Анна Валерьевна ЯКОВЛЕВА,
профессор кафедры экономической теории и экономического образования Российского государственного педагогического университета имени А. И. Герцена, доктор экономических наук, доцент
yeif@mail.ru
191186, Россия, г. Санкт-Петербург, Реки Мойки наб., д. 48

Проблемы правового обеспечения в становлении института кибергигиены

Аннотация. *Киберпространство, кибермир или виртуальный мир стали неизбежной реальностью жизни современного общества. Период пандемии COVID-19 еще более активизировал отношения граждан с киберпространством, что, в свою очередь, ведет к росту киберпреступлений в современном виртуальном мире. Поэтому для защиты своего информационного пространства каждому пользователю, в самом широком смысле этого термина, стало необходимо применять безопасные методы при использовании Интернета. Совокупность этих мер безопасности получила название «кибергигиена».*
Данная статья посвящена проблемам правового обеспечения развивающегося института кибергигиены, который на современном этапе играет решающую роль в защите не только информационной инфраструктуры современного бизнеса, но и данных отдельных пользователей. Автор акцентирует внимание на том, что в данный период еще не сформировался понятийный аппарат правового обеспечения в практике информационных отношений в сфере кибергигиены. При этом подчеркиваются важность и необходимость становления и развития данного института на основе анализа растущих киберпреступлений, свидетельствующих о пока еще слабом уровне кибергигиены.
Ключевые слова: *кибергигиена; информационная безопасность; кибербезопасность; киберпреступления; институт кибиргигиены.*

DOI: 10.17803/2311-5998.2023.102.2.062-070

ANNA V. IAKOVLEVA,
Professor of the Department of economic theory and economic education of the Herzen Russian State Pedagogical University, Dr. Sci. (Economics), Associate Professor
yeif@mail.ru
48, Reki Mojki naberezhnaya, Saint Petersburg, Russia, 191186

Problems of Legal Support of the Cyber Hygiene Institute

Abstract. *Cyberspace, cyberworld or the virtual world has become an inevitable reality of the modern society life. The period of the COVID 19 pandemic has further intensified the relationship between citizens and cyberspace, which in turn leads to an increase in cybercrime in the modern virtual world. Therefore, it has become necessary for each user, taken in the broadest sense of the term, to use secure methods when navigating the Internet in order to protect their own information space. The combination of these security measures is called "cyber hygiene".*

This article is devoted to the problems of legal support for the developing concept of "cyber hygiene", which at present plays a decisive role in protecting, not only the information infrastructure of modern business, but also the data of individual users. The author focuses on the fact that, currently, the conceptual apparatus of legal support in the practice of information relations in the field of cyber hygiene has not yet been formed. At the same time, the importance and necessity of the formation and development of this legal concept is emphasized on the basis of an analysis of growing cybercrimes, indicating a still insufficient level of cyber hygiene.
Keywords: *cyber hygiene; information security; cybersecurity; cybercrime; institute of cyber hygiene.*

Каждое крупное нарушение в сфере информационной безопасности, кибербезопасности заставляет экспертов по безопасности со всего мира говорить о необходимости улучшения и продвижения кибергигиены. Доказательством тому служат достаточно известные инциденты последнего времени с далеко идущими последствиями. В частности, 6 ноября 2022 г. пользователь известного форума хакеров опубликовал CSV-файл объемом 60 ГБ, содержащий неанонимную личную информацию, включая 257 829 454 записи о 228 миллионах пользователей Deezer (французский интернет-сервис потоковой передачи музыки).

Согласно анализу выборки данных, раскрытая конфиденциальная информация, затронувшая миллионы людей из таких стран, как США, Великобритания, Франция, Германия, Бразилия, Мексика, Италия, Турция, Колумбия, Гватемала, включала адреса электронной почты, имена и фамилии пользователей, даты рождения, пол, данные о местоположении, включая город и страну, идентификатор пользователя и дату регистрации. Нужно сказать, что указанная утечка данных произошла еще в 2019 г.

В январе 2022 г. благотворительная организация Красный Крест подверглась компьютерной атаке, в результате которой было скомпрометировано более 500 тысяч записей: преступники похитили информацию о «крайне уязвимых лицах» (как правило, это жертвы войны и возможные свидетели). Подобная информация в последующем может быть продана международным преступным группировкам, которые часто преследуют этих людей.

