УДК 342.9

АКТУАЛЬНЫЕ ПРОБЛЕМЫ В ОБЛАСТИ ПРАВОВОГО РЕГУЛИРОВАНИЯ ОНЛАЙН-КУРСОВ

А. А. ГОНЧАРОВА
(Представлено: К. Д. САВИЦКАЯ)

В последние годы онлайн-образование стремительно развивается, что обусловлено как технологическими изменениями, так и изменением потребностей общества. Однако существующее законодательство в области онлайн-курсов во многих странах сталкивается с рядом актуальных проблем и недостатков. Данная научная работа посвящена анализу текущей правовой базы, регламентирующей онлайн-образование, и выявлению ключевых недостатков, мешающих эффективному развитию этой сферы.

Защита персональных данных и конфиденциальность информации участников онлайн-курсов является одним из ключевых аспектов правового регулирования в этой сфере. Учитывая специфику онлайн-обучения, когда значительная часть взаимодействия между студентами и образовательными организациями происходит в цифровой среде, вопросы обеспечения конфиденциальности персональных данных приобретают особую важность.

Нормативно-правовое регулирование в этой области призвано гарантировать, что персональная информация студентов, включая их контактные данные, учебные достижения, финансовую информацию и другие сведения личного характера, надежно защищена от несанкционированного доступа, использования, раскрытия или модификации. Образовательные организации, предлагающие онлайн-курсы, обязаны разрабатывать и внедрять политику и процедуры, соответствующие действующему законодательству о защите персональных данных [1].

Это включает в себя меры по безопасному хранению данных, ограничение доступа к ним только уполномоченным лицам, использование современных криптографических методов, регулярное обновление систем информационной безопасности. Кроме того, студенты должны быть в полной мере информированы о том, как их персональные данные будут собираться, обрабатываться и использоваться в рамках онлайн-образования, а также должны иметь возможность контролировать и при необходимости корректировать свою информацию.

Студенты, участвующие в онлайн-курсах, должны иметь возможность контролировать и при необходимости корректировать свою персональную информацию. Это важное право, которое обеспечивается действующим законодательством о защите персональных данных.

Прежде всего, образовательные организации, предлагающие онлайн-курсы, обязаны предоставлять студентам полную информацию о том, какие персональные данные они собирают, с какой целью и каким образом будут их использовать. Эта информация должна быть доступна в понятной и прозрачной форме, например, в виде политики конфиденциальности или условий использования платформы.

Студенты должны иметь возможность в любое время ознакомиться со своими персональными данными, хранящимися у образовательной организа ции. Как правило, для этого предусматриваются личные кабинеты или аккаунты студентов, через которые они могут просматривать, а внекоторых случаях и редактировать, свои контактные данные, успеваемость, финансовую информацию и другие сведения.

Если студент обнаруживает ошибки или неточности в своих данных, он должен иметь возможность подать запрос на их исправление. Образовательная организация, в свою очередь, обязана оперативно рассмотреть такой запрос и внести необходимые изменения.

Кроме того, студенты должны иметь право отозвать свое согласие на обработку персональных данных или ограничить их использование в определенных целях. Это особенно актуально в случаях, когда персональная информация используется в маркетинговых или рекламных целях.

Нарушение установленных норм в области защиты персональных данных может повлечь за собой серьезные юридические и финансовые последствия для образовательных организаций, предоставляющих онлайн-курсы. Поэтому обеспечение конфиденциальности информации участников онлайн-обучения является одним из основополагающих принципов, на которых должна строиться вся система правового регулирования в сфере цифрового образования.

Образовательные организации, предлагающие онлайн-курсы, должны внедрять комплексные меры безопасности для защиты персональных данных студентов:

– Надежное шифрование данных. Все персональные данные студентов, включая информацию об успеваемости, финансовые сведения и контактные данные, должны храниться и передаваться с использованием современных криптографических методов, таких как AES, RSA или SSL/TLS. Это гарантирует, что данные будут защищены от несанкционированного доступа даже в случае взлома систем.

– Контроль доступа. Доступ к персональным данным студентов должен быть строго ограничен только уполномоченными сотрудниками организации. Для этого должны применяться системы идентификации и аутентификации пользователей, многофакторная аутентификация, а также регулярный мониторинг и аудит действий с данными. Это позволит отслеживать все операции с персональными данными и предотвращать несанкционированный доступ.

– Резервное копирование и восстановление. Образовательные организации должны регулярно создавать резервные копии всех персональных данных студентов и обеспечивать возможность их оперативного восстановления в случае непредвиденных ситуаций, таких как сбои в работе системы или кибератаки. Это позволит быстро восстановить данные и обеспечить непрерывность учебного процесса.

