

культуры и спорта, участвующими в спортивной подготовке спортсмена, расторгается в случае их спортивной дисквалификации за допинг в спорте.

Стоит отметить, что дополнительные основания для прекращения трудового договора могут содержаться не только в законодательстве, но и непосредственно в самом трудовом договоре, однако они не должны противоречить закону.

**Заключение.** Изучив трудовое законодательство Республики Беларусь и Российской Федерации о дополнительных основаниях прекращения трудового договора с некоторыми категориями работников можно сделать вывод, что в тех или иных нормах увольнение работника содержит как общие основания прекращения трудового договора, так и дополнительные. Отдельные статьи схожи. Например, пункты 5 и 5<sup>1</sup> статьи 47 ТК Республики Беларусь соответствуют ст. 349<sup>1</sup> ТК РФ. Также существуют и нормы, не отраженные в ст. 47 ТК Республики Беларусь. Например, ст. 349<sup>2</sup> ТК РФ «Особенности регулирования труда работников Фонда пенсионного и социального страхования Российской Федерации». Целью закрепления в законах дополнительных оснований увольнения некоторых категорий работников является повышение ответственности работников, чья трудовая функция связана с выполнением особо ответственной работы, требующей соблюдения государственного и общественного интереса, материальной ответственности, нравственного долга, а также моральных ценностей, при этом обеспечивая гарантии защиты законных интересов физических и юридических лиц.

1. Трудовой кодекс Республики Беларусь [Электронный ресурс]: 26 июля 1999 г. № 296-З: принят Палатой представителей 8 июня 1999 года.; одобрен Советом Республики 30 июня 1999 года.: в ред. Закона Республики Беларусь от 29 июня 2023 г. № 273-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. Центр правовой информ. Респ. Беларусь. – Минск, 2024.

2. Трудовой Кодекс Российской Федерации [Электронный ресурс]: 30.12.2001 № 197-ФЗ: принят Государственной Думой 21 декабря 2001 года.; одобрен Советом Федерации 26 декабря 2001 года.: в ред. Закона Российской Федерации от 14.02.2024 г. // СПС КонсультантПлюс, 2024.

3. Определение Судебной коллегии по гражданским делам Верховного Суда Российской Федерации от 1 февраля 2021 г. № 14-КГ20-14-К1 // СПС КонсультантПлюс, 2024.

## ПРАВОВОЕ РЕГУЛИРОВАНИЕ ЗАЩИТЫ ИНФОРМАЦИИ ПО ЗАКОНОДАТЕЛЬСТВУ РЕСПУБЛИКИ БЕЛАРУСЬ

*Пыж А.С.,*

*магистрант БГУ, г. Минск, Республика Беларусь*

Научный руководитель – Валюшко-Орса Н.В., канд. юрид. наук, доцент

Одним из основных национальных интересов Республики Беларусь в информационной сфере является защита информации, основой обеспечения которой является ее правовое регулирование, что и обуславливает *актуальность* темы исследования. *Целью работы* является анализ правового регулирования защиты информации по законодательству Республики Беларусь.

**Материал и методы.** При проведении исследования использовалось законодательство Республики Беларусь в области защиты информации. Применены следующие методы: анализа, синтеза, формально-юридический и др.

**Результаты и их обсуждение.** Информация, в отношении которой неправомерные действия могут причинить вред ее обладателю или пользователю, подлежит защите. Информация в зависимости от категории доступа подразделяется на общедоступную и информацию ограниченного распространения. При этом доступ к общедоступной информации не может быть ограничен, а ее защита устанавливается только в целях недопущения ее уничтожения, модификации, блокирования [1]. Защита информации ограниченного распространения осуществляется путем установления и соблюдения единых требований. Данная информация должна обрабатываться в информационных системах с применением системы защиты информации, аттестованной в порядке [2],

установленном Оперативно-аналитическом центре при Президенте Республики Беларусь (далее – ОАЦ). Законодательство определяет защиту информации как правовые, организационные и технические меры, направленные на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации [1].

К *правовым мерам* защиты информации относятся обеспечение требований законодательства Республики Беларусь в сфере защиты информации. Также к правовым мерам относятся разработка технической документации и заключение обладателем информации с пользователем информации договора, в котором устанавливаются условия пользования информацией и ответственность сторон за нарушение указанных условий. Законодательную базу составляют «Концепция информационной безопасности» утв. Постановлением Совета безопасности Республики Беларусь от 18 марта 2019 г. № 1; Законы Республики Беларусь от 10 ноября 2008 г. № 455-3 «Об информации, информатизации и защите информации» [1], от 7 мая 2021 г. № 99-3 «О защите персональных данных», Указы Президента Республики Беларусь от 16 апреля 2013 № 196 «О некоторых мерах по совершенствованию защиты информации» (далее – Указ № 196) [3], от 09 декабря 2019 г. № 449 «О совершенствовании государственного регулирования в области защиты информации», правовые акты ОАЦ [2], технические стандарты.

