Оригинальная статья
УДК 341.236:004
DOI: 10.61205/S199132220031282-6

Вменение государству использования информационно-коммуникационных технологий

Вера Николаевна Русинова[1], *Сергей Павлович Сушков*[2]
[1, 2]Национальный исследовательский университет «Высшая школа экономики», Москва, Россия
[1]vrusinova@hse.ru
[2]sushkov.mels@gmail.com

Аннотация. Вменение государству использования информационно-коммуникационных технологий (ИКТ) для целей привлечения его к международной ответственности представляет собой сложную задачу как с практической, так и юридической точек зрения. В статье проведен анализ степени контроля государства над негосударственными акторами, использующими ИКТ, которой будет достаточно для вменения государству их поведения. Также рассмотрен вопрос разработки специальных правил вменения в отношении так называемого киберпространства.

Цель исследования — выявить возможность адаптации обычных норм права международной ответственности к случаям использования ИКТ негосударственными акторами. Задачи исследования — анализ норм о вменении государству поведения лиц, действующих по указаниям, под руководством или контролем государства, а также обобщение доктринальных подходов к применению данного основания вменения к использованию ИКТ. В круг задач исследования также входит изучение условий, при которых могут возникнуть специальные правила вменения использования ИКТ государству, обзор существующей практики государств и opinio juris в данной области общественных отношений.

Наряду с общенаучными методами исследования были использованы сравнительно-правовой, формально-юридический, исторический методы, а также методология структуралистского критического анализа права.

Вывод. Разработанный Международным Судом тест «эффективного контроля» вряд ли является уместным в «киберконтексте». Текст Статей об ответственности государств за международно-противоправные деяния 2001 г. допускает толкование термина «контроль» за рамками теста «эффективного контроля», а также позволяет применять его в контексте использования ИКТ совместно с тестом «общего контроля». Авторы отмечают крайне осторожный подход, сложившийся в практике государств к вменению вредоносных актов использования ИКТ конкретным государствам, что не способствует возникновению специальных правил вменения в соответствии со ст. 55 Статей об ответственности.

Ключевые слова: вменение, информационно-коммуникационные технологии, кибероперации, право международной ответственности, киберпространство

Благодарности. В данной научной работе использованы результаты проекта «Правовые механизмы преодоления неравенства», выполненного в рамках Программы фундаментальных исследований НИУ ВШЭ в 2024 г.

Для цитирования. Русинова В. Н., Сушков С. П. Вменение государству использования информационно-коммуникационных технологий // Журнал зарубежного законодательства и сравнительного правоведения. 2024. Т. 20. № 5. С. 74—84. DOI: 10.61205/S199132220031282-6

Original article

Attribution of a Use of Information and Communications Technologies to a State

Vera N. Rusinova[1], *Sergey P. Sushkov*[2]
[1, 2]National Research University “Higher School of Economics”, Moscow, Russia
[1]vrusinova@hse.ru
[2]sushkov.mels@gmail.com

Abstract. Attribution of the use of information and communication technologies (ICT) to a state for the purposes of invoking its international responsibility is a complex task from both a practical and legal point of view. The paper examines in detail the extent of state control over non-state actors using ICTs that would be sufficient to attribute their conduct to the state. In addition, the article considers the development of special rules of attribution for the so-called “cyberspace”.

The purpose of the study is to identify the possibility of adapting the usual norms of the law of international responsibility to cases of the use of ICT by non-state actors. The objectives of the study are to analyze the norms on imputing to the state the behavior of persons acting on instructions, under the guidance or control of the state, as well as to generalize doctrinal approaches to the application of this basis of imputation to the use of ICT. The scope of the research also includes the study of conditions under which special rules may arise for imputing the use of ICT to the state, a review of existing State practice and opinio juris in this area of public relations.

Along with general scientific research methods, comparative legal, formal legal, historical methods, as well as the methodology of structuralist critical analysis of law were used.

Conclusion. The test of “effective” control developed by the International Court of Justice is hardly appropriate in the “cyber context”. The text of the Articles on State Responsibility for Internationally Wrongful Acts of 2001 allows the interpretation of the

term “control” beyond the scope of the “effective control” test, and also allows it to be applied in the context of the use of ICT in conjunction with the “general” control test. The authors note the extremely cautious approach that has developed in the practice of States to impute malicious acts of using ICT to specific States, which does not contribute to the emergence of special imputation rules in accordance with Article 55 of the Articles on Liability.

Keywords: attribution, information and communications technologies, cyberoperations, law of state responsibility, cyberspace

Acknowledgments. The results of the project “Legal mechanisms of overcoming inequality”, carried out within the framework of the Basic Research Program at the National Research University Higher School of Economics (HSE University) in 2024, are presented in this work.

For citation. Rusinova V. N., Sushkov S. P. Attribution of a Use of Information and Communications Technologies to a State. *Journal of Foreign Legislation and Comparative Law*, 2024, vol. 20, no. 5, pp. 74—84. (In Russ.) DOI: 10.61205/S199132220031282-6

Введение. Далеко не за всеми случаями вредоносного использования информационно-коммуникационных технологий (далее — ИКТ) стоит конкретное государство. Более того, самый распространенный тип межгосударственных операций — шпионаж — сам по себе международно-противоправным деянием не является[1]. Единственной на текущий момент базой данных о значительных кибероперациях является онлайн «счетчик», который с 2005 г. ведет американский Совет по международным отношениям. Согласно этому ресурсу 34 государства подозреваются в спонсировании кибероперациий, и в этом списке Китай, Россия, Иран и Северная Корея указаны как ответственные за 77% подобных операций[2]. Однако представленные цифры и выводы, во-первых, довольно условны (не ясна методика, по которой одни случаи отражаются в счетчике, а другие — нет) и, во-вторых, предельно субъективны. Например, США не скрывает своих амбиций и потенциала в области кибероперациий, однако инициированные ими кибероперации представлены довольно скромно. В-третьих, несмотря на то что в основе этих данных лежит понятие «спонсирование», что даже не всегда соответствует «политической атрибуции», не говоря уже о международно-правовом вменении, основаниями для этих выводов являются публикации в СМИ и сообщения пользователей.

