ПРОБЛЕМЫ ИНФОРМАЦИОННОГО ПРАВА
PROBLEMS OF INFORMATION LAW

Научная статья
УДК/UDC 004.056
DOI: 10.21779/2224-0241-2022-44-4-154-161

Проблемы правового обеспечения кибербезопасности вузов

Р.А. Абдусаламов
Дагестанский государственный университет, г. Махачкала, Российская Федерация
Abd-rus@yandex.ru

Аннотация. В статье рассматриваются проблемы правового обеспечения кибербезопасности высших образовательных учреждений. На основе анализа состояния законодательства Российской Федерации об информационной безопасности, локальных нормативных актов высших образовательных учреждений и потенциальных угроз из цифрового пространства, выявлены проблемы правового обеспечения кибербезопасности высших образовательных учреждений.

Обосновывается влияние информационного пространства на образовательную деятельность, на безопасность электронных данных высших учебных заведений. Особый акцент делается на современном состоянии правового обеспечения кибербезопасности вузов, выявляются актуальные проблемы в данной сфере. С учетом выявленных трудностей обеспечения кибербезопасности высших учебных заведений указываются основные направления совершенствования правового регулирования в данной сфере.

Автор делает вывод, что категория «кибербезопасность» не является тождественной категории «информационная безопасность». В целях совершенствования правового обеспечения кибербезопасности вузов необходимо принять комплекс соответствующих мер правотворческого и организационного характера.

Ключевые слова: кибербезопасность, информационная безопасность, образовательные учреждения, правовое обеспечение, информационные угрозы

Для цитирования: Абдусаламов Р.А. Проблемы правового обеспечения кибербезопасности вузов // Юридический вестник ДГУ. 2022. Т. 44, № 4. С. 154–161. DOI: 10.21779/2224-0241-2022-44-4-154-161

Original article

Problems of legal provision of cybersecurity of universities

Ruslan A. Abdusalamov
Daghestan State University, Makhachkala, Russian Federation
Abd-rus@yandex.ru

Abstract. The article deals with the problems of legal provision of cybersecurity of higher educational institutions. Based on the analysis of the state of the legislation of the Russian Federation on information security, local regulations of higher educational institutions and potential threats from the digital space, the problems of legal provision of cybersecurity of higher educational institutions are identified.

The influence of the information space on educational activities, on the data security of higher educational institutions is substantiated. Special emphasis is placed on the current state of the legal provision of cybersecurity of universities, current problems in this area are identified. Taking into account the identified difficulties in ensuring cybersecurity of higher educational institutions, the main directions of improving legal regulation in this area are indicated.

The author concludes that the category “cybersecurity” is not identical to the category “information security”. In order to improve the legal provision of cybersecurity of universities, it is necessary to take the author proposed a set of appropriate measures of a law-making and organizational nature.

Key words: cybersecurity, information security, educational institutions, legal support, information threats

For citation: Abdusalamov R.A. Problems of legal provision of cybersecurity of universities. *Yuridicheskii vestnik DGU = Law Herald of DSU*, 2022, vol. 44, no. 4, pp. 154–161. DOI: 10.21779/2224-0241-2022-44-4-154-161 (In Russ.).

В эпоху развития информационных технологий и сетей термин «кибербезопасность» часто используется в различных исследованиях с позиций технических и смежных прикладных наук.

Сама по себе информационная сфера является системным фактором в жизни общества и активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации. Национальная безопасность России в значительной степени зависит от обеспечения информационной безопасности, и эта зависимость будет возрастать с технологическим прогрессом [3, с. 41].

В Доктрине информационной безопасности [4] термин информационная сфера понимается как «совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети «Интернет», сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, разработкой и использование этих технологий, обеспечение информационной безопасности, а также набор механизмов регулирования соответствующих общественных отношений».

Однако на уровне правового регулирования в официальных нормативных правовых актах содержание термина «кибербезопасность» не раскрывается. Попытка введения данного термина в отечественную правовую базу была предпринята путем разработки проекта Концепции Стратегии кибербезопасности Российской Федерации, подготовленная Временная комиссия Совета Федерации по развитию информационного общества в 2014 году.