В 2017 г. произошла атака программ-вымогателей, которая началась с уничтожения данных из компьютерных сетей Национальной системы здравоохранения Великобритании (NHS), а затем распространилась на компьютерные сети более чем в 100 странах мира. 2016 год печально известен взломом серверов Национального комитета Демократической партии во время президентских выборов в США. В 2015 г. было похищено 21,5 миллиона высокой степени секретных записей о текущих и бывших чиновниках федерального правительства США[1]. Этот список с каждым годом продолжает пополняться все новыми инцидентами.

[1] См.: *Vishwanath A., Neo L. S., Goh P., Lee S., Khader M., Ong G., Chin J.* Cyber hygiene: The concept, its measure, and its initial tests // Decision Support Systems. Vol. 128. January, 2020. URL: https://www.sciencedirect.com/science/article/abs/pii/S0167923619301897 (дата

К улучшению кибергигиены призывают не только эксперты по безопасности, но и политики и правительства почти всех стран. Например, в ответ на отчет Управления правительственной отчетности США (GAO), подробно описывающий продолжающееся использование Adobe Flash на компьютерах федерального правительства в июне 2018 г., сенатор-демократ Уайден написал письмо, в котором порицал Агентство национальной безопасности (АНБ), Министерство внутренней безопасности (DHS) и Белый дом за их неспособность применять меры по кибергигиене. Аналогичная критика за недостаточные усилия для обеспечения мер по кибергигиене также была высказана против президента Обамы и его команды[2].

Несмотря на то, что многие эксперты сетуют на недостаточный уровень кибергигиены, неясно, что действительно значит сам термин «кибергигиена». Следует согласиться с авторами, которые отмечают, что фактически нет ни одной академической исследовательской статьи, в которой объяснялось бы это понятие или шла бы речь о ее измерении. Путаница усугубляется еще и тем, что, например, поисковая система Google выдает сотни веб-страниц, созданных блогерами, ИТ-компаниями, и различными экспертами по кибербезопасности, предлагающими всевозможные меры — от очевидных (например, лучше защищать свою электронную почту) до очень специфических (как, например, рекомендация использовать определенную операционную систему или антивирусное программное обеспечение).

Советы из Интернета также включают в себя широкий спектр подходов. Некоторые призывают к усилению бдительности, другие — к повышенной информированности, а третьи советуют пользователям полностью изменить свое поведение (например, звонить в банк по телефону вместо того, чтобы отвечать на любые письма от них).

Еще большую путаницу вносят противоречащие друг другу рекомендации от разных организаций. Например, Национальный институт стандартов и технологий (NIST) в 2018 г. опубликовал руководство, в котором речь шла о кибергигиене в контексте практики управления исправлениями в ИТ[3]; Европейский союз в 2018 г. представил серию общеевропейских инициатив под названием #SaferInternet4EU, охватывающих широкий круг тем, в том числе улучшения кибергигиены среди детей[4].

Валютное управление Сингапура (MAS) в 2018 г. выпустило консультационный документ «Уведомление о кибергигиене», содержащий набор основных практик

обращения: 01.04.2022) ; *Яковлева А. В.* Проблемы правового регулирования информационной безопасности в условиях развития цифровой экономики. Саратов : Амирит, 2021. 272 с.

[2] *Vishwanath A., Neo L. S., Goh P., Lee S., Khader M., Ong G., Chin J.* Op. cit.

[3] Critical Cybersecurity Hygiene: Patching the Enterprise. August 31, 2018 // URL: https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/ch-pe-project-description-draft.pdf (дата обращения: 14.03.2022).

[4] См.: #SaferInternet4EU campaign // URL: https://www.betterinternetforkids.eu/en-GB/saferinternet4eu (дата обращения: 14.03.2022) ; Building a safer and better digital space for children in the EU — Brochure // URL: https://digital-strategy.ec.europa.eu/en/library/building-safer-and-better-digital-space-children-eu-brochure (дата обращения: 14.03.2022).