Меры, принимаемые государствами, пострадавшими от вредоносного использования ИКТ, включают санкции, высылку дипломатов, уголовные обвинения в соответствии с внутренним законодательством и в редких случаях — открытое объявление об «ответном хакерстве». Призвания к международно-правовой ответственности в этом списке — с оговоркой «на текущий момент» — нет. Вместе с тем, как и в «реальном мире», поведение в так называемом киберпространстве[3] может нарушать такие нормы международного права, как запрет применения силы, принцип невмешательства в дела другого государства, обязательства по уважению прав человека или нормы международного гуманитарного права (далее — МГП).

В связи с этим встает вопрос, насколько адекватно международно-правовые нормы о вменении поведения государству, обобщенные в Статьях об ответственности государств за международно-противоправные деяния 2001 г., подготовленных Комиссией международного права ООН (далее — Статьи об ответственности), могут быть адаптированы под специфику использования ИКТ. Потенциально для вменения государству использования ИКТ могут быть различные основания. Одним из самых востребованных и при этом вызывающих серьезные проблемы правового толка является вменение поведения лиц, действующих под руководством и контролем государства. Отсюда возникает потребность разобраться, на основании какого подхода к определению степени необходимого контроля может быть осуществлено вменение государству случаев использования ИКТ лицами и группами, действующими по его указаниям. При этом определение устройства, с помощью которого совершена «кибероперация», и лица, управляющего данным устройством, является крайне сложной задачей с технической точки зрения[4]. В настоящей работе, однако, не рассматриваются технические аспекты определения источника «кибероперации» и использовано допущение, что лицо, совершившее правонарушение в «киберпространстве», а также его связь с государством технически могут быть определены.

1. Вменение государству поведения лиц, действующих по указаниям, под руководством или контролем государства. Чаще всего для того, чтобы скрыть свою неправомерную деятельность с использованием ИКТ, государства привлекают негосударственных акторов. Это могут быть частные IT-организации, «фабрики троллей», отдельно действующие

[1] Это не исключает возможность совершения в ходе шпионажа нарушений отдельных норм международного права, как например, права на неприкосновенность частной и семейной жизни.

[2] Council on Foreign Relations official website, Cyber Operations Tracker. URL: https://www.cfr.org/cyber-operations/ (дата обращения: 05.06.2024).

[3] Для целей настоящей статьи «киберпространство» будет определено как «условная среда, состоящая из Интернета вместе с другими компьютерами и телекоммуникационными сетями, подключенными к Интернету или не подключенными к нему» (*Delerue F.* Cyber Operations and International Law. Cambridge, 2020. P. 12).

[4] См.: *Стрельцов А. А., Капустин А. Я., Русинова В. Н.* и др. Международная безопасность в среде информационно-коммуникационных технологий. М., 2023.

лица или группы так называемых патриотических хакеров[5], объединившихся для инициативной защиты государственных интересов. Их поведение может быть вменено государству, если эти лица действуют по указаниям, под руководством или контролем государства.

Однако на текущий момент в целом вопрос степени государственного контроля над частными лицами, необходимого для вменения их поведения государству, сопряжен со множеством дискуссий и противоречащих друг другу позиций международных судебных органов, международных организаций и ученых-правоведов.

1.1. Международно-правовой обычай и подходы к его толкованию. По сути, главной задачей разработки адекватного правила вменения государству поведения частных лиц является установление баланса между двумя идеями, лежащими в основе права международной ответственности. С одной стороны, действует фундаментальный принцип, согласно которому государства могут нести ответственность только за поведение акторов, действующих от лица государства[6]. С другой стороны, существует необходимость предотвратить ситуации, когда государство действует де-факто через частных лиц, но в то же время избегает международной ответственности и открещивается от их поведения, когда эти лица нарушают международное право[7].

В практике реализации нормы, закрепленной в ст. 8 Статей об ответственности, сложились два основных подхода (или теста) к необходимой степени контроля государства над негосударственными акторами: более и менее строгий.

Строгий подход отражен в решениях Международного Суда ООН, вынесенных по делу о действиях военного и полувоенного характера на территории Никарагуа и против него (далее — дело Никарагуа) и делу о геноциде в Боснии. Согласно данному тесту вменение поведения частных лиц государству возможно, если они действовали в соответствии с указаниями государства или под его «эффективным контролем»[8]. Государство должно осуществлять такой контроль и выдавать такие указания в отношении каждой операции негосударственных акторов, а не в целом в отношении их общих действий[9]. Недопустимо рассматривать «эффективный контроль» государства в разрезе всего комплекса деятельности частных лиц; необходимо оценивать наличие «эффективного контроля» в отношении каждого конкретного действия, в ходе которого совершено правонарушение[10]. Таким образом, общий контроль государства над негосударственными акторами и высокая степень зависимости последних от государства не являются достаточными основаниями для вменения государству их поведения[11].

Тест «эффективного контроля» подвергался острой критике в правовой доктрине. Так, А. Кассезе утверждал, что Международный Суд сформулировал этот подход без опоры на какую-либо практику, а затем в деле о геноциде в Боснии подтвердил его[12]. В деле Никарагуа Международный Суд провозгласил тест эффективного контроля как «аподиктическое знание», не требующее какого-либо доказывания[13]. Комиссия международного права (далее — КМП) в Статьях об ответственности поддержала этот подход, ссылаясь на позицию Международного Суда в деле Никарагуа, а затем сам Суд подтвердил, что ст. 8 Статей об ответственности отражает нормы обычного права[14]. Следовательно, образовался своего рода «эффект эхокамеры», где два органа ссылаются друг на друга, чтобы подтвердить наличие устоявшейся практики. Дж. Кроуфорд описывал это явление как «петлю обратной связи»[15].

Более мягкий подход был применен в деле «Прокурор против Душко Тадича» (далее — дело Тадича), где Апелляционная камера Международного трибунала по бывшей Югославии (далее — МТБЮ, Трибунал) в отличие Международного Суда постановила, что международное право не устанавливает высокий порог контроля во всех без исключения случаях, а степень контроля может варьироваться в зависимости от фактических обстоятельств каждого дела[16]. Согласно данному подходу степень контроля, необходимого для вменения, зависит от того, является ли

---

[5] См.: Интервью специального представителя Президента Российской Федерации по вопросам международного сотрудничества в области информационной безопасности, директора ДМИБ МИД России А. Р. Люкманова МИА «Россия сегодня». 05.01.2024. URL: https://mid.ru/ru/foreign_policy/news/1924120/ (дата обращения: 05.06.2024).