– Физическая безопасность. Помещения, в которых хранятся персональные данные студентов, должны быть оборудованы системами видеонаблюдения, контроля доступа и другими мерами физической защиты. Это исключит возможность несанкционированного физического доступа к данным.

– Обучение персонала. Сотрудники организации, имеющие доступ к персональным данным студентов, должны проходить регулярное обучение по вопросам информационной безопасности, соблюдения конфиденциальности и правилам работы с персональными данными. Это повысит уровень осведомленности сотрудников и снизит риск человеческих ошибок.

– Аудит и соответствие нормативным требованиям. Образовательные организации должны регулярно проводить аудит систем защиты персональных данных, а также обеспечивать соответствие их политик и процедур действующему законодательству о защите персональных данных. Это гарантирует, что все меры безопасности соответствуют требованиям регуляторов и обеспечивают надлежащую защиту персональных данных.

Применение этих комплексных мер безопасности позволит образовательным организациям надежно защитить персональные данные студентов, участвующих в онлайн-курсах, и минимизировать риски их утечки или неправомерного использования.

Вопрос интеллектуальной собственности и авторских прав в сфере онлайн-образования является очень важным и многогранным. Лекции, видео, презентации, тесты и другие материалы, разработанные преподавателями, являются объектами авторских прав. Организация-разработчик онлайн-курса должна обеспечить надлежащее оформление авторских прав на весь контент. Студентам, проходящим онлайн-курс, предоставляется ограниченная лицензия на использование контента в образовательных целях, но не на его распространение или коммерческое использование. Организация должна иметь процедуры для урегулирования вопросов авторских прав при использовании внешних материалов в курсе [2].

Преподаватели, создающие контент для онлайн-курсов, сохраняют права на свои интеллектуальные разработки. Организация-разработчик должна заключать с преподавателями четкие договоры, определяющие условия использования их интеллектуальной собственности. Преподаватели должны иметь право на часть доходов от коммерческого использования их разработок.

Организация должна применять технические меры защиты контента от нелегального копирования или распространения, такие как DRM, водяные знаки и ограничения скачивания. Необходимо вести мониторинг использования контента онлайн-курсов и оперативно реагировать на случаи нарушения авторских прав. В договорах со студентами должны быть четко прописаны условия использования контента и запреты на его неправомерное распространение.

Некоторые организации предоставляют открытый доступ к своим онлайн-курсам на условиях открытых лицензий (CreativeCommons и др.). Это позволяет свободно использовать и адаптировать контент в некоммерческих образовательных целях при соблюдении условий лицензии.

Для онлайн-курсов могут использоваться различные типы лицензий, в зависимости от целей и бизнес-модели организации:

– Коммерческие или проприетарные лицензии:

1. Лицензии на использование всего курса или отдельных компонентов (видео, тесты и пр.)
2. Подписные модели доступа к курсу на определенный срок
3. Разовая оплата полного доступа к курсу

– Открытые лицензии:

1. CreativeCommons (CC-BY, CC-BY-SA, CC-BY-NC и др.) - позволяют свободное использование, адаптацию и распространение в некоммерческих целях
2. GNU FreeDocumentationLicense - лицензия для открытых образовательных ресурсов
3. OpenCourseWare - лицензия MIT для свободного использования учебных материалов

– Смешанные модели:

1. Базовый открытый доступ к части курса, расширенный платный доступ
2. Открытый доступ к части контента, платный доступ к дополнительным материалам
3. Бесплатный доступ для индивидуальных пользователей, платный для организаций

Выбор лицензии зависит от целей онлайн-курса, бизнес-модели, целевой аудитории и прочих факторов. Организации должны тщательно прорабатывать вопросы интеллектуальной собственности на этапе разработки курса [3].

Комплексное и грамотное управление вопросами интеллектуальной собственности и авторских прав является ключевым фактором успешного развития онлайн-образования, защиты прав всех участников и обеспечения устойчивости бизнес-моделей образовательных организаций.

Для защиты авторских прав на материалы онлайн-курсов могут применяться различные технические меры. Например, системы управления цифровыми правами (DRM) могут ограничивать возможность скачивания, копирования и печати материалов курса, привязывать доступ к курсу к аутентификации пользователя, а также отслеживать и ограничивать количество устройств, с которых осуществляется доступ. Водяные знаки (Watermarking) позволяют встраивать невидимые или скрытые метки в видео, изображения и документы, что помогает отслеживать источник утечек при нелегальном распространении. Также могут использоваться меры по ограничению экспортируемости контента, такие как запрет на скачивание и сохранение материалов курса, а доступ возможен только в онлайн-режиме. Регулярный мониторинг интернета с использованием сервисов поиска и отслеживания использования контента онлайн также может помочь своевременно реагировать на случаи незаконного распространения. Шифрование и хэширование файлов, в том числе применение криптографических методов и использование хэшей для аутентификации целостности файлов, также являются эффективными техническими мерами защиты. Наконец, ограничение возможности копирования, например, за счет технического ограничения функций копирования, вырезания и скриншотов в среде просмотра контента, может быть полезным. Выбор конкретных технических мер зависит от бизнес-модели, ценности контента, рисков, доступных ресурсов организации и других факторов. Важно находить баланс между защитой авторских прав и удобством пользовательского опыта [4].

