5. Голованов Я.К. Королев: факты и мифы. Москва : Наука, 1994.
6. Анотований реєстр описів. Том 2. Частина 1 : Фонди періоду після 1918 року. URL: http://dako.gov.ua/wp-content/uploads/2019/06/ANOTOVANYI_REESTR_TOM-2_CHASTYNA-1.pdf.
7. Первое ракетное соединение вооруженных сил страны. Военно-исторический очерк / под ред. Г.Н. Малиновского. Москва : ЦИПК, 1996. С. 182–209.
8. Малков С.П. История правового регулирования космической деятельности по исследованию и освоению небесных тел в России : автореф. дисс. ... канд. юрид. наук : 12.00.01 «Теория и история права и государства; история учений о праве и государстве». Санкт-Петербург, 2005. URL: https://www.dissercat.com/content/istoriya-pravovogo-regulirovaniya-kosmicheskoi-deyatelnosti-po-issledovaniyu-i-osvoeniyu-neb.
9. Дослідження космосу в Україні. Винаходи та інновації. Винахідники України. Логос України. URL: http://www.logos.biz.ua/proj/vynahid/online/34.php.

УДК 343.5
DOI https://doi.org/10.32844/2618-1258.2020.1.5

ЯКОВЛЄВ П.О.

ПРОБЛЕМАТИКА ТЛУМАЧЕННЯ КАТЕГОРІЇ «ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ» В СУЧАСНІЙ ЮРИДИЧНІЙ ДОКТРИНІ УКРАЇНИ

У статті висвітлено проблематику тлумачення категорії «інформаційна безпека держави» у сучасній юридичній доктрині. Відзначено, що поняття інформаційної безпеки держави стало одним із найбільш уживаних як на рівні чинного законодавства, так і на рівні наукової полеміки. На основі аналізу положень національне законодавство України акцентовано увагу на тому, що воно містить зазначену категорію, проте її зміст викладено недосконало. Зазначена обставина може мати певні негативні наслідки для правозастосовної практики, адже процес забезпечення інформаційної безпеки системою уповноважених державних органів складається з широкого комплексу адміністративних дій і рішень, здійснення яких пов'язане з потенційною можливістю обмеження прав і свобод громадян України

Запропоновано авторський перелік чинників, які зумовлюють складнощі розуміння категорії «інформаційна безпека держави». Зокрема, це різноманітність контексту, у якому тлумачиться категорія «інформаційна безпека», неоднозначність кількості складових частин структури інформаційної безпеки як явища, недостатнє врахування того, що забезпечення інформаційної безпеки є самостійним напрямом державного управління, а також особливості міжнародно-правового визначення відповідної категорії. Очевидно, що наведений перелік чинників не є вичерпним і може бути продовжений. Проаналізуємо вказані чинники більш детально. Обґрунтовано, що юридичний вимір тлумачення змісту категорії «інформаційна безпека держави» має базуватися на усвідомлення того, що забезпечення інформаційної безпеки є самостійним напрямом державної політики, системою владно-управлінських дій і рішень, які реалізуються за участі громадянського суспільства та спрямовані на всебічне забезпечення і захист публічних інтересів держави та приватних інтерсексів громадян як учасників інформаційних процесів.

Зазначено, що перспективним напрямом наукових досліджень є вироблення узагальнюючого поняття «інформаційна безпека держави», яке б відображало безперервний процес функціонування уповноважених державних органів у взаємодії з інститутами громадянського суспільства, що спрямований на попередження за-

© ЯКОВЛЄВ П.О. – кандидат юридичних наук, докторант (Харківський національний університет імені В.Н. Каразіна)

гроз, відвернення ризиків і припинення дій, які посягають на національний інформаційний простір, а також загрожують державному ладу і створюють передумови для порушення прав громадян.

Ключові слова: *інформація, інформаційна безпека держави, національна безпека, права громадян, інформаційний простір, кібербезпека, державне управління.*

The article deals with the problems of interpretation of the category "information security of the state" in the current legal doctrine. It is noted that the concept of information security of the state has become one of the most used at the level of current legislation and at the level of scientific controversy. On the basis of the analysis of the provisions, the national legislation of Ukraine emphasizes that it contains the specified category, but its content is poorly stated. This circumstance may have some negative consequences for law enforcement practice, since the process of providing information security by the system of authorized state bodies consists of a wide range of administrative actions and decisions, the implementation of which is connected with the potential restriction of the rights and freedoms of Ukrainian citizens.

