Особенности гражданско-правового обеспечения кибербезопасности образовательных организаций

Г. В. Федулов
аспирант кафедры гражданско-правовых дисциплин РЭУ им. Г. В. Плеханова.
Адрес: ФГБОУ ВО «Российский экономический университет имени Г. В. Плеханова»,
117997, Москва, Стремянный пер., д. 36.
E-mail: georg-fed@rambler.ru

Peculiarities of Civil Law Provision for Cybersecurity of Educational Organizations

G. V. Fedulov
Post-Graduate Student of the Department of Civil Legal Disciplines of the PRUE.
Address: Plekhanov Russian University of Economics, 36 Stremyanny Lane,
Moscow, 117997, Russian Federation
E-mail: georg-fed@rambler.ru

Аннотация

В современный период развития процессов глобализации и цифровизации экономики российские организации, осуществляющие образовательную деятельность, несмотря на то что немалая часть таких организаций осуществляет в том числе научную деятельность, прямо не отнесены к субъектам критической информационной инфраструктуры (КИИ), что в свою очередь является определенного рода недостатком Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Особенно важным это является в связи со все большим возрастанием числа киберугроз, в том числе в отношении субъектов образовательной деятельности. Предметом исследования являются основные подходы к гражданско-правовому регулированию вопросов обеспечения кибербезопасности организаций, осуществляющих образовательную деятельность, и сотрудничающих с ними лиц прежде всего в целях безопасного использования результатов образовательных услуг. Методика исследования основана на определении и раскрытии основных правил правового обеспечения вопросов кибербезопасности в целом и образовательной среде в частности. Научную новизну исследования определяют предложенные автором гражданско-правовые подходы к локальному нормативному обеспечению кибербезопасности субъектов образовательной деятельности. В статье также проводится сравнительно-правовое исследование основополагающих нормативных правовых актов в области обеспечения безопасности ряда индустриально развитых стран мира.

Ключевые слова: гражданское право, кибербезопасность, образовательная деятельность, защита, цифровая экономика, критический, электронный, информационный, инфраструктура, компьютерные инциденты.

Abstract

In the modern period of development of the processes of globalization and digitalization of the economy, Russian organizations engaged in educational activities are not directly related to the subjects of critical information infrastructure (CII). In turn, this is a certain shortcoming of the Federal Law No. 187-ФЗ dated July 26, 2017 «On the Security of Critical Information Infrastructure of the Russian Federation». This is of particular importance due to the growing number of cyber threats, including in relation to subjects of educational activity. The subject of the research is the main approaches to civil law regulation of the issues of ensuring the cybersecurity of organizations carrying out educational activities and their collaborators, primarily in order to safely use the results of educational services. The research methodology is based on the definition and disclosure of the basic rules of legal support for cyber security issues in general and the educational environment as well. The scientific novelty of the study is determined by the civil law approaches proposed by the author to the local regulatory support of cybersecurity of the subjects of educational activities. The paper also conducts a comparative legal study of the fundamental regulatory legal acts in the field of ensuring the security of a number of industrialized countries of the world.

Keywords: civil law, cybersecurity, educational activities, protection, digital economy, critical, electronic, information, infrastructure, computer incidents.

Организации, осуществляющие образовательную деятельность (образовательные организации), согласно правилам, установленным частью 7 статьи 13, частью 3 статьи 15, подпунктом «г» пункта 1 части 2 статьи 29 Федерального закона «Об образовании в РФ», наделены правом осуществлять свою деятельность, в том числе на основании гражданско-правовых договоров соответственно об организации практики, о сетевой форме реализации образовательных программ (ОП), об образовании (о предоставлении образовательных услуг), осуществляемых за счет средств физических и (или) юрлиц и др. Указанные договоры регулируются прежде всего нормами главы 39 ГК РФ (ГК) о возмездном оказании услуг, а также иными нормативными правовыми актами.