[6] ICJ. Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro). Judgment of 26 February 2007 // I. C.J. Reports. 2007. § 406 (далее — Bosnian Genocide case).

[7] ICTY. Prosecutor v. Dusko Tadic. IT-94-1-A. Appeal Judgement of 15 July 1999 (далее — Tadic case). § 117, 123. См. также: *Cassese A.* The Nicaragua and Tadić Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia // European Journal of International Law. 2007. Vol. 18. Iss. 4. P. 654.

[8] Bosnian Genocide case. § 400. См. также ICJ. Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America). Merits Judgment of 27 June 1986 // I.C.J. Reports. 1986. P. 14. § 115 (далее — Nicaragua case).

[9] Bosnian Genocide case. § 400.

[10] Ibid. § 401.

[11] Nicaragua case. § 115.

[12] См.: *Cassese A.* Op. cit. P. 654.

[13] Ibid. P. 651.

[14] Ibid.

[15] См.: *Crawford J.* State Responsibility: The General Part. Cambridge, 2013. P. 146—147.

[16] Tadic case. § 117.

негосударственный актор отдельным человеком (неорганизованной группой людей) или организованной и иерархически структурированной группой, например воинским подразделением.

В случае контроля над человеком (неорганизованной группой) вменение возможно, если государство «выдало конкретные указания» на совершение конкретного правонарушения[17], что соответствует «стандартам» контроля, установленным Международным Судом[18].

В случае контроля над организованной группой для вменения ее поведения государству достаточен лишь его «общий контроль» (англ. "overall control")[19]. Для установления «общего контроля» необходимо доказать, что государство предоставляло поддержку группе в форме, например, финансирования, обучения, оснащения или иную оперативную поддержку[20], координировало военную деятельность группы либо участвовало в общем планировании этой деятельности[21] таким образом, чтобы можно было сказать, что государство «играет роль» в организации, координации и планировании действий организованной группы. При этом для вменения государству поведения организованной группы нет необходимости доказывать, что государство выдавало конкретные указания на совершение определенных действий, нарушающих международное право[22], или осуществляло планирование всех операций группы[23].

Такого же подхода придерживается и Международный комитет Красного Креста (далее — МККК), который отмечает, что для целей вменения более подходящим является стандарт «общего контроля», поскольку он лучше отражает отношения между вооруженной группой и государством. Кроме того, этот стандарт позволяет вменить государству сразу несколько действий, в то время как тест «эффективного контроля», требующий анализа каждой отдельной операции, труднодоказуем на практике. Наконец, согласно позиции МККК применение стандарта «общего контроля» позволяет избежать ситуации, когда государство становится стороной международного вооруженного конфликта, но в то же время не несет ответственность за нарушения, совершенные в ходе этого конфликта[24].

Стандарт «общего контроля», однако, не был принят Международным Судом, который отмечал, что данный стандарт «практически разрывает связь, которая должна существовать между поведением органов государства и его международной ответственностью»[25]. В попытке установить баланс между стандартом «эффективного контроля» и стандартом «общего контроля» Международный Суд допустил, что тест «общего контроля» может быть уместен при квалификации вооруженного конфликта как международного, но в то же время не должен быть применен при разрешении вопросов вменения[26]. По мнению Суда, «логически допустимо», чтобы тест «общего контроля» и тест «эффективного контроля» различались и существовали параллельно без всякого противоречия, поскольку они призваны разрешать совершенно разные вопросы: квалификацию вооруженного конфликта и международную ответственность государства[27]. МТБЮ, предвосхищая такой аргумент, прямо отразил в решении по делу Тадича, что «исходя из принципов логики» должны быть одинаковыми условия, при которых вооруженный конфликт может быть квалифицирован как международный или поведение может быть вменено государству[28].

КМП намеренно не затрагивала вопрос необходимого для вменения уровня контроля[29]. Статьи об ответственности гласят, что поведение лица или группы лиц может быть вменено государству, «если это лицо или группа лиц фактически действует по указаниям либо под руководством и контролем этого государства при осуществлении такого поведения» (ст. 8). Комиссия подчеркивала, повторяя логику МТБЮ, что вопрос о необходимой степени контроля над частными лицами в любом случае «должен решаться с учетом обстоятельств каждого конкретного дела»[30]. КМП также отмечала, что «каждый случай должен рассматриваться с учетом конкретных обстоятельств дела», которые раскрывают связь между руководством и контролем, осуществляемым государством, и конкретным поведением, о котором заявляет другая сторона[31].

Широкая формулировка ст. 8 допускает применение как строгого стандарта «эффективного контроля», так и более гибкого стандарта «общего контроля». Сложно спорить с тем, что «такая встроенная двусмысленность... дает возможность для прогрес-

---

[17] Tadic case. § 118.

[18] См.: *Cassese A.* Op. cit. P. 657.

[19] Tadic case. § 120.

[20] Ibid. § 137.

[21] Ibid. § 131.

[22] Ibid. § 131, 137.

[23] Ibid. § 137.

[24] International Committee of the Red Cross. Commentary on the Third Geneva Convention: Convention (III) relative to the Treatment of Prisoners of War (Commentaries on the 1949 Geneva Conventions). Cambridge, 2021. P. 113, § 304, fn. 129; P. 164—165, § 443—444.

[25] Bosnian Genocide case. § 406.

[26] Ibid. § 404.

[27] Ibid. § 405.

[28] Tadic case. § 104.

[29] См.: *Crawford J.* Op. cit. P. 147.

[30] Комментарии Комиссии международного права ООН к Проекту статей об ответственности государств за международно-противоправные деяния. A/56/10. 2001. С. 99. § 5 (далее — Комментарии КМП к Статьям об ответственности).

[31] Там же. С. 100, § 7.

сивного развития права международной ответственности государств»[32].