The author's list of factors that cause difficulties in understanding the category "information security of the state" is proposed. In particular, this is the variety of contexts in which the category "information security" is interpreted, the ambiguity of the number of components of the information security structure as a phenomenon, the insufficient consideration that providing information security is an independent direction of public administration, and also the peculiarities of international legal definition of the relevant category. Obviously, the list of factors is not exhaustive and can be continued. Let's analyze these factors in more detail. It is substantiated that the legal dimension of interpreting the content of the category "information security of the state" should be based on the realization that providing information security is an independent direction of public policy, a system of governing and administrative actions and decisions implemented with the participation of civil society and aimed at comprehensive provision and protection public interests of the state and private interest citizens as participants of information processes.

It is noted that a promising area of scientific research is the development of a generalized concept of "information security of the state", which would reflect the continuous process of functioning of authorized state bodies in cooperation with civil society institutions, aimed at preventing threats, preventing risks and preventing national action space, as well as threaten the state system and create preconditions for violation of citizens' rights.

Key words: *information, information security of the state, national security, citizens' rights, information space, cyber security, public administration.*

Вступ. На початку XXI століття категорія «інформаційна безпека» стала одним із найбільш уживаних понять, яким оперують на всіх рівнях політики громадські діячі, спеціалісти різних галузей діяльності та, зокрема, юристи-науковці. Це пов'язано з тим, що в сучасному світі інформаційне середовище будь-якої держави є потенційним об'єктом протиправних посягань із боку недоброзичливих держав, контрольованих ними суб'єктів, а також приватних осіб та корпорацій. Україна, на жаль, не стала виключенням, адже за останні кілька років національний інформаційний простір неодноразово ставав об'єктом інформаційних атак і диверсій.

На теперішній час в Україні сформовано певну законодавчу базу забезпечення інформаційної безпеки нашої держави. Проте, незважаючи на те, що зазначена категорія вживається у багатьох актах чинного законодавства різної юридичної сили і предмету правового регулювання, її визначення на нормативному рівні залишається недосконалим. Так, у Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» від 09.01.2007 р. № 537-V інформаційна безпека визначається як стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігається нанесення шкоди зазначеним об'єктам через низку неправомірних дій [1]. Разом із цим зміст вказаного визначення є занадто «загальним» за наповненням і не відповідає вимогам часу, адже з нього не зрозуміло, що саме слід розуміти під інформаційною безпекою держави. Крім цього, зазначений законодавчий акт було прийнято тринадцять років тому і, незважаючи на формальну чинність, термін його регулятивного призна-

чення сплив. За цих умов, на тлі недосконалості законодавчо визначеного поняття «інформаційна безпека держави», зазначена дефініція зустрічається в багатьох наукових працях та обговорюється на численних науково-практичних конференціях і круглих столах. Це свідчить про увагу юридичної доктрини України до дослідження різних аспектів забезпечення інформаційної безпеки держави. У зв'язку із цим очевидною стає доцільність з'ясування чинників неоднозначного наукового тлумачення терміна «інформаційна безпека держави» у сучасній юридичній науці. Відповідно, **метою** статті є висвітлення чинників, які зумовлюють проблематику формування уніфікованого підходу до тлумачення змісту поняття «інформаційна безпека держави».

Обрані у спектр наукової уваги питання частково досліджувалися такими вченими, як О.М. Кісілевич-Чорнойван, Б.В. Паш, О.М. Степко, В.І. Шульга та ін. Проте доктринальна розробка аспектів дослідження інформаційної безпеки держави як соціально-правового феномену на сьогодні є недостатньою і потребує поглиблення з урахуванням актуалізації проблематики використання інформації як ресурсу державного розвитку і забезпечення національної безпеки кожної демократичної правової держави сучасного світу.