В рамках понятийного аппарата Концепции кибербезопасность определяется как совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями. При этом под киберпространством разработчики данной Концепции предлагают понимать сферу деятельности в информационном пространстве, образованную совокупностью коммуникационных каналов Интернета и других телекоммуникационных сетей, технологической инфраструктуры, обеспечивающей их функционирование, и любых форм осуществляемой посредством их использования человеческой активности.

Нормативные правовые акты стратегического характера, принятые на высшем государственном уровне, в контексте обеспечения безопасности используют понятие «информационная безопасность». Указ Президента РФ от 02.07.2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» придает информационной безопасности статус стратегического национального приоритета. Указ Президента РФ от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» дает определение информационной безопасности как состояния защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства. С учетом того, что данные нормативные правовые акты приняты после разработки Концепции Стратегии кибербезопасности, можно констатировать, что законодатель не воспринял идеи данной Концепции и не посчитал необходимым на данном этапе внедрять кибербезопасность в качестве одного из национальных приоритетов по направлению обеспечения безопасности.

Между тем, понятие кибербезопасности, предложенное в Концепции, представляется более предпочтительным, нежели понятие информационной безопасности, благодаря четкому определению границ применения в виде пределов киберпространства с расшифровкой понятия последнего в данной Концепции, в то время как в Доктрине информационной безопасности не раскрывается понятие информационного пространства, в результате чего границы обеспечения информационной безопасности остаются неопределенными.

Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» оперирует термином «защита информации». Как видно, объектом правовой защиты выступает информация, под которой согласно ст. 2 данного закона подразумеваются сведения (сообщения, данные) независимо от формы их представления. Сразу бросается в глаза, что при такой трактовке за рамками правовой защиты остается бесперебойное функционирование устройств, обеспечивающих доступность информационной системы и сохранения контроля у реального владельца, а не у посторонних лиц.

Следовательно, вся отечественная иерархическая система правового регулирования направлена на регламентацию отношений в сфере обеспечения информационной безопасности, вынося за рамки правового регулирования кибербезопасность, феномен которой исследуется в основном на теоретическом уровне.

В.Н. Кадулин и В.Е. Клочкова настаивают на невозможности отождествления кибербезопасности с информационной безопасностью, указывая на то, что кибербезопасность необходимо рассматривать в качестве отдельного понятия, как часть более

широкого понятия – безопасность. При этом целевое предназначение кибербезопасности заключается в исследовании процессов формирования, функционирования и эволюции киберобъектов с целью выявления источников киберопасности, которые могут нанести им ущерб [1, с. 8].

Если брать за основу определение киберпространства, предложенное Концепцией Стратегии кибербезопасности, то следует констатировать, что информационные системы образовательных организаций интегрированы в систему киберпространства, а, значит, могут выступать объектом посягательства в процессе осуществления кибератаки. Таким образом, нахождение информационной системы образовательного учреждения в киберпространстве обуславливает вероятность угрозы совершения в отношении ее различных кибератак.

На сегодняшний день особую важность занимает вопрос, связанный с правовым обеспечением кибербезопасности высших учебных заведений. Главным образом это связано с внедряемыми цифровыми технологиями в образовательный процесс, необходимостью создания эффективного механизма информационной безопасности электронных данных вузов.

С.В. Исаев приводит перечень ресурсов образовательного учреждения, интегрированных в систему киберпространства: информация и программное обеспечение, материальные объекты (компьютеры, принтеры, сетевое оборудование), телекоммуникационные сервисы (официальная электронная почта, собственный интернет-сайт, информационно-справочные системы), люди, связанные с образовательным учреждением, их квалификация, умения и опыт, репутация, имидж организации и ее работников, средства на банковских счетах [2, с. 13].

С таким подходом можно согласиться лишь частично. Действительно, информация и программное обеспечение, материальные объекты, телекоммуникационные сервисы непосредственно интегрированы в систему киберпространства. Однако личности людей, связанных с образовательным учреждением, воплощенных в электронные профили, репутация, имидж образовательной организации, ее сотрудников, средства на банковских счетах являются объектом противоправного посягательства путем использования киберпространства.

