідуальний кримінальний почерк кіберзлочинця, вид та характеристики розроблених ним програм, які були використані ним у злочинній діяльності тощо. Також, на нашу думку, важливим є залучення ІТ-фахівців для допомоги слідчим та спеціалістам у розслідуванні кіберзлочинів, оскільки сфера захисту від кіберзлочинності стрімко та динамічно розвивається, що зумовлює потребу у підвищенні ефективності боротьби з кіберзлочинами та пошуку нових форм співпраці між правоохоронними органами та суспільством.

Також у розслідуванні кіберзлочинів важливе місце відводиться експерту. Відповідно до ст. 69 КПК України експертом у кримінальному провадженні є особа, яка володіє науковими, технічними або іншими спеціальними знаннями, має право відповідно до Закону України «Про судову експертизу» на проведення експертизи і якій доручено провести дослідження об'єктів, явищ і процесів, що містять відомості про обставини вчинення кримінального

правопорушення, та дати висновок з питань, які виникають під час кримінального провадження і стосуються сфери її знань [6]. Відповідно до КПК України експерт має право: 1) знайомитися з матеріалами кримінального провадження, що стосуються предмета дослідження; 2) заявляти клопотання про надання додаткових матеріалів і зразків та вчинення інших дій, пов'язаних із проведенням експертизи; 3) бути присутнім під час вчинення процесуальних дій, що стосуються предметів та об'єктів дослідження; 4) викладати у висновку експертизи виявлені в ході її проведення відомості, які мають значення для кримінального провадження і з приводу яких йому не були поставлені запитання; 5) ставити запитання, що стосуються предмета та об'єктів дослідження, особам, які беруть участь у кримінальному провадженні; 6) одержати винагороду за виконану роботу та відшкодування витрат, пов'язаних із проведенням експертизи і викликом для надання пояснень чи показань, у разі, якщо проведення експертизи не є службовим обов'язком особи, яка залучена як експерт; 7) заявляти клопотання про забезпечення безпеки у випадках, передбачених законом; 8) користуватися іншими правами, передбаченими Законом України «Про судову експертизу» [6].

У відношенні розслідування кіберзлочинів важливе має значення має комп`ютерно-технічна експертиза. Комп`ютерно-технічна експертиза – експертиза, що належить до виду інженерно-технічних експертиз, та об'єктом дослідження якої є комп'ютерна техніка та (або) комп'ютерні носії інформації. Комп`ютерно-технічна експертиза проводиться з метою: визначення статусу об'єкта як комп'ютерного засобу, виявлення і вивчення його ролі в розслідуваному злочині, а також отримання доступу до інформації на електронних носіях з подальшим всебічним її дослідженням. Предметом комп'ютерно-технічної експертизи є факти (обставини), що мають значення для органів досудового розслідування або суду, та встановлюються на основі дослідження закономірностей розробки та експлуатації комп'ютерних засобів і систем, що забезпечують реалізацію інформаційних процесів [7].

Завданням комп'ютерно-технічної експертизи є і виявлення інформації, що міститься на комп'ютерних носіях, і визначення її цільового призначення (для цього експертові надають не лише комп'ютерну техніку, а й комп'ютерний носій інформації). Інколи можна обмежитися наданням лише комп'ютерного носія, попередньо проконсультувавшись з експертом. Для цього слідчий має пояснити експертові, яка саме інформація його цікавить. Такий підхід дозволить скоротити час, потрібний для проведення дослідження [8, с. 101].

До видів носіїв інформації належать: 1) накопичувачі на жорстких магнітних дисках – пристрої для зберігання інформації, робота яких здійснюється за принципом магнітного запису; 2) твердотілі накопичувачі (англ. SSD, solid-state drive) – комп'ютерні запам'ятовувальні пристрої на основі мікросхем пам'яті та контролера керування ними, що не містять рухомих механічних частин, які можуть бути виконані, як окремими так і вбудованими в інше обладнання; 3) USB флеш-накопичувачі – носії інформації, що використовують флешпам'ять для збереження даних та підключаються до комп'ютера чи іншого пристрою через USB-порт; 4) карти пам'яті – носії інформації, що також використовують флеш-пам'ять для збереження даних та підключаються до комп'ютера чи іншого пристрою за допомогою різних спеціалізованих адаптерів [7].