Результати дослідження. За останнє десятиліття юридична доктрина Україна збагатилася значною кількістю наукових праць із проблематики забезпечення інформаційної безпеки. Активізація діяльності вчених-юристів у напрямі наукової розробки аспектів забезпечення інформаційної безпеки була зумовлена, передусім, прийняттям базових нормативних актів у сфері забезпечення інформаційної безпеки: Конституції України від 28.06.1996 року, Доктрини інформаційної безпеки України, яку введено в дію Указом Президента України від 25 лютого 2017 року № 47/217, Закону України «Про національну безпеку України» від 21.06.2018 року № 2469-VIII, Конвенції Ради Європи про кіберзлочинність від 23.11.2001 року та іншими [2; 3; 4; 5]. Також важливим чинником, який зумовлює постійний приріст наукового доробку з питань інформаційної безпеки, є намагання все більшої кількості науковців реагувати на високу динаміку удосконалення і зімни форм і методів посягання на інформаційну складову частину життєдіяльності держав і народів. Відповідно, як зауважує О.М. Кісілевич-Чорнойван, простежуються намагання сформувати всеохоплююче, багатопланове поняття інформаційної безпеки, яке б відбивало реальність з урахуванням складності і дискусійності даного питання [6].

Переходячи безпосередньо до аналізу проблематики тлумачення категорії «інформаційна безпека держави», вважаємо доцільним виокремити кілька чинників, які зумовлюють складнощі розуміння вказаного поняття. Зокрема, це різноманітність контексту, у якому тлумачиться категорія «інформаційна безпека», неоднозначність кількості складових частин структури інформаційної безпеки як явища, недостатнє врахування того, що забезпечення інформаційної безпеки є самостійним напрямом державного управління, а також особливості міжнародно-правового визначення відповідної категорії. Очевидно, що наведений перелік чинників не є вичерпним і може бути продовжений. Проаналізуємо вказані чинники більш детально.

Першим, найбільш важливим чинником, який зумовлює проблематику визначення категорії «інформаційна безпека», **є різноманітність контексту**, у якому вказане явище аналізується вченими-юристами. Так, ураховуючи положення чинного законодавства, інформаційна безпека як поняття вживається в контексті визначення функцій держави та громадянських обов'язків громадян України (ст. 17 Конституції України), в контексті визначення складових частин державної політики у сфері національної безпеки і оборони України (ст. 3 Закону України «Про національну безпеку»), в контексті розвитку інформаційного суспільства (п. 13 Закону України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки»), в контексті регламентації прав і обов'язків суб'єктів сектору безпеки і оборони держави (нормативні акти, які регламентують статус суб'єктів забезпечення національної безпеки і оборони), в контексті встановлення юридичної відповідальності за правопорушення, об'єктом яких є інформація, інформаційні інтереси держави та особи (Кодекс України про адміністративні правопорушення містить, за нашими підрахунками, 41 склад адміністративних правопорушень об'єктом посягання, у яких визначено інформацію або елементи інформаційної інфраструктури України [7]). Крім цього, тлумачення категорії інформаційної безпеки відбувається в контексті регламентації розвитку та захисту технічного забезпечення національного інформаційного простору, в контексті аналізу правових аспектів планування та реалізації державної політики у сфері захисту кіберпростору України і використання ресурсів Інтернет та ін.

Через те, що сучасна юридична доктрина розглядає інформаційну безпеку в контексті прив'язки до певного родового об'єкта, зміст категорії «інформаційна безпека» визначається в логічній «прив'язці» до такого об'єкта. Так, О.М. Кісілевич-Чорнойван, досліджуючи спів-

відношення понять «інформаційна безпека» та «міжнародна інформаційна безпека» у працях значної кількості науковців, справедливо робить висновок про те, що більшість сучасних правознавців сходяться на думці, що інформаційна безпека розглядається або як стан захищеності важливих інтересів особи, суспільства і держави, за якого зводиться до мінімуму нанесення шкоди через негативний інформаційний вплив, або як стан захищеності інформаційного середовища як складової частини національної безпеки, який забезпечує його формування, використання і розвиток в інтересах громадян та організацій держави [6]. Відповідно, такий підхід заздалегідь визначає, що інформаційна безпека аналізується у статиці як сформований «стан», характеристика безпекового, правового або технологічного середовища. Разом із тим останнім часом науковці поступово починають орієнтуватися на те, що інформаційна безпека держави являє собою певну діяльність, тобто враховувати динамічний вимір тлумачення цієї категорії. В.І. Шульга зазначає, що інформаційна безпеки держави є процесом, діяльністю та результатом діяльності людини, яка спрямована на забезпечення безпеки в інформаційній сфері у майбутньому з урахуванням змістовних показників [8]. Це дає підстави вважати, що юридична доктрина впритул наблизилася до активізації дослідження інформаційної безпеки держави з урахуванням поєднання двох зазначених підходів.