Стремительная цифровизация общества приводит к быстрому развитию технологий, и, вместе с тем, появляются кардинально новые виды кибератак, к которым не готовы современные системы защиты. Для адаптации и создания механизмов противодействия всегда необходимо время, поэтому обеспечить защиту и предотвратить все атаки в полной мере не удастся. Следует рассмотреть некоторые типы кибератак, для дальнейшего анализа кибербезопасности в университете.

Распространенным примером комплексной информационной и кибератаки является распространение в различных Интернет-ресурсах недостоверной информации об отзыве лицензии на осуществление образовательной деятельности у образовательной организации высшего образования с одновременной кибератакой на электронные сервисы данной организации. В результате чего заинтересованные пользователи с целью проверки данной информации пытаются зайти на официальный сайт вуза, который оказывается недоступен, и пользователи убеждаются в «правдивости» данной информации.

После этого начинается цепная реакция: потенциальные и реальные студенты нервничают и торопятся в образовательное учреждение, где встречают сотни таких же взволнованных людей. Они возмущенно пишут об этом в социальных сетях, что вызывает только новый приток обеспокоенных заказчиков. Организаторы атаки уже могут уходить, поскольку запущенный ими процесс стал самоподдерживающимся [5, с. 118].

Среди реальных примеров кибератак на отечественные вузы можно привести атаку 20 июня 2022 года, когда в результате хакерской атаки официальные сайты вузов были перегружены в результате искусственного увеличения входящего трафика. При этом атака была проведена в период вступительной компании, которая осуществлялась и посредством приема документов абитуриентов в электронном виде через сервис «Госуслуги».

Одним из самых популярных видов, конечно, являются DDoS-атаки. DDoS-атака использует большое количество вычислительной мощности, используемой тысячами или даже миллионами устройств, чтобы преднамеренно перегрузить целевую систему или запретить, либо нарушить ее обслуживание. Эти атаки обычно осуществляются ботнетами: группой компьютеров или интеллектуальных устройств, которые были скомпрометированы вредоносным автоматизированным программным обеспечением (ботом), чтобы ими можно было управлять удаленно и без ведома владельца для выполнения какой-либо коллективной задачи от имени создателя программного обеспечения. Боты могут использоваться для кражи личных данных, мошенничества с кредитными картами, вымогательства, кибершпионажа, а также для тайного сбора и отправки целевой информации, собранной через зараженную сеть, обратно её владельцу.

Другим видом является фишинговая атака — мошеннические электронные письма, используемые для получения доступа к конфиденциальной информации или защищенным компьютерным системам. Они убеждают пользователей переходить по вредоносным ссылкам, загружать вложения или предоставлять конфиденциальную информацию, например, имена пользователей и пароли.

Следующими можно выделить brute-force атаки. При этом виде атак некоторые злоумышленники используют приложения и скрипты для перебора множества комбинаций паролей, чтобы обойти процессы аутентификации. При простом пароле программа быстро подберёт нужную комбинацию, поэтому использование хорошего менеджера паролей является неотъемлемой частью защиты от киберугроз.

Также необходимо упомянуть атаки внутреннего типа. Имеется в виду, что на систему защиты влияет сотрудник организации или человек, который имеет непосредственный доступ к ней. Такие атаки могут производиться как намеренно, со злым умыслом, чтобы навредить организации, так и по ошибке одного или нескольких сотрудников. Нередки случаи, когда бывший сотрудник корпорации публиковал в общий доступ базы данных своей прошлой организации для достижения личных целей и подрыва репутации компании. Также взломы системы часто происходят и из-за халатности и некомпетентности сотрудников предприятия. Поэтому своевременное консультирование персонала лицами, отвечающими за кибербезопасность, также является очень важным критерием.

Основные виды вреда киберугроз можно классифицировать следующим образом: физический (то есть вред, оказывающий физическое или цифровое негативное воздействие на кого-либо, или что-то); экономический (то есть вред, связанный с негативными финансовыми или экономическими последствиями); психологический (то есть вред, который сосредоточен на человеке и его психическом благополучии и психике); ущерб репутации (то есть вред, относящийся к общему мнению о компании).