При этом на стороны таких договоров распространяются в том числе требования, во-первых, части 1 статьи 495 ГК об обязанностях исполнителя – продавца (поставщика услуг) предоставлять заказчику – покупателю (потребителю, получателю услуг) необходимую и достоверную информацию о предоставляемой услуге и, во-вторых, статьи 736 ГК о предупреждении заказчика об условиях использования выполненной работы (другими словами, при переходе гражданских прав на их результаты).

Также необходимо отметить, что в современных условиях «перечень объектов гражданских прав значительно расширяется: теперь все то, что представляет для субъекта экономический интерес, допустимо относить к числу объектов гражданских прав, уже включающих нематериальные объекты наряду с материальными предметами» [2; 4].

Таким образом, на образовательную организацию как исполнителя гражданско-правового договора возлагаются обязанности о сообщении заказчику – получателю образовательных услуг о (обо всех) требованиях, которые в свою очередь «необходимо соблюдать для эффективного и безопасного использования результата работы [услуги], а также о возможных для самого заказчика и других лиц последствиях несоблюдения соответствующих требований» (ст. 736 ГК РФ).

В результате у исполнителя возникает обязанность предоставления, а у заказчика – право – на получение безопасной информации, в отношении которой заказчик при взаимообмене таковой информацией с исполнителем также должен обеспечивать соблюдение режима безопасности. Следуя логике законодателя, стороны договоров, используемых в деятельности образовательных организаций, являются также субъектами критической информационной инфраструктуры (КИИ), на которых распространяются нормы Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (ФЗ о КИИ).

В данной связи полагаем важным отметить, что в настоящее время организации, осуществляющие образовательную деятельность, прямо не отнесены к субъектам КИИ (несмотря на то, что немалая часть таких организаций осуществляет в том числе научную деятельность), что в свою очередь, по нашему мнению, является недостатком указанного ФЗ. Особенно это важно в современных условиях цифровизации экономики и роста киберугроз. Полагаем целесообразным дополнить пункт 8 части 1 статьи 2 ФЗ о КИИ после слов «в сфере здравоохранения», словом «образования».

Учитывая, что в 2018 г. на КИИ России было зафиксировано около 4,3 млрд кибератак, 17 тыс. из которых были признаны Национальным координационным центром по компьютерным инцидентам (НКЦКИ) наиболее опасными [1;2], несколько сотен тысяч из этих кибератак пришлось на веб-сайты организаций, осуществляющих образовательную деятельность, что в свою очередь привело к их нестабильной работе, утрате большого количества информационных данных, а в ряде случаев – к нарушению персональных данных обучаемых, их родителей (законных представителей), преподавателей, иных лиц, осуществляющих сотрудничество с образовательными организациями на условиях договоров гражданско-правового характера, в том числе юрлиц и ИП, обеспечивающих взаимодействие систем и (или) сетей КИИ (субъектов образовательной деятельности).

Сложившееся негативное положение в области обеспечения кибербезопасности объективно предопределяет необходимость выработки новых способов защиты в данной сфере, в том числе посредством выработки мер гражданско-правового регулирования, осуществляемых образовательными организациями.

Основы правового обеспечения кибербезопасности были заложены в Законе о кибербезопасности (Акт об обмене информацией о кибербезопасности) от 18 декабря 2015 г. № 114-113 (Cybersecurity Act of 2015), в соответ-

ствии с которым началось межгосударственное сотрудничество в данной сфере и который определил в качестве цели кибербезопасности защиту инфосистемы или информации, которая хранится, обрабатывается или проходит через инфосистему, от угрозы кибербезопасности или уязвимости (в системе обеспечения) безопасности.