Другий чинник, який тривалий час зумовлював проблемність уніфікованого визначення категорії «інформаційна безпека держави», полягає в **невизначеній кількості складових частин інформаційної безпеки**. Ситуація дещо змінилася з набранням чинності вже згадуваної Доктрини інформаційної безпеки України. Документ визначає, що складовими частинами інформаційної безпеки держави України є національні інтереси в інформаційній сфері, які включають у себе приватний і публічний компонент. Приватний компонент вбирає в себе життєво важливі інтереси особи (забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації, на захист приватного життя; захищеність від руйнівних інформаційно-психологічних впливів), а публічний – життєво важливі інтереси суспільства і держави (захист українського суспільства від агресивного впливу деструктивної пропаганди інших держав, розвиток медіа-культури суспільства та соціально відповідального медіа-середовища, формування ефективної правової системи захисту особи, суспільства та держави від деструктивних пропагандистських впливів, розвиток технічної інфраструктури захисту національного інформаційного середовища та ін.). Структура інформаційної безпеки держави може бути значно ширшою. Посилаючись на науковий доробок Б.В. Паша, є підстави констатувати, що інформаційна безпека держави також може включати в себе свідомість, психіку людей; інформаційно-технічні системи різного масштабу і призначення, коло суб'єктів забезпечення інформаційної безпеки [9, с. 511]. Також вважаємо, що сьогодні повноцінним елементом структури інформаційної безпеки держави слід вважати ринок інформаційних послуг та інформаційних продуктів. У сучасній державі вказаний сегмент дедалі більше розширюється і відграє з кожним днем все більшу роль у формуванні економічного потенціалу держави. Оскільки інформація охоплює всі сфери людської діяльності, забезпечуючи зростання матеріальних і духовних сил суспільства, її вплив на механізм адміністративно-правового забезпечення інформаційної безпеки видається доволі значним. Відповідно, формування інформаційних ресурсів є запорукою вирішення проблем соціально-економічного розвитку країни.

Слід також наголосити, що більшість науковців під час наведення авторських варіацій тлумачення категорії «інформаційна безпека» не враховують можливостей потенційної участі громадянського суспільства у відповідних процесах. Імперативом сьогодення стало те, що інститути громадянського суспільства мають колосальні можливості для формування інформаційного простору держави. Більше того, в епоху постінформаційного суспільства генеруючий інформаційний ресурс інститутів громадянського суспільства в окремих напрямах перевищує можливості держави, а також, як зауважує А. Турчак, багато у чому визначає економічну потужність держави та потребує особливого захисту [10, с. 47]. З огляду на це подальше наукове дослідження змісту категорії «інформаційна безпека держави» має здійснюватися з урахуванням ролі та можливостей громадянського суспільства. Висловлена позиція повністю відповідає конституційному положенню про те, що забезпечення інформаційної безпеки є справою всього українського народу. Сучасним науковим працям, у центрі яких є розкриття змісту інформаційної безпеки, бракує врахування національного досвіду діяльності інститутів громадянського суспільства, які спеціалізуються на сприянні державі у питаннях забезпечення інформаційної безпеки. Більше того, діяльність окремих таких організацій, які протидіють інформаційним агресіям в Україні, широко висвітлена в публічному інформаційному просторі [11].