Физический или цифровой ущерб является одним из наиболее известных видов вреда для организаций, и его примерами являются: поврежденные или недоступные системы; поврежденные файлы данных; кража конфиденциальных или клиентских данных; и телесные повреждения сотрудников или клиентов. Примерами же экономического вреда могут быть: сокращение клиентов; снижение прибыли и роста; падение цены акций; кража финансов. Психологический тип киберущерба направлен непосредственно на моральное состояние отдельного человека или группы лиц, примерами этого типа могут послужить: чувство расстройства, депрессия или беспокойство; нервозность, которую испытывают стороны организации. Наконец, репутационный тип оказывает мощнейшее пагубное влияние на статусность и престижность учреждения, примерами такого ущерба являются: поврежденное общественное восприятие; снижение деловой репутации; негативное изменение шансов на расширение и рост организации.

Безопасность должна осуществляться не только на техническом уровне, но и на информационном. Создание удобной политики безопасности, которой будет следовать весь персонал и его своевременное обучение основным аспектам работы с данными является такой же важной частью, как и правильно подобранное программное обеспечение и система защиты. Корректность построения сети, а также правильная реализация в ней системы безопасности является основой, на которую затем наслаиваются технические и организационные инструменты. Плохо спроектированные системы чаще попадают в зону риска киберугроз, так как даже если система обладает обширными вспомогательными системами защиты, они всё равно не смогут закрыть все её уязвимости.

Вместе с тем, вспомогательные инструменты защиты играют важную роль в системе безопасности, их можно разделить на две основные категории: технические средства и организационные меры.

В свою очередь, технические средства также делятся на множество подкатегорий для узкоспециализированной работы. Организационные меры являются информационным уровнем безопасности, о важности которого в этой статье упоминалось выше. К таким мерам можно отнести: регулярное проведение обучения сотрудников основам информационной безопасности, разграничение между ними прав и ролей, чтобы рядовой сотрудник не имел доступ к самым конфиденциальным данным учреждения, а также частная стандартизация и сертификация устройств и программного обеспечения. Техническими средствами защиты могут послужить различные устройства или программное обеспечение.

К устройствам относятся различные межсетевые экраны, которые проводят мониторинг входящего и исходящего сетевого трафика на подозрительную активность. К программному обеспечению же относят многообразные протоколы, системы шифрования и резервирования.

Так, технические средства можно разбить на следующие типы инструментов: для мониторинга сетевой безопасности, для сканирования уязвимостей системы и сети, для аудита паролей и для шифрования. Стоит подробнее описать шифрование, это механизм, ограждающий пользователя от лишнего сетевого трафика, чтобы его было невозможно отследить. Шифрование обеспечивает конфиденциальность сотрудника организации в сети путём переадресации запросов на разных прокси-серверах.

Из-за растущей зависимости от цифровых технологий современные организации в целом и образовательные учреждения в частности уязвимы для воздействия технических сбоев и человеческих ошибок, которые приводят к атакам со стороны киберпреступников. Киберпреступники, мотивированные финансовой выгодой, представляют наиболее очевидную и постоянную угрозу для разного рода учреждений.

Дело в том, что множество ведущих университетов напрямую взаимодействует с развивающимися компаниями и правительственными учреждениями. Соответственно между ними происходит обмен конфиденциальной информацией, получив которую злоумышленники могут нанести огромный репутационный риск с негативными финансовыми или экономическими последствиями. Чаще всего именно такое стремление преследуют злоумышленники при совершении целевой атаки, так как большая часть персональной информации о студентах уже есть в открытом доступе на порталах заведения или в других источниках. Стоит также отметить, что подобного рода атаки, а также атаки масштабного характера проводятся чаще всего именно на известные университеты, которые непосредственно и сотрудничают с крупными организациями. Как правило, такие университеты инвестируют достаточно много ресурсов в инфраструктуру кибербезопасности, поэтому более рядовые атаки для подобных учреждений проходят незаметно.