При рассмотрении подходов к уровню контроля, необходимого для вменения поведения государству, следует также прибегнуть к методологии структуралистского критического анализа, заключающегося в выявлении «скрытых» факторов и условий, способствующих принятию определенных международно-правовых решений. Основополагающей предпосылкой такого метода является допущение, что в международном праве возможно существование нескольких одинаково верных ответов на определенные правовые вопросы (например, на вопрос о степени необходимого контроля над негосударственными акторами). Задачей исследователя в таком случае является анализ «структурных предубеждений» (англ: "structural biases") и предпочтений институтов, принимающих решение, определение «способа мышления» этих институтов, а также интересов, из которых эти институты исходили при выборе одного из правил и стандартов, в равной степени убедительных[33].

Применяя данный метод, можно допустить возможность опасений судей Международного Суда в деле Никарагуа того факта, что вменение США поведения, нарушающего МГП, могло лишь усугубить конфликт Суда с Соединенными Штатами, которые к тому моменту уже игнорировали разбирательство в Международном Суде. В связи с этим судьи могли принять «соломоново решение», установив, что США нарушили международное право, поддерживая «контрас», но при этом их поведение США вменено не было[34].

Судьи МТБЮ, напротив, могли быть заинтересованы в квалификации вооруженного конфликта как международного, поскольку такое решение существенно расширило юрисдикцию Трибунала и создало важный прецедент для привлечения как можно бóльшего круга лиц к уголовной ответственности. Члены КМП могли быть заинтересованы в том, чтобы избежать прямого противопоставления позиций Международного Суда и МТБЮ и гармонично истолковать решения судов как не исключающие друг друга. Наконец, судьи Международного Суда могли счесть необходимым согласиться с мнением Комиссии, сделав вид, что позиции МТБЮ и Международного Суда не противоречат друг другу, но при этом не позволить поставить под сомнение авторитет своего предыдущего решения.

1.2. Доктринальные подходы к применению данного основания вменения к использованию ИКТ. Представителей юридической науки, анализировавших применение в «кибер-контексте» правила, закрепленного в ст. 8 Статей об ответственности, можно условно разделить на две группы: одни ученые считают необходимым снизить стандарт контроля для целей вменения поведения государству, другие признают снижение таких стандартов недопустимым.

Наиболее консервативной является позиция, согласно которой необходимо неукоснительно соблюдать стандарт «эффективного контроля» при вменении использования ИКТ государству. Так, эксперты, участвовавшие в разработке Таллинского руководства 2.0, выразили мнение, что при вменении использования ИКТ государству необходимо руководствоваться стандартом «эффективного контроля»[35]. Под «эффективным контролем» авторы этого руководства понимали такую степень контроля, когда именно государство «определяет проведение и ход конкретной операции, а кибердеятельность, осуществляемая негосударственным субъектом, является "неотъемлемой частью этой операции"»[36]. Кроме того, по мнению экспертов, эффективный контроль включает как способность государства обеспечивать проведение мероприятий, составляющих «кибероперацию», так и способность отдать приказ о прекращении тех мероприятий, которые уже проводятся[37]. Общая поддержка негосударственного субъекта со стороны государства (например, предоставление государством вредоносного программного обеспечения) не является достаточным основанием для вменения поведения такого актора государству[38]. Таким образом, авторы Таллинского руководства 2.0 выступили с позиции поддержки практики Международного Суда, требующего установления контроля над конкретной операцией, а не над негосударственным субъектом в целом.

М. Росчини также полагает, что к использованию ИКТ должен применяться тест «эффективного контроля», поскольку сложности с установлением лица, ответственного за «кибероперацию», существенно увеличивают риск того, что государства, которые в действительности никак не связаны с этим актом, могут быть легкомысленно или злонамеренно обвинены в его совершении[39]. Такой сценарий может быть особенно опасен, потому что вменение поведения государству необходимо не только для привлечения государства к международной ответственности, но и для реализации права на самооборону и применения к государству контрмер.

---

[32] Yearbook of the International Law Commission. Vol. II. Part One. 2001. A/CN.4/SER.A/2001/Add.1 (Part 1). P. 49.

[33] Подробнее см.: *Koskenniemi M.* What is Critical Research in International Law? Celebrating Structuralism // Leiden Journal of International Law. 2016. Vol. 29. Iss. 3. P. 727—735.

[34] Nicaragua case. § 116, 216, 220, 226.

[35] См.: Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations / ed. by *M. N. Schmitt.* Cambridge, 2017. P. 96. § 5.

[36] Ibid. P. 96. § 6.

[37] Ibid.

[38] Ibid. P. 97. § 8, 9.

[39] См.: *Roscini M.* Cyber Operations and the Use of Force in International Law. Oxford, 2014. P. 38.

Н. Н. Липкина констатирует, что предложения о снижении стандарта вменения «пока не находят подтверждения в международной практике в виде сформированного opinio juris государств»[40]. Более того, автор ставит под сомнение целесообразность снижения минимальной планки контроля, необходимого для вменения поведения государству, поскольку случаи применения контрмер к государству без достаточных доказательств ответственности государства за «кибероперацию» «потенциально могут служить поводом для эскалации конфликта»[41] и приходит к выводу, что при оценке стандартов вменения необходимо исходить из баланса целей: с одной стороны, обеспечения международной стабильности и суверенитета государств, а с другой стороны, обеспечения так называемой кибербезопасности[42].

Вместе с тем недостижимость на практике стандарта «эффективного контроля» при попытке привлечь государство к ответственности за неправомерное использование ИКТ побудила многих авторов к критике подхода Международного Суда и поиску альтернативных стандартов. Ф. Дельру утверждает, что в некоторых случаях степень контроля, которую ожидает увидеть Международный Суд, является слишком высоким порогом, чтобы его можно было применить к случаям использования новых технологий[43]. Ученый называет три причины, почему применение теста «эффективного контроля» не всегда может быть уместно для сферы киберпространства. Во-первых, сама природа Интернета позволяет координировать деятельность различных лиц, не осуществляя при этом значимой степени контроля над ними. Соответственно, государства способны вовлекать негосударственных субъектов в противоправную деятельность с использованием ИКТ, при этом не имея значимого контроля над ними. В результате государства могут достигать своих противоправных целей, избегая при этом юридической ответственности, поскольку координация деятельности в виртуальном пространстве не требует контроля со стороны государства, необходимого для вменения ему поведения[44].

