Четвериков Илья Алексеевич,
студент 4 курса, Юридический институт,
НИУ «БелГУ»

Научный руководитель:
Сороколетова Марина Александровна,
старший преподаватель кафедры трудового
и предпринимательского права,
Юридический институт, НИУ «БелГУ»

КИБЕРБЕЗОПАСНОСТЬ КАК ЭЛЕМЕНТ ОХРАНЫ ТРУДА

Аннотация. Статья представляет собой исследование проблем обеспечения кибербезопасности как элемента охраны труда. В рамках настоящей статьи затрагивается понятие кибербезопасности и информационной безопасности, анализируется современное состояние института охраны труда. В качестве результатов исследования представлен авторский вывод о том, что в условиях повышенных рисков кибератак и угроз неправомерного получения доступа к информации и информационным ресурсам работодателя, необходимо возложение обязанности на работодателя обеспечивать защиту информации и корреспондирующее этому право работника на безопасные условия труда.

Ключевые слова: Кибербезопасность, информационная безопасность, безопасные условия труда, охрана труда, защита информации, право на безопасные условия труда.

В настоящее время информация выполняет конструктивную роль в любой в сфере, в том числе в сфере труда. Информация является составляющей работы любой организации, предприятия или учреждения, а выполнение трудовой функции работника непосредственно протекает в условиях обработки информации, то есть поиска, хранения, копирования, распространения, архивирования информации.

Кроме того, в настоящее время на рынке труда все более востребованными являются специалисты, обладающие информационно-коммуникативными компетенциями. Это подразумевает под собой наличие навыков и опыта работы с информационными технологиями, например, в рамках ведения деловой и корпоративной переписки посредством использования компьютеров, создания и работы с документами, использования периферийных устройств и накопителей информации, различных программ, в том числе обеспечивающих защиту информации.

Актуальность исследования кибербезопасности сквозь призму охраны труда связана с тем, что в настоящее время «повсеместно наблюдается разработка и внедрение элементов автоматизации производства, оптимизации бизнес-процессов с использованием прикладных программных продуктов. Подобная ситуация, безусловно приводящая к общему качественному преобразованию экономики, снижению совокупных издержек, росту производства и качества готовых товаров и услуг, в свою очередь оказывает значительное воздействие на рынок труд» [1, с. 47].

Н.В. Пугачева также справедливо подчеркивает, что «применение труда все больше и больше связано с автоматизацией, компьютеризацией, использованием инновационных достижений, повышением значимости информации в экономической деятельности и появлением в этой сфере конфиденциальной информации» [2, с. 219].

Внимание вопросу информационной безопасности в российском государстве первоочередно было уделено в Указе Президента РФ от 5 декабря 2016 г. № 646 «Об

утверждении Доктрины информационной безопасности Российской Федерации» [3]. Данный нормативный правовой акт стал стратегической основой для реализации мероприятий, обеспечивающих противодействие информационным угрозам.

Понятие кибербезопасности на законодательном уровне не определено, однако достаточно часто указанный термин соотносится с информационной безопасностью как частное и общее, таким образом, понимая кибербезопасность элементом информационной безопасности.

В работе А.Б. Смушкина кибербезопасность также рассматривается частью информационной безопасности, которая непосредственно связана с обеспечением противодействия инцидентов в киберпространстве [4, с. 114].

Сравнительное сопоставление информационной безопасности и кибербезопасности приводится в научной публикации А. Менлиевой, К. Пирлиева и Г. Атабаевой. По мнению авторов, понятие кибербезопасности полностью поглощается понятием информационной безопасности, но второе из указанных понятий значительно шире. Кибербезопасность предполагает собой состояние защищенности от угроз в киберпространстве или в сфере использования компьютерных технологий [5, с. 1456].

Проблема обеспечения кибербезопасности как элемент охраны труда имеет низкий уровень теоретической разработки. В частности, слабый научный интерес и как следствие недостаточная научная активность наблюдается вокруг проблемы обеспечения кибербезопасности как элемента охраны труда. Иначе говоря, необходимо поставить вопрос о том, может ли обеспечение информационной безопасности в трудовой сфере рассматриваться в качестве элемента охраны труда? Если да, то насколько институт охраны труда в настоящее время отвечает современным реалиям и обеспечивает защиту прав и свобод работников?