кибербезопасности, которые должны внедрить финансовые учреждения с целью управления киберугрозами. К таким практикам относятся: своевременное устранение недостатков безопасности системы; установка и реализация надежной безопасности системы; обеспечение безопасности системных подключений; установка антивирусного программного обеспечения; ограничение использования учетных записей системного администратора, которые могут изменять конфигурацию системы; усиление аутентификации пользователей.

В целом можно говорить о том, что MAS включило в понятие «кибергигиена» многофакторную аутентификацию, использование межсетевых экранов и антивирусные программы. Важно подчеркнуть, что MAS предлагает вышеперечисленные меры предусмотреть в качестве базового стандарта гигиены для кибербезопасности, превратив их в юридически обязательные требования[5].

Следует отдельно отметить Директиву ЕС 2022/2055 Европейского Парламента и Совета от 14.12.2022 «О мерах по обеспечению высокого общего уровня кибербезопасности в Союзе, внесении изменений в Регламент (ЕС) № 910/2014 и Директиву (ЕС) 2018/1972, а также об отмене Директивы (ЕС) 2016/1148 (Директива NIS 2)», в которой указано, что политика продвижения кибергигиены обеспечивает основу для защиты инфраструктур сетей и информационных систем, оборудования, программного обеспечения и безопасности онлайн-приложений, а также данных бизнеса или конечных пользователей, на которые полагаются организации.

Данная политика включает общий базовый набор методов, таких как обновление программного и аппаратного обеспечения, смена паролей, управление новыми установками, ограничение доступа на уровне администратора и резервное копирование данных; упреждающую основу для обеспечения готовности и общую безопасность и защищенность в случае инцидента или киберугрозы.

В документе указано, что Европейское агентство сетевой и информационной безопасности (ENISA) будет отслеживать и анализировать политику государств-членов в области кибергигиены. Далее в тексте документа подчеркивается, что осведомленность о кибербезопасности и кибергигиене необходима для повышения уровня кибербезопасности в Союзе, в частности в свете растущего числа подключенных к сети устройств, которые все чаще используются в кибератаках. В связи с этим следует предпринять усилия для повышения общей осведомленности о рисках, связанных с такими устройствами, как на внутреннем так и на внешнем рынке.

Основные и важные организации должны использовать широкий спектр определяющих методов кибергигиены, таких как принципы нулевого уровня слепого доверия, обновление программного обеспечения, конфигурация устройств, сегментация сети, управление идентификацией и доступом или осведомленность

[5] См.: MAS consults on draft Notice on Cyber Hygiene for financial institution. 27 September, 2018 // URL: https://www.allenandgledhill.com/sg/publication/articles/7505/mas-consults-on-draft-notice-on-cyber-hygiene-for-financial-institutions (дата обращения: 14.03.2022) ; Consultation Paper on Notice on Cyber Hygiene. 03 September, 2018 // URL: https://www.mas.gov.sg/publications/consultations/2018/consultation-paper-on-notice-on-cyber-hygiene (дата обращения: 14.03.2022).

пользователей, организовать обучение своего персонала и повышать осведомленность о киберугрозах, фишинге или методах социальной инженерии.

Кроме того, организации должны оценивать свои собственные возможности кибербезопасности и при необходимости стремиться к интеграции технологий повышения кибербезопасности, таких как искусственный интеллект или системы машинного обучения, для расширения своих возможностей и безопасности сетей и информационных систем.

Данной Директивой вменяется в обязанность государствам — членам ЕС осуществлять продвижение и развитие образования и обучения по кибербезопасности, а также руководство по передовым методам и средствам контроля кибергигиены, предназначенным для граждан, заинтересованных сторон и организаций[6].

Из всего вышеизложенного становится ясно, что кибергигиена не является единичным действием, а включает комплекс разнообразных мер: от эффективного управления исправлениями до отказа от использования определенных типов программного обеспечения, а также от резервного копирования файлов компьютеров до избежания кибертравли и определения ложных новостей. И этот комплекс мер должен быть применим к различным субъектам: от организаций гражданского общества и ИТ-менеджеров до обычных пользователей Интернета, детей и даже президента.