Поскольку существует вероятность потери целостности, доступности и конфиденциальности информации вузов из-за наличия разнообразных угроз, она должна быть должным образом защищена. Фактически ежедневно учебные заведения сталкиваются с событиями, которые могут стать угрозами для информационной сферы, такие как:

1) незаконное присвоение чужого имущества;

2) кража имущества (информационного оборудования, компонентов);

3) подделка данных, несанкционированное изменение;

4) нарушение прав частной собственности и конфиденциальности информации;

5) несанкционированный доступ или злоупотребление правами;

6) вымогательство или шантаж с использованием компьютеров;

7) несанкционированный доступ;

8) злонамеренное искажение или уничтожение данных;

9) нарушение авторских прав или прав интеллектуальной собственности и т.д.

Таким образом, информационная безопасность – это, по сути, не конкретная цель и не конечное состояние безопасности данных, а, скорее, процесс обеспечения конфиденциальности, целостности и доступности информации. Доступность означает предоставление доступа к информации и связанным с ней ресурсам авторизованным пользователям по мере необходимости [6, с. 187].

Основной задачей информационной безопасности вузов является минимизация и предотвращение рисков и угроз, а не устранение последствий. Именно принятие превентивных мер для обеспечения конфиденциальности, целостности и доступности информации является наиболее эффективным подходом при создании системы информационной безопасности.

При этом следует исходить из того, что объекты информационной безопасности – это то, на что направлены негативные действия, которые наносят ущерб, и действия, которые предотвращают первое. Объектами, на которых сосредоточены негативные последствия в информационной сфере, являются:

1) все типы источников информации – информация, записанная на материальном носителе с деталями, позволяющими их идентифицировать;

2) система создания, распространения и использования информации (информационные системы и технологии, средства массовой информации, библиотеки, архивы, персонал, нормативные документы и так далее).

Под субъектами информационных отношений понимаются как владельцы, так и пользователи информации и поддерживающей инфраструктуры.

В целях регулирования поведения субъектов информационной сферы существует ряд нормативных правовых актов для реализации прав и обязанностей, которые направлены на обеспечение защиты объектов правоотношений. Здесь законодатель вводит ограничения на информационные права и свободы в целях защиты интересов граждан, общества и государства. Методы гражданского, административного и конституционного права используются при формировании правовых норм, установлении прав и обязанностей.

В связи с активным распространением информационных технологий в учебных заведениях увеличивается рост и мошеннических действий в сфере цифровых технологий. Безусловно, что в качестве последствий могут выступать как потеря данных, так и получение доступа к таким данным мошенниками, которые в последующем могут ими распорядиться по своему усмотрению [7, с. 137]. В свою очередь, это может привести к нарушению режима обработки и персональных данных.

В данном контексте уместно отметить, что перечень информации, которая может быть признана персональной, не закреплен в действующем законодательстве исчерпывающим образом. Иными словами, это может быть абсолютно любая информация, которая будет позволять идентифицировать, например, преподавателя или студента (его номер телефона, паспортные данные, электронная почта, личная страница в сети Интернет и т.д.) [8, с. 100]. Такое перечисление может быть безграничным, особенно в нынешних условиях, когда внедряются во все сферы жизни общества информационно-телекоммуникационные средства связи, в т.ч. и в сферу оказания образовательных услуг. Все это накладывает отпечаток и на расширение информации, которая будет признаваться персональной.

Фактически можно говорить о том, что на сегодняшний день происходят кардинальные изменения в сфере информационных технологий и смещение приоритетов в сторону киберпространства. Компьютерные технологии и Интернет активно используются для реализации образовательных целей. Кроме того, приобретается транснациональный характер киберпространства [9, с. 13], в котором участники имеют возможность угрожать информационным системам различных стран из любой точки мира, в результате для борьбы с ними необходимо высокоэффективное международное сотрудничество. Имеет место быть расширение киберпреступности, кибертерроризма и киберэкстремизма [10, с. 273].