В свою очередь под угрозой кибербезопасности понимается действие, не защищенное Первой поправкой к Конституции США, в соответствии с которой Конгресс США, а также федеральное правительство и власти штатов не вправе, во-первых, поддерживать какую-либо (какую бы то ни было) религию, либо утверждать госрелигию; во-вторых, запрещать (свободу совести) свободное вероисповедание; в-третьих, посягать на (запрещать) свободу слова и свободу прессы; в-четвертых, ограничивать (запрещать) свободу собраний и, в-пятых, ограничивать (запрещать) право народа (народонаселения США) обращаться к федеральному правительству с петициями (заявлениями) об удовлетворении жалоб в инфосистеме или с ее помощью, что в свою очередь может привести к несанкционированным действиям, неблагоприятно влиять на безопасность (принятие мер по обеспечению безопасности), доступность, конфиденциальность или целостность инфосистемы или информации, которая хранится, обрабатывается или проходит через информационную систему. При этом термин «угроза кибербезопасности» не включает каких-либо действий, которые связаны только с нарушением условий обслуживания клиентов или лицензионного соглашения.

Необходимую для описания или идентификации информацию определяют в качестве индикатора киберугроз. Сюда же отнесены, во-первых, злонамеренная разведка, в том числе аномальные схемы сообщений, которые, передаются с целью сбора технической информации, связанной с угрозой кибербезопасности или уязвимостью безопасности; во-вторых, метод преодоления контроля безопасности или эксплуатации уязвимости безопасности; в-третьих, уязвимость безопасности, включая аномальную активность, которая указывает на наличие уязвимости безопасности; в-четвертых, способ предоставления пользователю легитимного доступа к информационной системе или информации, которая хранится, обрабатывается или проходит через инфосистему, чтобы ненамеренно разрешить поражение контроля безопасности или использование уязвимости безопасности; в-пятых, злонамеренное управление и киберконтроль; в-шестых, фактический или потенциальный вред, причиненный инцидентом, включая описание информации, отфильтрованной в результате конкретной угрозы кибербезопасности и, в-седьмых, любой другой атрибут угрозы кибербезопасности, если раскрытие такого атрибута не запрещено законом, или же любая их комбинация.

Следующим межгосударственным нормативным правовым актом в области кибербезопасности явилась принятая в формате Евросоюза в Страсбурге (Французская Республика) 6 июля 2016 г. Директива Европейского Парламента и Совета ЕС 2016/1148 о мерах по достижению высокого общего уровня (обеспечения) безопасности сетевых систем и инфосистем, вступившая в силу 8 августа 2016 г.

В соответствии с указанной Директивой, прежде всего в целях разработки принципов киберкризисного сотрудничества, была создана группа по сотрудничеству, состоящая из представителей государств – членов Евросоюза, Еврокомиссии и Евроагентства по сетевой и инфобезопасности (ENISA). Основными задачами группы по киберкризисному сотрудничеству являются оказание, во-первых, поддержки и, во-вторых, содействия стратегическому партнерству и сотрудничеству государств, входящих в ЕС, осуществляемого в области обеспечения безопасности указанных систем.

При этом, согласно пункту 8 преамбулы Директивы 2016/1148, под действие которой подпадают все возможные инциденты и риски (риски кибербезопасности), в связи с чем она распространяется на операторов основных (информационных) услуг и провайдеров цифровых (диджитализированных) услуг (не распространяясь при этом на провайдеров удостоверительных сервисов в значении Еврорегламента 910/2014 Европарламента и Евросовета от 23 июля 2014 г.), подлежит обязательному применению без какого-либо «ущерба возможности для каждого государства – члена ЕС принимать необходимые меры, гарантирующие защиту интересов своей безопасности, охрану общественного порядка и общественной безопасности, а также меры, направленные на проведение расследования, раскрытия и уголовного преследования преступлений». Так, например, в соответствии со статьей 346 Договора о функционировании Евросоюза (TFEU), государства, образующие ЕС, в свою

очередь «не обязаны предоставлять информацию, раскрытие которой противоречит существенным интересам их безопасности. В данном случае значимыми являются Решение 2013/488/ЕС Совета ЕС от 23 сентября 2013 г. о правилах безопасности для защиты секретных данных в ЕС и соглашения о неразглашении или неофициальные соглашения о неразглашении, такие как протокол Traffic Light (Traffic Light Protocol), содержащий набор обозначений для маркировки конфиденциальной информации с целью указания аудитории ее дальнейшего распространения».