Третім чинником, який визначає проблематику розуміння сутності та тлумачення категорії «інформаційна безпека держави», є **недостатнє врахування того, що забезпечення інформаційної безпеки є самостійним напрямом державного управління.** Юридичний вимір тлумачення змісту категорії «інформаційна безпека держави» має базуватися на усвідомлення того, що забезпечення інформаційної безпеки є самостійним напрямом державної політики, системою владно-управлінських дій і рішень, які реалізуються за участю громадянського суспільства та спрямовані на всебічне забезпечення і захист публічних інтересів держави та приватних інтерсексів громадян як учасників інформаційних процесів. Якщо вдатися до деталізованого аналізу сутності державного управління у сфері забезпечення інформаційної безпеки, то слід мати на увазі складну систему управлінських заходів. Зокрема, це розроблення нормативно-правових і організаційно-методичних документів; розроблення концепції інформаційної безпеки, спеціальних правових і організаційних заходів, що забезпечують збереження і розвиток інформаційних ресурсів; формування правового статусу суб'єктів системи інформаційної безпеки; розроблення законодавчих і нормативних актів, що регулюють порядок ліквідації наслідків загроз інформаційній безпеці; відновлення порушеного права і ресурсів, розроблення компенсаційних заходів; вдосконалення організації форм і методів запобігання і нейтралізації загроз інформаційній безпеці; розвиток сучасних методів забезпечення інформаційної безпеки, розвиток науково-практичних основ інформаційної безпеки; розвиток законодавчої і нормативно-правової бази забезпечення інформаційної безпеки [12, с. 96]. Спираючись на зазначене, вважаємо доцільним доповнити чинну Доктрину інформаційної безпеки визначенням інформаційної безпеки саме як самостійного напряму державної управлінської політики з урахуванням конкретизації форми участі інститутів громадянського суспільства України в залученні до розробки і практичної реалізації управлінських заходів, спрямованих на забезпечення інформаційної безпеки.

Четвертий чинник ускладнення тлумачення змісту поняття «інформаційна безпека держави» випливає з **особливостей міжнародно-правової регламентації вказаного поняття**. Сучасні джерела міжнародного права, особливо на рівні ООН, містять значну кількість правових конструкцій, які тим чи іншим чином регламентують аспекти реалізації державної політики з питань забезпечення інформаційної безпеки. Здебільшого це положення загальних відомих документів ООН у галузі прав людини. Разом із тим найбільше інформаційна безпека згадується в резолюціях Генеральної асамблеї ООН (далі – ГА ООН), які присвячені питанню розвитку інформаційно-комунікаційного, інформаційно-технічного простору і питанням загальної безпеки на інформаційному рівні. Упродовж останніх десятиліть ГА ООН ухвалила значну кількість документів, які містять категорію «інформаційна безпека», кваліфікаційні ознаки цього поняття, але не тлумачать його. Як приклад виокремимо кілька документів. Зокрема, це Резолюція ГА ООН 60/45 «Досягнення в галузі інформатизації та телекомунікацій у контексті міжнародної безпеки» в редакції від 02.12.2008 р. [13]. Резолюція закріплює положення про те, що держави – члени ООН розробляють управлінські заходи, спрямовані на протидію загрозам інформаційної безпеки з урахуванням гарантування дотримання вільного доступу до інформації. Також слід вказати на положення Резолюції ГА ООН 64/211 «Створення глобальної культури кібербезпеки та оцінка національних зусиль із захисту найважливіших інформаційних інфраструктур» від 21.12.2009 р. [14]. Зокрема, в документі визначено, що кожна держава самостійно визначає заходи захисту власних інформаційних інфраструктур за умови забезпечення рівного доступу до інформаційних технологій та обімну інформацією з міжнародним співтовариством із питань актуальних загроз інформаційній безпеці. Так чи інакше, але міжнародно-правова регламентація аспектів інформаційної безпеки не містить чіткого тлумачення цього поняття.

Висновки. Наведене вище дає підстави констатувати, що категорія «інформаційна безпека держави» є однією з найбільш уживаних у сучасній юридичній доктрині і національному законодавстві України. Разом із тим юридична наука поки на виробила уніфікованого визначення змісту терміна «інформаційна безпека держави». Безперечно, це має певні негативні наслідки для правозастосовної практики, адже процес забезпечення інформаційної безпеки системою уповноважених державних органів складається з широкого комплексу адміністративних дій і рішень, здійснення яких пов'язане з потенційною можливістю обмеження прав і свобод громадян України. Основні чинники, які зумовлюють складнощі розуміння вказаного поняття, ми пов'язуємо з різноманітністю контексту, в якому тлумачиться категорія «інформаційна безпека», неоднозначністю кількості складових частин структури інформаційної безпеки як явища, недостатнім урахування того, що забезпечення інформаційної безпеки є самостійним напрямом державного управління, а також особливостями міжнародно-правового визначення відповідної категорії.