Так, прежде всего, согласно ст. 209 ТК РФ, под охраной труда понимается «система сохранения жизни и здоровья работников в процессе трудовой деятельности, включающая в себя правовые, социально-экономические, организационно-технические, санитарно-гигиенические, лечебно-профилактические, реабилитационные и иные мероприятия» [6]. Необходимо уточнить, что институт охраны труда в российском трудовом праве направлен на обеспечение сохранения жизни и физического здоровья работников.

Также, если обратиться к понятию безопасных условий труда, то под ними в Трудовом кодексе Российской Федерации понимаются «условия труда, при которых воздействие на работающих вредных и (или) опасных производственных факторов исключено либо уровни воздействия таких факторов не превышают установленных нормативов» [6].

Вся информация, обладателем которой является работодатель, находится в руках работников, трудовые функции которых связаны с ее хранением, обработкой, использованием и пр. Так, например, в результате неправомерного получения доступа со стороны третьих лиц к информации, хранящейся на персональном компьютере работника, и использующейся им в процессе трудовой деятельности, может пройти утечка данных, в результате которой будет причинен вред работодателю. Особую опасность представляет утечка конфиденциальной информации или сведений, в отношении которых введен режим коммерческой тайны.

Между тем, обеспечение сохранности и конфиденциальности информации путем реализации правовых, организационных и технических мер осуществляется в интересах самого работодателя. Принять меры правового, организационного, технологического характера, направленные на защиту информации работодателя, является правом, а не обязанностью работодателя. Работник, в свою очередь, осуществляет свою трудовую функцию и в связи с этим обработку информации в условиях, которые ему обеспечивает работодатель. С учетом изложенного обоснованно возникает вопрос о том, необходимо ли на современном этапе предусмотреть в нормах трудового права обязанность работодателя

обеспечивать защиту информации, тем самым создавая для работника безопасные условия труда и гарантируя защиту от киберугроз?

По большей мере правовое регулирование в сфере труда и охраны труда ориентировано на защиту прав и свобод работников от угроз, имеющих физический характер. Специфика угроз в киберпространстве заключается в том, что они существуют в виртуальной среде, но способы причинить вред охраняемым законом благам и ценностям, в том числе интересам работодателей.

Очевидно, что действующий институт охраны труда и трудовое регулирование в целом слабо ориентировано на защиту прав работников от угроз в информационном пространстве и обеспечение безопасных условий труда с учетом существования угрозы неправомерного получения доступа и последующего использования информации, принадлежащей работодателя, третьими лицами. Так, на законодательном уровне не введена обязанность работодателя обеспечивать защиту принадлежащей ему информации, использующейся работником при выполнении трудовой функции, в ситуациях, когда такая информация может быть неправомерно получена третьими лицами при отсутствии вины самого работника.

Таким образом, можно сделать вывод о том, что на современном этапе развития отношений кибербезопасность вполне может трактоваться в качестве элемента охраны труда. В условиях повышенных рисков кибератак существуют угрозы неправомерного получения доступа к информации и информационным ресурсам работодателя, использующимся работником. При этом именно на работодателя должна возлагаться обязанность обеспечить соответствующими мерами защиту информации и корреспондирующее этому право работника на безопасные условия труда.

Список литературы:

1. Коновалова О.В., Волконский В.А. Развитие информационно-коммуникативных компетенций молодого специалиста сферы анализа рисков и экономической безопасности в условиях современных вызовов рынка труда // Управление персоналом и интеллектуальными ресурсами в России. 2020. № 83. С. 47-50.

2. Пугачева Н.В. Обеспечение права работодателя на защиту информации: проблемы правового регулирования // Ежегодник трудового права. 2024. Вып. 14. С. 219-230.

3. Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».

4. Смушкин А.Б. Кибербезопасность: понятие, структура, механизм правового обеспечения // Правоприменение. 2025. № 3. С. 114-123.

5. Менлиева А., Пирлиев К., Атабаева Г. Сравнение понятий информационной и кибербезопасности // Вестник науки. 2024. № 3 (74). С.1454-1458.

6. Трудовой кодекс Российской Федерации от 30 декабря 2001 г. № 197-ФЗ (ред. от 30.02.2026) // Собрание законодательства Российской Федерации. 2002. №1 (часть I). Ст. 3.