Во-вторых, не всегда возможно проведение прямых аналогий между практикой, разработанной при рассмотрении споров, связанных с вооруженными конфликтами, и поведением в киберпространстве, где государства имеют намного больше возможностей по «обучению, снабжению, оснащению и вооружению» негосударственных акторов, начиная с предоставления вредоносных программ или рассылки инструкций пользователям и заканчивая предоставлением доступа к государственным серверным мощностям[45]. Наконец, Ф. Дельру отмечает крайнюю неразвитость взаимодействия государств в сфере использования ИКТ, что может стать критическим фактором при сборе доказательств, которые нередко находятся за пределами потерпевшего государства[46].

С. Шакелфорд предложил во всех случаях применять стандарт «общего контроля» в силу секретности, присущей «кибероперациям» и не позволяющей практически ни при каких обстоятельствах достоверно доказать «эффективный контроль» государства[47]. Соответственно, для вменения поведения государству должно быть достаточно установить операционный контроль государства при проведении «кибероперации»[48]. М. Росчини, однако, обращает внимание на то, что даже МТБЮ применяет низкий стандарт «общего контроля» только к организованным и иерархически структурированным группам[49]. Если только ИКТ не используются юридическим лицом, представляется, что потерпевшей стороне было бы крайне затруднительно доказать организованность определенной группы лиц, расположенной на территории другого государства. Кроме того, если использование ИКТ осуществляется единичными хакерами, то тест «общего контроля» не может быть применим в принципе.

В свете этого Й.-К. Вольтаг предлагает при вменении использования ИКТ государству применять тест «эффективного контроля» к физическим лицам и неорганизованным группам и по умолчанию всегда применять тест «общего контроля» к организованным и иерархически структурированным группам[50]. В ответ на предложения о применении критерия «общего контроля» к случаям использования ИКТ Х. Лахман возразил, что отсутствуют какие-либо веские причины для расщепления международного права и создания различных правил для «реального мира» и «киберпространства»[51].

Между тем некоторые авторы решили выйти за рамки спора об общем и эффективном контроле и предложили концептуально новый подход к вмене-

---

[40] *Липкина Н. Н.* Развитие концепции контроля как критерия присвоения государству поведения в киберпространстве // Вестник Саратовской государственной юридической академии. 2021. № 4(141). С. 244.

[41] Там же. С. 243.

[42] Там же. С. 244.

[43] См.: *Delerue F.* Op. cit. P. 144.

[44] Ibid. P. 145.

[45] Ibid.

[46] Ibid. P. 145—146.

[47] См.: *Shackelford S. J.* From Nuclear War to Net War: Analogizing Cyber Attacks in International Law // Berkley Journal of International Law. 2009. Vol. 25. No. 3. P. 234.

[48] Ibid.

[49] См.: *Roscini M.* Op. cit. P. 38.

[50] См.: *Woltag J.-C.* Cyber Warfare: Military Cross-Border Computer Network Operations under International Law. Cambridge, 2014. P. 92—93.

[51] См.: *Lahmann H.* Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution. Cambridge, 2020. P. 88.

нию государству использования ИКТ. Например, П. Маргулис разработал собственную sui generis концепцию «виртуального контроля», которая не основывается на традиционных критериях «общего» и «эффективного» контроля. Тест «виртуального контроля» должен учитывать сложности в определении источника «кибероперации» и реальные возможности государств по мониторингу деятельности на их территории. Кроме того, согласно этому подходу государство должно нести бремя доказывания отсутствия оснований для вменения ему «кибероперации», если оказывает поддержку негосударственному актору, стоящему за «кибероперацией»[52].

Данное предложение пока не находит отражения ни в практике, ни в opinio juris государств[53], более того, оно вызвало критику и с позиции защиты прав человека, поскольку призыв к более пристальному мониторингу деятельности в «киберпространстве» может привести к систематическому нарушению права на частную жизнь[54]. Вместе с тем согласимся с П. Маргулисом в том, что проблему вменения государству поведения негосударственных акторов, использующих ИКТ, действительно сложно решить в рамках парадигмы общего — эффективного контроля.

1.3. Анализ стандарта контроля, необходимого для вменения государству поведения негосударственных акторов, использующих ИКТ. Проблема вменения государству использования ИКТ состоит в том, что даже достижение планки «общего» контроля сложно доказуемо. Тем более нереалистичным выглядит предложение авторов Таллинского руководства 2.0, поддерживающих неукоснительное применение теста «эффективного контроля». Применение такой планки в контексте использования ИКТ равнозначно признанию, что в подавляющем большинстве случаев вменение государству поведения негосударственных акторов, использующих ИКТ, будет невозможно.

Однако критерий «эффективного контроля» не является незыблемым постулатом, отступление от которого невозможно ни при каких обстоятельствах. Во-первых, и КМП, и МТБЮ, и ряд государств справедливо отмечали, что необходимая степень контроля и руководства будет зависеть от фактов каждого отдельно взятого случая и что ст. 8 Статей об ответственности, отражающая нормы обычного права, довольно расплывчато сформулирована, допуская тем самым различные толкования степени контроля, необходимого для вменения поведения государству[55]. Следовательно, при наличии определенной специфики конкретного дела, а именно — совершении правонарушения в киберпространстве, допустимо использование менее строгих подходов к степени контроля, чем того требует тест «эффективного контроля».

Во-вторых, Международный Суд разработал критерий «эффективного контроля» при рассмотрении дел, связанных с заявлениями о нарушениях МГП и совершении геноцида, т. е. наиболее тяжких нарушений международного права. По всей видимости, тяжесть правонарушений, вменяемых государствам, оказала влияние на формирование стандарта необходимого контроля над негосударственными акторами.