У зв'язку із цим перспективним напрямом наукових досліджень є вироблення узагальнюючого поняття «інформаційна безпека держави», яке б відображало безперервний процес функціонування уповноважених державних органів у взаємодії з інститутами громадянського суспільства, що спрямований на попередження загроз, відвернення ризиків і припинення дій, які посягають на національний інформаційний простір, а також загрожують державному ладу і створюють передумови для порушення прав громадян.

Список використаних джерел:

1. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України від 09.01.2007 р. № 537-V. *Відомості Верховної Ради України*. 2007. № 12. Ст. 102.

2. Конституція України від 28.06.1996 р. *Відомості Верховної Ради України*. 1996, № 30, ст. 141.

3. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» : Указ Президента України від 25 лютого 2017 року № 47/217. *Офіційний вісник Президента України*. 2017. № 5. С. 15.

4. Про національну безпеку України: Закон від 21.06.2018 р. № 2469-VIII. *Відомості Верховної Ради України*. 2018. № 31. Ст. 241.

5. Про ратифікацію Конвенції про кіберзлочинність: Закон України від 07.09.2005 р. № 2824-IV. *Відомості Верховної Ради України*. 2006. № 5. Ст. 71.

6. Кісілевич-Чорнойван О.М. Інформаційна безпека та міжнародна інформаційна безпека: проблема визначення понять. *Інтернет-сайт «Правник. Бібліотека наукової юридичної літератури».* URL : http://www.pravnuk.info/2013-12-27-15-12-23/120-informacijna-bezpeka-ta-mizhnarodna-informacijna-bezpeka-problema-viznachennya-1ponyat.html (дата звернення: 14.04.2020).

7. Кодекс України про адміністративні правопорушення від 07.12.1984 р. № 8073−10. *Відомості Верховної Ради УРСР*. № 51. Ст. 1122.

8. Шульга В. І. сучасні підходи до трактування поняття інформаційна безпека. *Електронний журнал «Ефективна економіка».* 2015. № 4. URL : http://www.economy.nayka.com.ua/?op=1&z=5514 (дата звернення: 28.04.2020).

9. Паш Б.В. Складові інформаційної безпеки держави: постановка питання. *Матеріали IX Міжнародної науково-практичної конференції* (20-22 квітня 2017 року, м. Ужгород). Том 1. Видання Ужгородського національного університету. Ужгород. 2017. С. 509–513.

10. Турчак А. Основні складові інформаційної безпеки держави. *Аспекти публічного управління*. 2019. № 5 Т. 7 С. 44–56.

11. Antiseparatizm campaigns for for the security service of Ukraine in 2015-2016 of Ukraine in 2015-2016. *Інтернет-сторінка ГО «Інформаційна безпека».* URL : http://inform-security.com/ua (дата звернення: 15.04.2020).

12. Степко О.М. Аналіз головних складових інформаційної безпеки держави. *Науковий вісник Інституту міжнародних відносин НАУ. Серія: Економіка, право, політологія, туризм*. Київ : Видавництво Національного авіаційного університету. 2011. Вип. 1(3). С. 90–99.

13. Резолюція 64/211, прийнята Генеральною Асамблеєю Організації Об'єднаних Націй «Створення глобальної культури кібербезпеки та оцінка національних зусиль із захисту найважливіших інформаційних інфраструктур». *Офіційний інтернет-сайт Організації Об'єднаних Націй*. URL : https://undocs.org/ru/A/RES/64/211 (дата звернення: 16.04.2020).

14. Резолюції 65/141, прийнята Генеральною Асамблеєю Організації Об'єднаних Націй «Використанні інформаційно-комунікаційних технологій з метою розвитку». *Офіційний інтернет-сайт Організації Об'єднаних Націй*. URL : https://undocs.org/ru/A/RES/65/141 (дата звернення: 08.04.2020).