На практике мы наблюдаем, что каждый раз предлагаются разные меры, и пользователям не всегда понятны их значение и важность. Кроме того, такое расплывчатое определение столь важного понятия, как «кибергигиена» и не всегда проверенные предлагаемые меры мало помогают повышению киберустойчивости, тем самым сбивая с толку и ИТ-менеджеров, и конечных пользователей, предлагая противоречивые советы, которые еще больше ослабляют нашу способность защитить киберпространство. Если мы когда-либо надеемся достичь кибер-устойчивости, нам необходимо четко объяснить, что такое кибергигиена и почему она так важна[7].

Известно, что первым употребил термин «кибергигиена» старший вице-президент по интернет-архитектуре и технологиям MCI WorldCom Винтон Г. Серф в своем заявлении для объединенного экономического комитета 23 февраля в 2000 г.. Он сказал: «Я считаю, что сам Интернет по большей части безопасен, хотя есть шаги, которые, как мы знаем, можно предпринять для повышения безопасности и устойчивости. Большинство уязвимостей исходит от тех, кто использует Интернет (компании, правительства, академические учреждения и отдельные лица), но не соблюдает то, что я называю хорошей кибергигиеной. Они недостаточно чувствительны к необходимости защиты безопасности интернет-сообщества,

---

[6] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance) // URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj (дата обращения: 14.01.2023).

[7] *Vishwanath A., Neo L. S., Goh P., Lee S., Khader M., Ong G., Chin J.* Op. cit.

частью которого они являются. Когда дело касается безопасности, открытость Интернета — это одновременно его благословение и проклятие»[8].

В английской Энциклопедии законодательства по информационным технологиям (The IT Law Wiki) «кибергигиена» определяется как шаги, которые пользователи компьютеров могут предпринять для повышения своей кибербезопасности и лучшей защиты в Интернете. Это может включать реорганизацию ИТ-инфраструктуры, оборудования и устройств; использование патчей для лицензионного программного обеспечения и удаление нелицензионного программного обеспечения; постоянный мониторинг, обучение и осведомленность; а также формализацию существующих неформальных мер контроля информационной безопасности[9].

Агентство Европейского союза по сетевой и информационной безопасности (ENISA) отмечает, что кибергигиена должна рассматриваться так же, как и личная гигиена, и после правильной интеграции в организацию это будут простые повседневные распорядки, правильное поведение и периодические проверки, чтобы убедиться, что онлайн-здоровье организации находится на высоте. Кибергигиена включает оборудование, программное обеспечение, ИТ-инфраструктуру, обучение информированности о кибербезопасности и собственные устройства сотрудников компании[10].

В китайском источнике «Что такое кибергигиена? Почему она важна?» о кибергигиене говорится как о шагах, предпринимаемых пользователями компьютеров для защиты своего оборудования и поддержания его в наилучшем состоянии: «Так же, как вы следуете определенным гигиеническим привычкам, чтобы оставаться здоровым, компьютерная сеть, которую вы используете, также должна быть в порядке. Кибергигиена означает проверку того, соответствует ли сеть, используемая вашей компанией, надлежащим требованиям, чтобы у киберпреступников (хакеров) было меньше возможностей взлома и контроля». Другими словами, термин «кибергигиена» означает обеспечение безопасности и актуализации вашего компьютера и сети, что затрудняет доступ хакеров к ним[11].

В индийском Интернете (англо- и хиндиязычном) четкое определение термина «кибергигиена» отсутствует. Чаще всего индийский Google при соответствующем запросе выводит на страницу Лаборатории Касперского с разделами «Cyber hygiene definition» и «What is cyber hygiene?». Несмотря на то, что страница эта создана специально для Индии, ее содержание полностью совпадает с содержанием других англоязычных страниц Лаборатории (для Великобритании, США и Австралии). На странице Министерства электроники и IT Индии также

[8] Statement of Dr. Vinton G. Cerf Senior Vice President of Internet Architecture & Technology MCI WorldCom For the Joint Economic Committee February 23, 2000 // URL: https://www.jec.senate.gov/archive/Documents/Hearings/cerf22300.htm (дата обращения: 15.04.2022).

[9] The IT Law Wiki // URL: https://itlaw.wikia.org/wiki/Cyber_hygiene (дата обращения: 15.04.2021).