До завдань комп'ютерно-технічної експертизи належить також пошук і визначення вірусів та наявних програмних продуктів, у тому числі й шкідливих, призначених для несанкціонованого втручання в роботу комп'ютерів і комп'ютерних мереж. Це завдання доволі складне, адже є багато програмних продуктів, про існування яких нічого не відомо, призначення яких доволі складно визначити навіть після виконання їх програмного коду, а надто зі 100-відсотковою впевненістю стверджувати, що їх немає на комп'ютерному носії [8, с. 101].

При призначенні комп'ютерно-технічної експертизи особливу увагу слід приділяти збору об'єктів дослідження. Найменші некваліфіковані дії з комп'ютерною системою часто закінчується безповоротною втратою цінної розшукової та доказової інформації. У зв'язку з цим, для збору об'єктів дослідження доцільним є залучення фахівця [7].

На думку Кулик Я.О. при призначенні судової експертизи може виникнути проблема формулювання правильних, точних, недвозначних питань, які необхідно поставити на розгляд перед експертом. Як правило, особи, які беруть участь у справі і суд не володіють спеціальними знаннями в області науки, техніки, мистецтва, ремесла, відповідно визначити коло питань, відповідь на які дасть можливість встановити що мають значення для розгляду і вирішення справи обставини, видається проблематичним. Крім того, значущим обставиною є відсутність спеціальних знань в учасників судочинства і як наслідок, неможливість сформулювати коректні питання перед експертом. У складних випадках, коли для формулювання питань необхідні спеціальні знання, учасників судочинства відчувають певні труднощі, тактично грамотним рішенням є залучення до підготовки питань експерта, який буде проводити експертизу [9].

На нашу думку, формулювання вірного кола питань та наявність спеціальних знань в учасників судочинства є ключовим елементом у проведенні комп'ютерно-технічних експертиз. Беручи до уваги специфіку кіберзлочинності, на нашу думку, нагальним є питання створення та оновлення наявних спеціальних рекомендацій та методичок для учасників судочинства щодо визначення правильних та точних питань до експертів у питаннях проведення комп'ютерно-технічних експертиз. Також вважаємо за необхідне, проведення регулярних навчань (тренінгів) для працівників правоохоронних органів та судочинства щодо питань набуття спеціальних навичок у сфері комп`ютерних та інформаційних технологій, що сприятиме у майбутньому уникнення можливих труднощів та помилок під час визначення питань до експерта, які ставляться з метою проведення комп'ютерно-технічних експертиз.

Також важливу роль у сфері кіберзахисту відіграє міжнародне співробітництво України. Так, Уряди України та Польщі підписали меморандум про співпрацю у сфері кіберзахисту. Меморандум забезпечить посилення спільної боротьби зі злочинами у кіберпросторі та зробить обмін досвідом та інформацією про кіберінциденти швидшим і ефективнішим [10]. Під час зустрічі, у якій також взяли участь експерти з кібербезпеки та міжнародного співробітництва, обговорили роль кожного органу в системах оборони країн, їхню сферу діяльності та зони відповідальності, роботу українських та польських команд реагування на кіберінциденти, а також загальну екосистему кібербезпеки та платформ обміну інформацією. Це й обмін інформацією та досвідом, і проведення спільних навчань, тренінгів, консультацій, а також інші заходи, які дозволять підсилити кіберспроможність обох країн [11].

Отже, вважаємо, міжнародну співпрацю одним з важливих чинників підвищення рівня кваліфікації українських спеціалістів у сфері кіберзахисту та протидії кіберзлочинам. Враховуючи динамічний характер кіберзлочинності, спільний обмін досвідом та проведення тренінгів з міжнародними партнерами є об`єктивно обумовленою необхідністю.