Национальные правовые акты в сфере обеспечения кибербезопасности, направленные на достижение общего высокого уровня безопасности сетевых систем и инфосистем, были приняты государствами – членами ЕС до 9 мая 2018 г. в соответствии с пунктом 1 статьи 25 Евродирективы 2016/1148.

Аналогичный законодательный акт был принят Конгрессом США: Закон об Агентстве по кибербезопасности и безопасности инфраструктуры (CISA, H.R.3359 – Cybersecurity and Infrastructure Security Agency Act of 2018) от 3 января 2018 г. № 115-278 вступил в силу 16 ноября 2008 г., в соответствии с которым CISA включено в инфраструктуру (находится в ведении) Министерства внутренней безопасности США. К его компетенции отнесены, во-первых, осуществление (разработка и практическая реализация) программ, операций (спецопераций) и связанной с ними политики безопасности в целом и кибербезопасности, в том числе и критически важной инфраструктуры для CISA, включая деятельность по реагированию на активность в области кибербезопасности; во-вторых, координация (своей деятельности) с федеральными органами, включая отраслевые (федеральные) агентства, и нефедеральными организациями, включая международные организации, для осуществления деятельности CISA в области кибербезопасности и критической инфраструктуры в зависимости от обстоятельств; в-третьих, координация национальных усилий по обеспечению безопасности и защите от критических инфраструктурных рисков; предоставление (по запросу) аналитических материалов, экспертиз и другой технической помощи владельцам и операторам критически важной инфраструктуры и при необходимости предоставление материалов анализа, экспертиз и другой технической помощи в координации с отраслевыми агентствами и другими федеральными департаментами и агентствами; в-четвертых, разработка и использование механизмов для активного и постоянного сотрудничества между CISA и отраслевыми агентствами для обеспечения надлежащей координации, ситуационной осведомленности и связи с отраслевыми агентствами; в-пятых, поддержание и использование механизмов регулярных и постоянных консультаций и сотрудничества между отделами CISA для дальнейшей оперативной координации, комплексной ситуационной осведомленности и улучшения интеграции в рамках CISA в соответствии с Законом о CISA; в-шестых, разработка, координация и внедрение комплексных стратегических планов деятельности CISA и оценки рисков кибербезопасности и безопасности инфраструктуры; в-седьмых, выполнение функции связи в чрезвычайных ситуациях, в-восьмых, осуществление кибербезопасности, инфраструктурной безопасности и взаимодействия с заинтересованными сторонами, а также координация такой деятельности и взаимодействие с критически важными секторальными агентствами в зависимости от ситуации.

Подобные акты были приняты и в других экономически развитых странах мира, в том числе в Республике Сингапур, где в настоящее время действует Стратегия национальной кибербезопасности 2016 (National Cybersecurity Strategy) и Акт о кибербезопасности Сингапура Cybersecurity Act 2018, CSA), устанавливающие, в том числе идентификационные процедуры информационных сетей именно как КИИ и определившие в качестве основного субъекта институционального механизма обеспечение безопасности КИИ Республики Сингапур Агентство кибербезопасности Сингапура (Cyber Security Agency of Singapore) [1. – С. 56].

Вышеперечисленные подходы нашли свое отражение в принятом в Российской Федерации ФЗ о КИИ, а также ряде иных нормативных правовых актов, в том числе приказах ФСБ России от 24 июля 2018 г. № 366 о НКЦКИ и от 24 июля 2018 г. № 368 «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными

организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения».