Таким образом, роль информационной безопасности в наше время очень велика, поскольку в век компьютеризации большая часть информации хранится и передается с использованием информационных систем, а значит, необходимо постоянно совершенствовать различные механизмы для поддержания информационной безопасности высших учебных заведений на высоком уровне.

Проведенный анализ позволяет говорить о том, что внедрение цифровых технологий на сегодняшний день фактически посягает на безопасность образовательных учреждений (их данных).

На наш взгляд, для обеспечения защиты информационных ресурсов возникает необходимость разработки политики информационной безопасности, включающей в себя обязательные требования к защите информационных ресурсов и информации, распространение и предоставление которых ограничено, а также требования к контролю за обеспечением безопасности и защиты информационных ресурсов.

Представляется, что это позволит частично решить проблему, связанную с кибербезопасностью высших учебных заведений. Более того, особый акцент со стороны законодателя должен быть сделан и на совершенствовании правового регулирования в аспекте установления мер, которые будут способствовать созданию безопасных условий для осуществления образовательной деятельности.

Нормативные правовые акты, регулирующие деятельность образовательных организаций высшего образования, в частности, Федеральный закон от 29.12.2012 г. № 273-ФЗ «Об образовании в Российской Федерации», подзаконные акты Правительства РФ и Минобрнауки не закрепляют специальных положений, направленных на обеспечение информационной безопасности и кибербезопасности.

Более того, в целом в контексте обеспечения кибербезопасности как пример нормы, регулирующей данные отношения, можно привести только положение пп. 4 п. 4 ст. 16 Федерального закона от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», которое закрепляет обязанность обладателя информации, оператора информационной системы обеспечить недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование.

Анализ уставов образовательных организаций также позволяет констатировать отсутствие специальных правовых норм, направленных на обеспечение информационной безопасности и кибербезопасности. Например, Устав Московского государственного университета имени М.В. Ломоносова, утвержденный Постановлением Правительства РФ от 28.03.2008 г. № 223, содержит только указание на то, что университет обеспечивает защиту сведений, составляющих государственную тайну, и иной охраняемой законом информации.

На уровне локального регулирования отдельные образовательные организации высшего профессионального образования принимают собственные отдельные положения об информационной безопасности либо включают разделы об информационной безопасности в положение о комплексной безопасности образовательной организации.

Так, Положение о политике информационной безопасности Самарского государственного медицинского университета закрепляет только общие положения об информационной безопасности, заимствованные из Федерального закона от 27.07.2006 г. № 149-ФЗ. Отсутствует перечень должностных лиц, ответственных за обеспечение информационной безопасности, перечень технических устройств, интегрированных в систему цифрового пространства и подлежащих защите от противоправных посягательств. Положение о службе комплексной безопасности Тверского государственного университета от 22.03.2020 г. содержит только положение о том, что специалист по информационной безопасности входит в состав службы комплексной безопасности. Не определены задачи, функции специалиста по информационной безопасности, необходимый уровень его профессиональных компетенций. Кроме того, наличие специалиста по информационной безопасности только в единственном числе приводит к отсутствию в образовательном учреждении специалистов по информационной безопасности в период его болезни или отпуска, а временное возложение его обязанностей на иных сотрудников образовательного учреждения, не обладающих какой-либо профессиональной компетенцией в данной сфере, что усилит уязвимость ресурсов образовательного учреждения, интегрированных в цифровое пространство.

Таким образом, можно констатировать, что современное состояние правового регулирования в сфере обеспечения кибербезопасности образовательных организаций высшего профессионального образования, как на федеральном уровне, так и на уровне локального нормативного регулирования в конкретных образовательных организациях, не соответствует уровню потенциальных и реальных угроз. Акцентирование внимания исключительно

на вопросах информационной безопасности выводит за рамки правового регулирования кибербезопасность, которая по своим сущностным признакам не является тождественным и взаимозаменяемым понятием с информационной безопасностью.

Это обуславливает необходимость внедрения основ обеспечения кибербезопасности в отечественную правовую систему, как на стратегическом доктринальном, так и на уровне законодательного, подзаконного и локального регулирования. При этом необходимо создать основы специального правового регулирования кибербезопасности в целях разграничения с нормами, регулирующими информационную безопасность.