Для совершенствования правового регулирования онлайн-курсов и борьбы с пиратством и незаконным распространением авторских материалов можно рассмотреть следующие меры и рекомендации:

– Обновление законодательства: Государства должны провести анализ своего законодательства и, при необходимости, внести изменения, чтобы оно отражало современные вызовы онлайн-образования. Это может включать расширение определения пиратства и незаконного распространения авторских материалов, а также ужесточение наказаний.

– Лицензирование и контроль: Провайдеры онлайн-курсов должны активно работать с правообладателями для установления лицензионных соглашений и контроля за использованием авторских материалов. Они должны также использовать технические решения, такие как цифровые отпечатки и системы управления авторскими правами, для обнаружения и предотвращения незаконного распространения.

– Обучение и информирование: Провайдеры онлайн-курсов должны предоставлять обучение и информацию участникам о правилах использования авторских материалов и последствиях нарушений. Это поможет повысить осведомленность и этическое поведение студентов.

– Разработка технологических решений: Технологические инновации могут сыграть важную роль в предотвращении пиратства и незаконного распространения. Разработка и использование эффективных технических решений, таких как системы DRM (DigitalRightsManagement), могут помочь защитить авторские материалы и предотвратить их несанкционированное распространение.

– Сотрудничество со сторонними организациями: Провайдеры онлайн-курсов могут сотрудничать с правообладателями, ассоциациями, профессиональными организациями и другими заинтересованными сторонами для разработки и реализации совместных программ и инициатив по борьбе с пиратством и незаконным распространением.

Эти меры должны быть реализованы в сочетании с общим осведомлением и образованием пользователей, чтобы создать этическую среду онлайн-образования и защитить права авторов и правообладателей.

ЛИТЕРАТУРА

1. О защите персональных данных : Закон Респ. Беларусь : 7 мая 2021 г. № 99-З: принят Палатой представителей 2 апреля 2021 г.: одобр. Советом Респ. 21 апреля 2021 г. // ЭТАЛОН: информ.-поисковая система (дата доступа: 08.10.2024).
2. Об авторском праве и смежных правах : Закон Респ. Беларусь : 17 мая 2011 г. № 262-З: принят Палатой представителей 27 апреля 2011 г.: одобр. Советом Респ. 28 апреля 2011 г.// ЭТАЛОН: информ.-поисковая система (дата доступа: 08.10.2024).
3. Дмитриева Ю. Защита авторских прав в интернете Интеллектуальная собственность // Авторское право и смежные права. – 2016. – № 9. – С. 60.
4. Еременко В.И. Совершенствование законодательства в сфере защиты интеллектуальных прав в информационно-телекоммуникационных сетях [Электронный ресурс] // Законодательство и экономика. – 2015. – № 8. – Доступ из справ.-правовой системы «КонсультантПлюс» (дата доступа 08.10.2024).
5. Волосянков Н. Как защитить авторские права в онлайн образовании? – 2019 – [Электронный ресурс] – URL: https://www.if24.ru/valyuta-durova-mozhet-stat-dorozhe-nornikelya/ (дата доступа 08.10.2024).

6. Алексеев А.А. Проблемы обеспечения информационной безопасности при использовании дистанционных образовательных технологий // Право.by. 2020. № 4.
7. Бородич С.А., Давидович А.Л. Правовые аспекты защиты персональных данных участников образовательного процесса при использовании дистанционных образовательных технологий // Право.by. 2020. № 5.
8. Слободянюк А.В. Актуальные вопросы правового регулирования обработки персональных данных в образовательном процессе с применением дистанционных технологий // Право.by. 2022. № 2.
9. Макарова Е.А. Развитие дистанционного образования в Великобритании. М.: ИНФРА-М, 2019.
10. Блоховцова, Г. Г. Перспективы развития дистанционного образования. Преимущества и недостатки / Символ науки. – 2016. – №10. – URL: https://cyberleninka.ru/article/n/perspektivy-razvitiya-distantsionnogo-obrazovaniya-preimuschestva-i-nedostatki (дата доступа: 08.10.2024).