На основании вышеозначенных документов Российской Федерации образовательным организациям по аналогии с субъектами КИИ, учитывая, что одним из базовых (основополагающих) критериев отнесения к субъектам КИИ является деятельность в определенной сфере экономической деятельности (отрасли экономики) [3; 5], в целях защиты персональных и иных конфиденциальных данных субъектов образовательной деятельности, а также надлежащего обеспечения информационной и финансово-экономической (прежде всего, электронные платежи и информация об экономической деятельности) безопасности, эффективного противодействия неблагоприятным последствиям, вызванным рисками киберугроз, в том числе, кибератак, в рамках полномочий, определенных статьей 23 (о правовом статусе индивидуальных предпринимателей) и главой 4 ГК (о правовом статусе юрлиц), а также главой 3 ФЗ об образовании в РФ (о правовом статусе лиц, осуществляющих образовательную деятельность), целесообразно самостоятельно, руководствуясь статьей 7 ФЗ о КИИ, локальным нормативным актом, во-первых, присвоить одну из категорий значимости каждому из своих объектов КИИ; во-вторых, разрабатывать и осуществлять мероприятия по обеспечению безопасности значимых объектов КИИ и, в-третьих, незамедлительно информировать о компьютерных инцидентах ФСБ России (его территориальное подразделение).

В целях проведения категорирования приказом руководителя организации, осуществляющей образовательную деятельность, должна быть создана комиссия образовательной организации по категорированию (КООК). В состав КООК должны входить наиболее компетентные специалисты. Возглавляет комиссию руководитель образовательной организации или уполномоченное им лицо.

В процессе осуществления деятельности КООК, во-первых, определяет критические процессы и объекты уязвимости; во-вторых, формирует перечень объектов, которые могут быть отнесены к КИИ; сформированный перечень подлежащих категорированию объектов образовательная организация передает специализированной организации – субъекту КИИ (п. 8 ч. 1 ст. 2 ФЗ о КИИ) – СОКИИ, с которой у нее заключен гражданско-правовой договор на информационно-телекоммуникационное обслуживание.

В свою очередь СОКИИ в течение пяти рабочих дней после утверждения собственного перечня объектов КИИ направляет таковой во ФСТЭК (с этого момента максимальный срок категорирования составляет 1 год); во-вторых, совместно с СОКИИ оценивает масштаб возможных последствий на объекте, который может быть отнесен к КИИ, исходя из социальной значимости, экономической значимости, значимости объекта, который может быть отнесен к КИИ и др.; по согласованию с СОКИИ осуществляется присвоение каждому из таких объектов одной из категорий значимости либо принимается решение об отсутствии необходимости присвоения им одной из указанных категорий (ч. 3 ст. 7 ФЗ о КИИ). Самой высокой является первая категория, самой низкой – третья.

Согласованное с СОКИИ решение КООК оформляется актом, подписываемым руководителем КООК, и передается в СОКИИ, которая в свою очередь формирует собственный акт категорирования объекта КИИ, обобщающий такого рода решения, который подписывается членами комиссии СОКИИ и утверждается ее руководителем.

В течение 10 дней со дня утверждения акта СОКИИ обязан направить во ФСТЭК сведения (по утвержденной форме) о результатах присвоения объекту КИИ (согласованному с КООК) одной из категорий значимости (либо об отсутствии необходимости присвоения ему одной из таких категорий). ФСТЭК в течение тридцати дней осуществляет проверку сведений, полученных от СОКИИ, и вносит сведения об объекте КИИ в реестр значимых объектов КИИ, о чем в течение десяти дней уведомляет СОКИИ, которая ставит в известность о принятом ФСТЭК решении КООК в срок, установленный гражданско-правовым договором с образовательной организацией [3; 4]

Система инфобезопасности образовательной организации должна предусматривать, во-первых, установление требований к обеспечению инфобезопасности значимого объекта (киберзначимого объекта), которые включаются в реализуемое СОКИИ техзадание; во-вторых, разработку оргмер и техмер по надлежащему обеспечению инфобезопасности СОКИИ ки-