В целях совершенствования правового обеспечения кибербезопасности вузов необходимо предпринять следующие меры правового и организационного характера:

- ввести в понятийно-терминологический аппарат Федерального закона от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» дефиниции «кибербезопасность» и «киберпространство» с учетом достижений Концепции Стратегии кибербезопасности 2014 года;

- ввести в Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» отдельную статью, посвященную правилам обеспечения кибербезопасности;

- внести в Федеральный закон от 29.12.2012 г. № 273-ФЗ «Об образовании в Российской Федерации» изменения, в соответствии с которыми возложить на образовательные организации обязанность надлежащего обеспечения кибербезопасности;

- ввести в штатные структуры образовательных организаций высшего образования должности специалистов по кибербезопасности либо обязать заключать договоры на обслуживание информационных ресурсов и технических устройств, интегрированных в систему цифрового пространства, с сертифицированными организациями в сфере обеспечения кибербезопасности.

Список источников

1. *Толепбаев Б.Б.* Эффективность и кибербезопасность систем дистанционного обучения вузов // Российская наука в современном мире. 2022. С. 73–75.

2. *Олейник А.С., Герасимов В.М.* Технология обеспечения информационной и кибербезопасности в учреждениях высшего образования // Управление образованием: теория и практика. 2022. № 5 (51). С. 240–247.

3. *Дубень А.К.* Информационная безопасность как составная часть национальной безопасности Российской Федерации // The Scientific Heritage. 2021. № 74-4(74). С. 41–45.

4. Об утверждении Доктрины информационной безопасности Российской Федерации // Собрание законодательства Рос. Федерации. 2016. № 50. Ст. 7074.

5. *Наскидашвили К.А.* Информационная безопасность. Виды угроз информационной безопасности // Вестник студенческого научного общества ГОУ ВПО "Донецкий национальный университет". 2020. Т. 1. № 12. С. 187–189.

6. *Юмашева Т.А.* Правовые акты в сфере информационной безопасности как один из важнейших источников информационной безопасности РФ // Актуальные проблемы безопасности жизнедеятельности в образовании. 2022. С. 266–269.

7. *Болдырев А.Н.* Информационная безопасность. Виды угроз информационной безопасности // Современные тенденции развития гуманитарных, правовых и экономических исследований Республики Калмыкия: теория и практика. 2021. С. 137–140.

8. *Итинсон К.С., Чиркова В.М.* Обеспечение кибербезопасности в образовательных учреждениях: осведомленность, правила, стратегия // Балтийский гуманитарный журнал. 2021. Т. 10. № 4(37). С. 99–102.

9. Коммуникации в киберпространстве: тенденции цифровой эпохи / С.Ю. Нарциссова, С.В. Куликова, Е. В. Маклакова [и др.]. Москва: Издательский Дом "Инфра-М", 2020. 254 с.

10. *Давыдов В.Н.* Информационная безопасность образовательного пространства // Профилактика проявлений экстремизма и терроризма как фактор обеспечения социальной безопасности в современной России. 2017. С. 263–280.

References

1. *Tolepbaev B.B.* Efficiency and cybersecurity of distance learning systems of universities [Effektivnost' i kiberbezopasnost' sistem distantsionnogo obucheniya vuzov], *Rossiiskaya nauka v sovremennom mire (Russian Science in the Modern World)*, 2022, pp. 73-75. (In Russ.).

2. *Oleinik A.S., Gerasimov V.M.* Information and cybersecurity technology in higher education institutions [Tekhnologiya obespecheniya informatsionnoi i kiberbezopasnosti v uchrezhdeniyakh vysshego obrazovaniya], *Upravlenie obrazovaniem: teoriya i praktika (Education management: theory and practice*), 2022, no. 5(51), pp. 240-247. (In Russ.).

3. *Duben' A.K.* Information security as an integral part of the National security of the Russian Federation [Informatsionnaya bezopasnost' kak sostavnaya chast' natsional'noi bezopasnosti Rossiiskoi Federatsii], *Upravlenie obrazovaniem: teoriya i praktika (The Scientific Heritage),* 2021, no. 74-4(74), pp. 41-45. (In Russ.).