Висновки. Отже, вважаємо, що на сьогоднішній день питання підвищення ефективності розслідування кіберзлочинів є нагальним, що зумовлено викликами сучасності. На нашу думку, важливим є системне залучення ІТ-фахівців для допомоги слідчим у розслідуванні кіберзлочинів. Також вважаємо за необхідне розробку нових та оновлення

наявних спеціальних методичних рекомендацій для застосування окремих форм спеціальних знань при розслідуванні кіберзлочинів, зокрема, для визначення правильних та точних питань до експертів для проведення комп'ютерно-технічних експертиз, так само як і проведення регулярних навчань (тренінгів) для працівників правоохоронних органів та судочинства щодо питань набуття спеціальних навичок у сфері комп`ютерних та інформаційних технологій. Також вагоме значення має співпраця з міжнародними партнерами. Одним з позитивних прикладів такої співпраці є підписання меморандуму про співпрацю у сфері кібербезпеки, який забезпечить посилення спільної боротьби зі злочинами у кіберпросторі, сприятиме пришвидшенню та підвищенню ефективності обміну досвідом та інформацією про кіберінциденти. Підписання даного меморандуму має на меті проведення спільних навчань, тренінгів, консультацій, а також інших заходів, які дозволять підсилити кіберспроможність обох країн.

ЛІТЕРАТУРА

1. Про осіб, які вчинили кримінальні правопорушення. Сайт Офісу Генерального прокурора України. URL: https://gp.gov.ua/ua/posts/pro-osib-yaki-vchinili-kriminalni-pravoporushennya-2 (19.08.2022)

2. Увага! Нова кібератака групи Armageddon на державні органи України. Сайт Державної служби спеціального зв`язку та захисту інформації України. URL: https://cip.gov.ua/ua/news/uvaga-nova-kiberataka-grupi-armageddon-na-derzhavni-organi-ukrayini (дата звернення: 20.08.2022)

3. Увага! Нова кібератака на державні органи України. Сайт Державної служби спеціального зв`язку та захисту інформації України. URL: https://cip.gov.ua/ua/news/uvaga-nova-kiberataka-na-derzhavni-organi-ukrayini (дата звернення: 25.08.2022)

4. Голубєв В.О. Розслідування комп'ютерних злочинів.Монографія. Запоріжжя. Гуманітарний університет «ЗІДМУ». 2003. 296 с.

5. Лук`янчиков Є.Д., Лук`янчиков Б.Є. Участь спеціаліста в розслідуванні комп`ютерних злочинів. Актуальні питання розслідування кіберзлочинів. Матеріали Міжнародної науково-практичної конференції. Харків. 2013. URL: http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/553/Aktualni%20pytannia%20rozsliduvannia%20kiberzlochyniv_Materialy%20konferentsii_2013.pdf?sequence=1&isAllowed=y (дата звернення: 25.08.2022)

6. Кримінальний процесуальний кодекс України. Кодекс. Закон України № 4651-VI 13 квітня 2012 р. База даних «*Законодавство України*». ВР України. URL: https://zakon.rada.gov.ua/laws/show/4651-17/conv#n958 (дата звернення: 28.08.2022)

7. Комп`ютерно-технічна експертиза. Сайт Київського науково-дослідного інституту судових експертиз. URL: https://kndise.gov.ua/kompyuterno-tehnichna/ (дата звернення: 29.08.2022)

8. Коліса Я.Ю. Взаємодія служб у боротьбі з кіберзлочинністю. Криміналістичний вісник № 1 (23). 2015. URL: http://elar.naiau.kiev.ua/bitstream/123456789/1868/1/%D0%9A%D0%BE%D0%BB%D1%96%D1%81%D0%B0%20%D0%AF.%20%D0%AE..pdf (дата звернення: 29.08.2022)

9. Кулик Я.О. Проблеми призначення судової експертизи у кримінальному провадженні. URL: https://www.ukrlogos.in.ua/10.11232-2663-4139.16.68.html (дата звернення: 30.08.2022)

10. Уряди України та Польщі підписали меморандум про співпрацю у сфері кіберзахисту. Урядовий портал. Єдиний веб-портал органів виконавчої влади України. URL: https://www.kmu.gov.ua/news/uriady-ukrainy-ta-polshchi-pidpysaly-memorandum-pro-spivpratsiu-u-sferi-kiberzakhystu (дата звернення: 10.09.2022)

11. Україна поглиблює співпрацю з Польщею у сфері кібербезпеки. Урядовий кур`єр. Газета Кабінету Міністрів України. URL: https://ukurier.gov.ua/uk/news/ukrayina-pogliblyuye-spivpracyu-z-polsheyu-u-sferi/ (дата звернення: 12.09.2022)