берзначимого объекта, включая разработку СОКИИ модели угроз, разработку СОКИИ техпроекта, разработку СОКИИ рабочей (эксплуатационной) документации; внедрение СОКИИ совместно с образовательной организацией оргмер и техмер по надлежащему обеспечению инфобезопасности СОКИИ киберзначимого объекта и обеспечение ввода его в действие, включая (а) установку и настройку СОКИИ средств защиты информации; (б) разработку СОКИИ совместно с КООК организационно-распорядительных документов; (в) предварительные испытания СОКИИ киберзначимого объекта и системы инфобезопасности; (г) опытную эксплуатацию СОКИИ, осуществляемую совместно с образовательной организацией киберзначимого объекта и системы инфобезопасности; (д) анализ (аналитическое исследование) уязвимостей киберзначимого объекта и принятие комплексных мер по их нивелированию (устранению); (е) приемочные (приемо-сдаточные) испытания киберзначимого объекта и подсистемы инфобезопасности; (ж) обеспечение СОКИИ инфобезопасности киберзначимого объекта в ходе его эксплуатации и при выводе его из эксплуатации.

При этом независимо от наличия киберзначимых объектов КИИ образовательная организация совместно с СОКИИ обязаны: (1) в соответствии с требованиями пункта 6 части 4 статьи 6 и пункта 1 части 2 статьи 9 ФЗ о КИИ незамедлительно информировать о компьютерных инцидентах ФСБ России и Банк России (при посягательствах на осуществление образовательной организацией электронных платежных и иных финансовых операций); (2) оказывать содействие представителям НКЦКИ, являющимся должностными лицами ФСБ России в обнаружении, предупреждении и ликвидации последствий компьютерных инцидентов (компьютерных атак), установлении причин и условий возникновения такого рода инцидентов; (3) в случае установки на объектах КИИ техсредств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных инцидентов (компьютерных атак) и реагирования на указанного рода инциденты, обеспечивать выполнение порядка, техусловий установки, эксплуатации и сохранности указанных техсредств [3; 5].

Разработку подобного рода локальных нормативных актов образовательной организации необходимо проводить в соответствии с требованиями не только административного и гражданского законодательства, но и иными требованиями, установленными в том числе нормами техрегулирования, осуществляя при этом непрерывное взаимодействие с СОКИИ. Положения вышеозначенных актов локального нормотворчества образовательная организация вправе включать в трудовые и гражданско-правовые договоры, заключаемые с работниками и иными лицами, осуществляющими сотрудничество с организациями, выполняющими образовательную деятельность.

Внедрение подобного рода подхода к обеспечению инфобезопасности в образовательных организациях, в том числе методами гражданско-правового регулирования, по нашему мнению, позволит надлежащим образом защитить права и в том числе персональные и иные конфиденциальные данные субъектов образовательной деятельности от киберугроз и существенным образом снизить риски возникновения неблагоприятных последствий, вызванных компьютерными инцидентами.

Список литературы

1. *Горян Э. В.* Институциональные механизмы обеспечения безопасности критической информационной инфраструктуры Российской Федерации и Сингапура: сравнительно-правовой аспект // Административное и муниципальное право. – 2018. – № 9. – С. 49–60.

2. *Захарова Л.* За год на Россию было совершено более четырех миллиардов кибератак // Российская газета. – 2018. – 12 декабря. – С. 1.

3. Критическая информационная инфраструктура (КИИ). – Новосибирск : Научно-технический центр «Атлас», 2019. – С. 4–5.

4. *Рожкова М. А.* Об имущественных правах на нематериальные объекты в системе абсолютных прав (часть третья – права на сведения и данные как разновидности информации) [Электронный ресурс] // Закон.ру. 2019. 14 января, с. 2. – URL: https://zakon.ru/blog/2019/1/14/ob imuschestvennyh_ pravah_na_nematerialnye_obekty_v_sisteme_absolyutnyh_prav_chast_tretya__prava_na_ (дата обращения: 18.06.2019).

5. *Талипова Л. Р.* Концептуальные основы правовой регламентации критической информационной инфраструктуры в Российской Федерации // Гуманитарные, социально-экономические и общественные науки. – 2018. – № 5. – С. 3. –URL: http://www.online-science.ru/userfiles/file/ kwlyrqx2wvdxxokgihlrfuygweabg29l.pdf (дата обращения: 18.06.2019)