Немаловажное значение имеют *организационные меры*, которые проводятся при проектировании, создании и аттестации системы защиты информации; обеспечении ее функционирования в процессе эксплуатации информационной системы; обеспечении защиты информации в случае прекращения эксплуатации информационной системы. До проектирования СЗИ собственником информационной системы проводится классификация информации по категориям доступа; категоризация информационной системы. Проектирование может осуществляться только организацией, имеющей специальное разрешение ОАЦ. К организационным мерам *при создании системы защиты информации* относятся: обеспечение особого режима допуска на территорию (в помещения), где может быть осуществлен доступ к информации, а также разграничение доступа к информации по кругу лиц и характеру информации. Аттестация системы защиты информации проводится в соответствии с Положением о порядке аттестации систем защиты информации, утвержденным приказом ОАЦ от 20 февраля 2020 г. № 66 «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449» [2]. Ввод в эксплуатацию информационной системы допускается только после получения аттестата соответствия. В *процессе эксплуатации* осуществляется контроль за соблюдением требований законодательства и технической документации, а также обучение пользователей информационной системы.

К *техническим мерам* по защите информации относятся меры по использованию средств технической и криптографической защиты информации, а также меры по контролю защиты информации. Требования к техническим и криптографическим средствам определены Положением о технической и криптографической защите информации, утвержденном Указом № 196 [3]. *Средства технической защиты информации* по своему исполнению могут быть физические, аппаратные, программные. Физические средства применяются при организации режима охраны, пропускного режима и противопожарной защиты. Аппаратные средства выполняют функции обнаружения и нейтрализации подслушивающих и звукозаписывающих устройств и т.п. К программным СТЗИ относятся специальные программы, такие как: идентификации и аутентификации пользователей, разграничения доступа; защиты от несанкционированного доступа; антивирусные программы и т.д. *Средства криптографической защиты информации* реализуют криптографические алгоритмы, суть которых заключается в том, что информация зашифровывается в закрытый текст; затем в зашифрованном виде передается пользователю, который расшифровывает ее с помощью ключа шифрования. Технические и криптогра-

фические средства должны в обязательном порядке иметь сертификат соответствия, выданный в Национальной системе подтверждения соответствия Республики Беларусь, или положительное экспертное заключение по результатам государственной экспертизы, порядок проведения которой определяется ОАЦ. Необходимо использовать комплекс технических и криптографических средств для выстраивания нескольких уровней защиты информации; в этом случае ее эффективность значительно возрастет.

**Заключение.** Таким образом, следует отметить, что защита информации является одной из составляющих информационной безопасности, которая определена как состояние защищенности информационного пространства, информационной инфраструктуры и информационных ресурсов от внешних и внутренних угроз в информационной сфере. В свою очередь, эффективная защита информации возможна лишь при системном применении единых правовых, организационных и технических мер.

1. Об информации, информатизации и защите информации [Электронный ресурс]: Закон Респ. Беларусь от 10 ноября 2008 г. № 455-З: с изм. и доп. от 10 октября 2022 г. № 209-З // ЭТАЛОН. Законодательство Респ. Беларусь / Нац. Центр правовой информ. Респ. Беларусь. – Минск, 2024.

2. О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449 [Электронный ресурс]: Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66 (с изм. от 29 декабря 2022 г. № 210) // ЭТАЛОН. Законодательство Респ. Беларусь / Нац. Центр правовой информ. Респ. Беларусь. – Минск, 2024.

3. О некоторых мерах по совершенствованию защиты информации [Электронный ресурс]: Указ Президента Респ. Беларусь от 16 апреля 2013 г. № 196 (в ред. Указа Президента Респ. Беларусь от 09.12.2019 № 449) // ЭТАЛОН. Законодательство Респ. Беларусь / Нац. Центр правовой информ. Респ. Беларусь. – Минск, 2024.

## РЕГИОНАЛЬНАЯ СОСТАВЛЯЮЩАЯ ОРГАНИЗАЦИЙ СЕКТОРА ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

*Рудаков И.С.,*

*студент 2 курса ВГУ имени П.М. Машерова, г. Витебск, Республика Беларусь*

*Научный руководитель – Янкевич Е.М., канд. экон. наук*

Сектор информационных и коммуникационных технологий (ИКТ) представляет собой одну из ключевых отраслей в современной экономике, играющую важную роль в развитии страны и обеспечении её конкурентоспособности на мировой арене.

В Республике Беларусь сектор ИКТ считается стратегической отраслью, способствующей модернизации и разнообразию экономики страны, что определяет актуальность исследования.

*Цель статьи* – анализ показателей развития организаций сектора информационно-коммуникационных технологий по областям и г. Минску.

**Материал и методы.** При исследовании использованы данные Национального статистического комитета Республики Беларусь, материалы информационных ресурсов по теме исследования. Методы: сравнение, анализ, синтез.

**Результаты и их обсуждение.** ИКТ – комплекс производственных процессов, методов и программно-технических средств, которые собраны воедино с целью сбора, обработки, хранения, трансляции информации. Нами выявлено, что используемые системы электронной почты, мессенджеры, видеоконференции и другие средства связи позволяют хозяйствующему субъекту быстро и эффективно обмениваться информацией и сотрудничать независимо от территориального расположения [1].

Более того, использование ИКТ может снизить издержки на многие аспекты бизнеса, включая бумажную документацию, затраты на транспорт и коммуникации, что помогает улучшить финансовый результат.

Нами проанализированы показатели числа организаций и выручки услуг сектора ИКТ по областям и г. Минску за 2016–2022 гг., что показано в таблице.