[10] ¿Qué es la higiene cibernética y por qué es importante? // URL: https://ciberseguridad.com/guias/higiene-cibernetica/#%c2%bfque_es_la_higiene_cibernetica (дата обращения: 15.04.2021).

[11] 什么是网络卫生？为什么重要? // URL: https://zh.anipi.org/maintain-cyber-hygiene-4980#menu-1 (дата обращения: 15.04.2021).

нет четкого определения этого термина, хотя он представлен в Общем онлайн-курсе по кибербезопасности, целью которого является прежде всего обучение практическим навыкам кибергигиены. В целом складывается впечатление, что там отсутствует разграничение понятий «кибергигиена» и «кибербезопасность», они оказываются взаимозаменяемыми[12].

Что касается позиции отечественных авторов в отношении термина «кибергигиена», то под ней понимается: соблюдение элементарных основ цифровой безопасности при работе с сетью Интернет (С. Кузнецов)[13]. Такой же точки зрения придерживается Е. В. Сафронов, с той лишь оговоркой, что это должно происходить на уровне повседневной привычки[14]. В. Минин отмечает, что главное — соблюдать информационную гигиену и профилактику. Нужны внимание и самоконтроль, а также корпоративное обучение со стороны руководителей ИТ- и ИБ-служб[15].

А. А. Козырева в своем исследовании предприняла попытку определить понятие «кибергигиена», с учетом возможности его применения в правовом поле, как «систематическое применение технических мер предосторожности, предпринимаемых пользователями с целью обеспечения конфиденциальности личной информации, безопасности и безопасности конфиденциальных данных от преступлений с применением современных ИКТ».

Таким образом, исследователи определяют термин «кибергигиена» через шаги, которые компьютерные пользователи могут предпринять, чтобы улучшить личную кибербезопасность и лучше защитить себя в Интернете. Следует не согласиться с авторами, указывающими на то, что «безусловно, закрепление ответственности за непременение кибергигиены на законодательном уровне не является необходимым, так как это является личным делом каждого пользователя». При этом, отмечается, что именно внедрение «кибергигиенических» привычек может позволить минимизировать объем преступлений, совершаемых с применением ИКТ[16].

Мы считаем, что в век стремительного развития ИКТ и появления новых угроз соблюдение определенных «кибергигиенических» мер становится обязательным и требует закрепления ответственности за непременение указанных мер на законодательном уровне, так как, по нашему мнению, просто прививать культуру «кибергигиены» недостаточно.

В поддержку данного тезиса необходимо привести следующие аргументы. Так, по данным Центра рассмотрения жалоб на интернет-преступления (IC3) ФБР

---

[12] Government of India. Ministry of Electronics and Information Technology (MeitY) presents «Generic Online Training Course in Cyber Security» // URL: https://www.infosecawareness.in/cybhyg (дата обращения: 14.12.2022).

[13] *Кузнецов С.* Кибергигиена — личное дело? // URL: https://iz.ru/news/670025 (дата обращения: 14.03.2022).

[14] *Сафронов Е. В.* Азы кибергигиены: Методологические и правовые аспекты. М. : Проспект, 2018. С. 25.

[15] *Козырева А. А.* Определение термина «кибергигиена» и возможность его применения в правовом поле // Проблемы в российском законодательстве. 2018. № 7. С. 92—94.

[16] *Козырева А. А.* Указ. соч. С. 92—94.

(США) за 2021 г. им было получено рекордное количество жалоб от американской общественности: количество принятых жалоб составило 847 376, что на 7 % больше, чем в 2020 г., были заявлены потери, превышающие 6,9 миллиарда долларов.

Преступления, связанные с компрометацией корпоративной деловой электронной почты (BEC) и преступное использование криптовалюты по-прежнему отнимают больше всего денег: по 19 954 жалобам был заявлен общий убыток примерно в 2,4 миллиарда долларов, что на 33 % больше, чем в 2020 г. (1,8 миллиарда долларов).

Распространено также мошенничество с «выуживанием» информации (фишингом, вишингом, смишингом, фармингом): 323 972 жалобы, по которым был заявлен общий убыток в размере более 44 миллионов долларов. Количество инцидентов с программами-вымогателями также продолжает расти: в 2021 г. было зарегистрировано 3 729 247 таких инцидентов, по сравнению с 2020 г. этот показатель вырос на 51%[17]. Безусловно, это далеко не все преступления, которые представлены в указанном отчете. И, как мы можем отметить, сомнений не вызывает тот факт, что слабая кибергигиена обходится обществу дорого.