В связи с этим арбитры в деле «Баяндир Инсаат Туризм против Пакистана» отмечали, что стандарты контроля, необходимые для вменения в контексте иностранного вооруженного вмешательства или установления международной уголовной ответственности, не всегда могут быть адаптированы под реалии международного экономического права и не должны препятствовать вменению поведения, если того требуют конкретные факты инвестиционного спора[56]. Исходя из той же логики, вряд ли будет разумным проводить аналогию между правилами вменения нарушений, которые могут быть совершены в киберпространстве, и нарушений, которые рассматривал Международный Суд в деле Никарагуа и деле о геноциде в Боснии.

В-третьих, как было отмечено выше, критерий «эффективного контроля» изначально был довольно произвольно «утвержден» Международным Судом без достаточного анализа практики и opinio juris[57]. Даже спустя более 35 лет после установления теста «эффективного контроля» остаются вопросы к разумности и обоснованности применения настолько строгого подхода к вменению поведения негосударственных субъектов.

Помимо этого довольно искусственным является аргумент Суда о том, что могут различаться, с одной стороны, стандарты, разработанные для вменения поведения государству, и, с другой стороны, стандарты, разработанные для квалификации вооруженного конфликта как международного. Довольно странной выглядит апелляция Международного Суда к логике, допускающей параллельное существование двух разных

---

[52] См.: *Margulies P.* Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility // Melbourne Journal of International Law. 2013. Vol. 14. P. 514—517.

[53] См.: *Липкина Н. Н.* Указ. соч. С. 243.

[54] См.: *Lahmann H.* Op. cit. P. 96—97.

[55] Комментарии КМП к Статьям об ответственности. С. 99—100. § 5, 7; Tadic case. § 117; Yearbook of the International Law Commission. Vol. II. Part One. 2001. P. 49. См. также: *Crawford J.* Op. cit. P. 147.

[56] ICSID. Bayindir Insaat Turizm Ticaret Ve Sanayi A. Ş. v. Islamic Republic of Pakistan. Case No. ARB/03/29. Award of 27 August 2009, § 130.

[57] Подробнее о методе «утверждения» как о превалирующем методе толкования международных обычаев, используемых Международным Судом, см.: *Talmon S.* Determining Customary International Law: The ICJ's Methodology between Induction, Deduction and Assertion // The European Journal of International Law. 2015. Vol. 26. No. 2. P. 434—440.

подходов к необходимой степени контроля, в то время как МТБЮ, следуя тем же принципам логики, пришел к противоположному выводу. Кроме того, своим решением Международный Суд создал нежелательную «серую зону» для ситуаций, когда государство осуществляет «общий контроль» над вооруженной группой, является стороной международного вооруженного конфликта, но в то же время «эффективного контроля» над действиями вооруженной группы не имеет и, соответственно, не может нести ответственность за совершаемые этими лицами нарушения.

В-четвертых, не стоит исключать возможности прогрессивного развития права международной ответственности. Кодификация норм обычного права в Статьях об ответственности не означает фиксацию содержания этих норм в их окончательной форме. В доктрине отмечалось, что Статьи об ответственности и их «властный тон» способствовали «окостенению» права международной ответственности, ставшего неоправданно негибким[58]. Вместе с тем Статьи об ответственности были утверждены на 53-й сессии КМП, окончившейся 10 августа 2001 г. — за месяц до теракта 11 сентября. На тот момент проблема международного терроризма (и, соответственно, негосударственных субъектов — террористических организаций) еще не стояла так остро в международной повестке. Следовательно, возникает вопрос, насколько Статьи об ответственности и выводы Международного Суда, основывающиеся, в частности, на результатах работы КМП, адекватно оценивали вызовы, стоящие перед человечеством в XXI в. — эпохе, в которой к проблеме терроризма также добавились проблемы все бóльшего распространения «гибридных войн» и все большего влияния киберпространства на «реальный мир»[59].

По причинам, указанным выше, тест «эффективного контроля» не должен и не может применяться к поведению негосударственных субъектов, использующих ИКТ. Текст ст. 8 Статей об ответственности, отражающей нормы обычного права, вполне допускает толкование термина «контроль» за рамками стандартов, установленных Международным Судом в процессе дальнейшего развития правил вменения. На текущий момент альтернативой тесту «эффективного контроля» является совместное применение с ним теста «общего контроля». Он был разработан для «традиционных» вооруженных конфликтов, однако вполне может быть применен и в контексте использования ИКТ.

2. Специальные правила вменения. Статья 55 Статей об ответственности предусматривает, что правила, обобщенные КМП, не применяются, если существуют специальные нормы международного права, определяющие условия наличия международно-противоправного деяния. Международный Суд в деле о геноциде в Боснии указывал, что отступление от правил вменения, установленных в Статьях об ответственности, допустимо только при наличии «четко выраженного lex specialis правила вменения»[60].

Не следует исключать возможность создания специальных правил вменения, которые можно применить только к поведению в киберпространстве. Исходя из требования о «четко выраженном» характере такого правила, следует считать, что специальное правило вменения поведения лиц, использующих ИКТ, должно быть отражено как минимум в каком-либо источнике международного права. В связи с этим М. Росчини допускал создание в будущем специальных правил «кибервменения»[61]. Однако возникает вопрос: как в отсутствие специального международного договора выглядит практика государств и opinio juris в части вменения вредоносного использования ИКТ другим государствам?

На практике сложился очень осторожный подход к вменению вредоносных актов использования ИКТ конкретным государствам. Этот подход характеризуется двумя основными чертами. Во-первых, публичное разоблачение организатора «кибератаки» не связывается с нарушением той или иной конкретной нормы международного права.

Так, после публичных заявлений о причастности России к кибератакам на Эстонию в 2007 г.[62], хотя позже они были опровергнуты, только с 2014 г. государства стали официально связывать вредоносные акты использования ИКТ с органами или должностными лицами конкретных государств, и в последнее время такие заявления звучат все чаще. Кроме того, тремя субъектами — США, ЕС, Великобританией — были введены односторонние принудительные меры («санкции») в отношении трех государств: Северной Кореи, России и Ирана[63].

Однако до сих пор ни одно государство официально не назвало другое ответственным за кибероперацию в качестве нарушения международного права. Формулировки, используемые для атрибуции вредоносного использования ИКТ какому-то государству, обычно выбираются крайне осторожно. Например,

---

[58] См.: *Margulies P.* Op. cit. P. 509.