4. Ob utverzhdenii Doktriny informatsionnoi bezopasnosti Rossiiskoi Federatsii» [On Approval of the Information Security Doctrine of the Russian Federation]: Decree of the President of the Russian Federation no. 646 dated 05/12/2016, *Sobranie zakonodatel'stva Rossiiskoi Federatsii (Collection of legislation of the Russian Federation*), 2016, no. 50, st. 7074. (In Russ.).

5. *Naskidashvili K.A.* Information security. Types of information security threats [Informatsionnaya bezopasnost'. Vidy ugroz informatsionnoi bezopasnosti], *Vestnik studencheskogo nauchnogo obshchestva GOU VPO "Donetskii natsional'nyi universitet" (Bulletin of the Student Scientific Society of the Donetsk National University*), 2020, vol. 1, no. 12, pp. 187-189. (In Russ.).

6. *Yumasheva T.A.* Legal acts in the field of information security as one of the most important sources of information security of the Russian Federation [Pravovye akty v sfere informatsionnoi bezopasnosti kak odin iz vazhneishikh istochnikov informatsionnoi bezopasnosti RF], *Aktual'nye problemy bezopasnosti zhiznedeyatel'nosti v obrazovanii (Actual problems of life safety in education)*, 2022, pp. 266–269. (In Russ.).

7. *Boldyrev A.N*. Information security. Types of information security threats [Informatsionnaya bezopasnost'. Vidy ugroz informatsionnoi bezopasnosti], *Sovremennye tendentsii razvitiya gumanitarnykh, pravovykh i ekonomicheskikh issledovanii Respubliki Kalmykiya: teoriya i praktika. (Modern trends in the development of humanitarian, legal and economic research of the Republic of Kalmykia*: *theory and practice*), 2021, pp. 137-140. (In Russ.).

8. *Itinson K.S., Chirkova V.M.* Ensuring cybersecurity in educational institutions: awareness, rules, strategy [Obespechenie kiberbezopasnosti v obrazovatel'nykh uchrezhdeniyakh: osvedomlennost', pravila, strategiya], Baltiiskii gumanitarnyi zhurnal (Baltic Humanitarian Journal, 2021), 2021, vol. 10, no. 4(37), pp. 99-102. (In Russ.).

9. *Narcissova S. Ju., Kulikova S. V., Maklakova E. V. [i dr.]* Kommunikacii v kiberprostranstve: tendencii cifrovoj jepohi [Communications in cyberspace: trends of the digital age]. Moscow: Infra-M Publishing House, 2020. 254 p. (In Russ.).

10. *Davydov V.N*. Information security of the educational space [Informatsionnaya bezopasnost' obrazovatel'nogo prostranstva], *Profilaktika proyavlenii ekstremizma i terrorizma kak faktor obespecheniya sotsial'noi bezopasnosti v sovremennoi Rossii [Prevention of manifestations of extremism and terrorism as a factor of ensuring social security in modern Russia*], 2017, pp. 263-80. (In Russ.).

ИНФОРМАЦИЯ ОБ АВТОРЕ

Абдусаламов Руслан Абдусаламович, заведующий кафедрой информационного права и информатики юридического института Дагестанского государственного университета, кандидат педагогических наук, доцент, г. Махачкала, Российская Федерация. *E-mail: Abd-rus@yandex.ru*

INFORMATION ABOUT THE AUTHOR

Abdusalamov Ruslan Abdusalamov, Head of the Department of Information Law and Informatics of the Law Institute of Dagestan State University, Candidate of Pedagogical Sciences, Associate Professor, Makhachkala, Russian Federation. *E-mail: Abd-rus@yandex.ru*

Поступила в редакцию 30.10.2022 г.; одобрена после рецензирования 18.11.2022 г.; принята к публикации 28.11.2022 г.

Received 30.10.2022; approved after reviewing 18.11.2022; accepted for publication 28.11.2022.