Таким образом, несмотря на то, что термин «кибергигиена» используется достаточно широко, на сегодняшний день он не имеет официальной трактовки, поскольку не закреплен на законодательном уровне. Отмечается, что в национальном законодательстве «кибер» как часть сложных слов не используется. В Доктрине информационной безопасности 2016 г.[18] закрепляется термин «информационная безопасность», что гораздо шире по своему значению, чем «кибербезопасность».

Тем не менее предполагается, что закрепление термина «кибергигиена» (который является неотъемлемой составляющей «кибербезопасности» или в широком смысле «информационной безопасности») в нормативных правовых документах будет способствовать применению и прививанию навыков личной информационной безопасности и осознанной ответственности пользователей информационно-коммуникационной сети Интернет.

В качестве основной задачи кибергигиены выделяется соблюдение технических мер предупреждения возможных преступлений, совершаемых с использованием современных ИКТ, лично каждым пользователем[19]. И в этой связи на первоначальном этапе встает вопрос о разработке стандартов кибергигиены в сфере информационной безопасности (кибербезопасности) и реализации их как юридически обязательных требований, а в дальнейшем — о развитии института кибергигиены в России.

Важно отметить. что 1 августа 2022 г. в России в рамках федерального проекта «Информационная безопасность» национальной программы «Цифровая

[17] См.: Internet Crime Report 2020 // URL: https://www.ic3.gov/media/pdf/annualreport/2020_ic3report.pdf (дата обращения: 16.05.2022) ; Internet Crime Report 2021 // URL: https://www.ic3.gov/media/pdf/annualreport/2021_ic3report.pdf (дата обращения: 18.04.2022).

[18] Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СЗ РФ. 2016. № 50. Ст. 7074.

[19] *Козырева А. А.* Указ. соч.

экономика» была запущена трехгодичная всероссийская программа кибергигиены (Минцифры России совместно с СПбГУТ имени М. А. Бонч-Бруевича, «Ростелеком-Солар» и АНО «Диалог Регионы»). Отмечается, что ее целью является привлечение внимания к вопросам кибербезопасности и формирование у граждан навыков безопасного поведения в Интернете. При ее реализации планируется повысить информационную безопасность госслужащих, обучить кибергигиене детей и подростков, а также провести всероссийский мониторинг уровня осведомленности граждан о базовых принципах кибербезопасности[20].

БИБЛИОГРАФИЯ

1. *Козырева А. А.* Определение термина «кибергигиена» и возможность его применения в правовом поле // Пробелы в российском законодательстве. — 2018. — № 7. — С. 92—94.
2. *Кузнецов С.* Кибергигиена — личное дело? // URL: https://iz.ru/news/670025 (дата обращения: 14.03.2022).
3. *Сафронов Е. В.* Азы кибергигиены: методологические и правовые аспекты. — М. : Проспект, 2018.
4. *Яковлева А. В.* Зрелость нормативно-правовой базы в области кибербезопасности стран Латинской Америки по модели CMM // Проблемы экономики и юридической практики. — 2022. — Т. 18. — № 4. — С. 20—29.
5. *Яковлева А. В.* Проблемы правового регулирования информационной безопасности в условиях развития цифровой экономики. — Саратов : Амирит, 2021. — 272 с.
6. *Vishwanath A., Neo L. S., Goh P., Lee S., Khader M., Ong G., Chin J.* Cyber hygiene: The concept, its measure, and its initial tests // Decision Support Systems. — Vol. 128. — January, 2020. — URL: https://www.sciencedirect.com/science/article/abs/pii/S0167923619301897 (дата обращения: 01.04.2022).
7. 什么是网络卫生？为什么重要? // URL: https://zh.anipi.org/maintain-cyber-hygiene-4980#menu-1 (дата обращения: 15.04.2022).

[20] Минцифры повышает киберграмотность россиян // URL: https://digital.gov.ru/ru/events/41771/ (дата обращения: 18.12.2022).