[59] Доводы об уместности теста «общего контроля» для решения данных вызовов см.: *Кожеуров Я. С.* Проблемы присвоения государству поведения лиц и образований, действующих под его руководством или контролем, в практике Международного Суда ООН // Lex russica. 2009. № 5. С. 1164; *Cassese A.* Op. cit. P. 665—667; *Margulies P.* Op. cit. P. 518.

[60] Bosnian Genocide case. § 401.

[61] См.: *Roscini M.* Op. cit. P. 34.

[62] Estonian Links Moscow to Internet Attack. 18.05.2007. URL: https://www.nytimes.com/2007/05/18/world/europe/18estonia.html (дата обращения: 05.06.2024).

[63] См.: *Rusinova V., Martynova E.* Fighting Cyber Attacks with Sanctions: Digital Threats, Economic Responses // Israel Law Review. 2024. Vol. 57. Iss. 1. P. 155—156.

при осуждении «кибератак», якобы совершенных Россией против Грузии, и Грузия, и Великобритания сформулировали свое заявление как разоблачение автора атак и как осуждение такого поведения, не используя при этом терминологию права международной ответственности[64].

Хотя США и Канада призвали Россию прекратить подобное поведение, они не стали юридически квалифицировать его как нарушение международного права[65]. США, хотя и указали на Службу внешней разведки России (СВР) в одном из последних случаев введения санкций, назвали ее «исполнителем широкомасштабной кампании кибершпионажа, которая использовала платформу SolarWinds Orion и другие информационно-технологические инфраструктуры»[66]. ЕС, присоединившись к кампании осуждения, выразил свою озабоченность и озабоченность своих государств-членов по поводу кибератаки, не сказав ни слова о причастности России[67], и осторожно выразил солидарность с США по поводу последствий «кибероперации SolarWinds, которая, по оценке США, была проведена Российской Федерацией»[68].

Во-вторых, эти действия не сопровождаются раскрытием доказательств, отвечающих хотя бы одному из стандартов, которые могут быть применимы в рамках международного судебного процесса. Например, хотя Национальный центр кибербезопасности Великобритании «с высокой степенью уверенности» утверждал, что ГРУ «почти наверняка несет ответственность», что составляет «95%+», в отношении целого списка «кибероперaций»[69], доказательства причастности государства остались нераскрытыми[70]. Таким образом, «осторожное вменение» отражает режим «называть и стыдить» и даже не техническую, а политическую атрибуцию и не представляет собой юридическое вменение с целью призвать к ответственности конкретное государство.

Между тем в 2021 г. Группа правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности подчеркнула, что «указания на то, что та или иная деятельность в сфере ИКТ была начата или иным образом происходит с территории или объектов ИКТ-инфраструктуры государства», может быть недостаточно для международно-правового вменения», а «обвинения в организации и совершении противоправных деяний, выдвигаемые против государств, должны быть обоснованными»[71].

Если обратиться к составленному в 2021 г. Компендиуму, в котором 15 государств представили свои официальные позиции по вопросу применения норм международного права к использованию ИКТ[72], то становится очевидным, что большинство

[64] Statement of the Ministry of Foreign Affairs of Georgia. 20.02.2020. URL: https://mfa.gov.ge/News/Statement-of-the-Ministry-of-Foreign-Affairs-o-(7).aspx?CatID=5 (дата обращения: 05.06.2024); Foreign & Commonwealth Office. UK Condemns Russia's GRU over Georgia Cyber Attacks, press release. 20.02.2020. URL: https://www.gov.uk/government/news/uk-condemns-russias-gru-over-georgia-cyber-attacks (дата обращения: 05.06.2024);

[65] The United States Condemns Russian Cyber Attack Against the Country of Georgia. 20.02.2020. URL: https://www.state.gov/the-united-states-condemns-russian-cyber-attack-against-the-country-of-georgia/ (дата обращения: 05.06.2024); Canada Condemns Russia's Malicious Cyber-Activity Targeting Georgia. 20.02.2020. URL: https://www.canada.ca/en/global-affairs/news/2020/02/canada-condemns-russias-malicious-cyber-activity-targeting-georgia.html (дата обращения: 05.06.2024).

[66] Imposing Costs for Harmful Foreign Activities by the Russian Government. 15.04.2021. URL: https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/ (дата обращения: 05.06.2024).

[67] Declaration by the High Representative on behalf of the European Union — Call to Promote and Conduct Responsible Behavior in Cyberspace. 21.02.2020. URL: https://www.consilium.europa.eu/en/press/press-releases/2020/02/21/declaration-by-the-high-representative-on-behalf-of-the-european-union-call-to-promote-and-conduct-responsible-behaviour-in-cyberspace/ (дата обращения: 05.06.2024).

[68] Declaration by the High Representative on behalf of the European Union expressing solidarity with the United States on the impact of the SolarWinds cyber operation. 15.04.2021. URL: https://www.consilium.europa.eu/en/press/press-releases/2021/04/15/declaration-by-the-high-representative-on-behalf-of-the-european-union-expressing-solidarity-with-the-united-states-on-the-impact-of-the-solarwinds-cyber-operation/ (дата обращения: 05.06.2024).

[69] UK Exposes Russian Cyber Attacks. 04.10.2018. URL: https://www.gov.uk/government/news/uk-exposes-russian-cyber-attacks (дата обращения: 05.06.2024).

[70] Comment by the Information and Press Department on accusations against Russia of carrying out large-scale cyberattacks on Georgian websites. 20.02.2020. URL: https://www.mid.ru/en/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/4050783 (дата обращения: 05.06.2024).

[71] Доклад Группы правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности от 14 июля 2021 г. A/76/135. § 71(g).

[72] Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266. URL: https://front.un-arm.org/wp-content/uploads/2021/08/A-76-136-EN.pdf (дата обращения: 05.06.2024). P. 7 (Australia), 28 (Estonia), 39—40 (Germany), 48 (Japan), 79 (Romania), 90 (Switzerland), 117 (the UK), 141—142 (the USA).

из них, в частности Австралия, Великобритания, Румыния, США, ФРГ, Швейцария, Эстония и Япония, в целом, ратуют за применение к ИКТ обычного международного права, сложившегося в области международной ответственности государств. При этом они не конкретизировали, идет ли речь о совместном применении двух тестов: «эффективного» и «общего» контроля, или нет. Только три государства — Бразилия, Нидерланды и Норвегия — подчеркнули, что при вменении действий с использованием ИКТ должен применяться тест «эффективного контроля»[73].

Заключение. Вменение поведения на основании международно-правового обычая, отраженного в ст. 8 Статей об ответственности, представляется крайне затруднительным. Требование установить «эффективный контроль» государства над негосударственным актором, действующим в киберпространстве, на практике может привести к тому, что привлечение государства к ответственности станет невозможным. В связи с этим нормы обычного международного права допускают использование теста «общего контроля» и не исключают разработку специального теста вменения, который отражал бы специфику поведения в киберпространстве, в будущем.

Вместе с тем не следует исключать возможность появления специальных правил вменения использования ИКТ государству при условии, что такие правила будут «четко выражены» в каком-либо правовом инструменте. В отсутствие такого инструмента на основании практики государств и opinio juris можно сделать вывод о крайне осторожном подходе к вменению конкретным государствам вредоносных актов использования ИКТ.

[73] Ibid. P. 21 (Brazil), 62 (The Netherlands), 71 (Norway).

Список литературы

1. Cassese A. The Nicaragua and Tadić Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia // European Journal of International Law. 2007. Vol. 18. Iss. 4.

2. Crawford J. State Responsibility: The General Part. Cambridge, 2013.

3. Delerue F. Cyber Operations and International Law. Cambridge, 2020.

4. Koskenniemi M. What is Critical Research in International Law? Celebrating Structuralism // Leiden Journal of International Law. 2016. Vol. 29. Iss. 3.

5. Lahmann H. Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution. Cambridge, 2020.

6. Margulies P. Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility // Melbourne Journal of International Law. 2013. Vol. 14.

7. Roscini M. Cyber Operations and the Use of Force in International Law. Oxford, 2014.

8. Rusinova V., Martynova E. Fighting Cyber Attacks with Sanctions: Digital Threats, Economic Responses // Israel Law Review. 2024. Vol. 57. Iss. 1.

9. Shackelford S. J. From Nuclear War to Net War: Analogizing Cyber Attacks in International Law // Berkley Journal of International Law. 2009. Vol. 25. No. 3.

10. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations / ed. by M. N. Schmitt. Cambridge, 2017.

11. Talmon S. Determining Customary International Law: The ICJ's Methodology between Induction, Deduction and Assertion // The European Journal of International Law. 2015. Vol. 26. No. 2.

12. Woltag J.-C. Cyber Warfare: Military Cross-Border Computer Network Operations under International Law. Cambridge, 2014.

13. Кожеуров Я. С. Проблемы присвоения государству поведения лиц и образований, действующих под его руководством или контролем, в практике Международного Суда ООН // Lex russica. 2009. № 5.

14. Липкина Н. Н. Развитие концепции контроля как критерия присвоения государству поведения в киберпространстве // Вестник Саратовской государственной юридической академии. 2021. № 4(141).

15. Стрельцов А. А., Капустин А. Я., Русинова В. Н. и др. Международная безопасность в среде информационно-коммуникационных технологий. М., 2023.

References

1. Cassese A. The Nicaragua and Tadić Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia. *European Journal of International Law*, 2007, vol. 18, iss. 4, pp. 649—668.

2. Crawford J. *State Responsibility: The General Part*. Cambridge, 2013.

3. Delerue F. *Cyber Operations and International Law*. Cambridge, 2020.

4. Koskenniemi M. What is Critical Research in International Law? Celebrating Structuralism. *Leiden Journal of International Law*, 2016, vol. 29, iss. 3, pp. 727—735.

5. Lahmann H. *Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution*. Cambridge, 2020.

6. Margulies P. Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility. *Melbourne Journal of International Law*, 2013, vol. 14, pp. 496—519.

7. Roscini M. *Cyber Operations and the Use of Force in International Law*. Oxford, 2014.

8. Rusinova V., Martynova E. Fighting Cyber Attacks with Sanctions: Digital Threats, Economic Responses. *Israel Law Review*, 2024, vol. 57, iss. 1, pp. 135—174.

9. Shackelford S. J. From Nuclear War to Net War: Analogizing Cyber Attacks in International Law. *Berkley Journal of International Law*, 2009, vol. 25, no. 3, pp. 192—251.

10. Schmitt M. N. (ed.). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge, 2017.

11. Talmon S. Determining Customary International Law: The ICJ's Methodology between Induction, Deduction and Assertion. *The European Journal of International Law*, 2015, vol. 26, no. 2, pp. 417—443.

12. Woltag J.-C. *Cyber Warfare: Military Cross-Border Computer Network Operations under International Law*. Cambridge, 2014.

13. Kozheurov Ya. S. Problems of attributing to a State a conduct of persons and entities acting under its direction or control in the practice of the International Court of Justice. *Lex russica*, 2009, no. 5, pp. 1157—1164. (In Russ.)

14. Lipkina N. N. Development of the concept of control as a criterion for attributing to a State conduct in cyberspace. *Vestnik Saratovskoy gosudarstvennoy yuridicheskoy akademii*, 2021, no. 4(141), pp. 238—244. (In Russ.)

15. Streltsov A. A., Kapustin Y. Ya., Polyakova T. A. et al. *International Security in the sphere of information and communication technologies*. Moscow, 2023. (In Russ.)

Информация об авторах

В. Н. Русинова, д.ю.н., проф., руководитель департамента международного права факультета права НИУ ВШЭ, главный редактор Журнала ВШЭ по международному праву

С. П. Сушков, аспирант Аспирантской школы по праву факультета права НИУ ВШЭ

Information about the authors

V. N. Rusinova, Dr. Sci. (Law), Prof., Head of the School of International Law, Faculty of Law, HSE University; Editor-in-Chief, HSE University Journal of International Law

S. P. Sushkov, Postgraduate Student, Postgraduate School of Law, Faculty of Law, HSE University

Поступила в редакцию 14.06.2024 Received 14.06.2024
Принята к публикации 06.09.2024 Accepted 06.09.2024