УДК 349.2

А. О. Маров,
курсант 2-го курса факультета милиции
Могилевского института МВД
Научный руководитель: Н. В. Пушко,
доцент кафедры правовых дисциплин
факультета повышения квалификации
и переподготовки кадров
Могилевского института МВД,
кандидат экономических наук, доцент

ДИСЦИПЛИНАРНАЯ ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ЗАКОНОДАТЕЛЬСТВА О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

В условиях цифровизации особое внимание уделяется защите персональных данных граждан. В Республике Беларусь принят Закон от 7 мая 2021 г. № 99-З «О защите персональных данных» [1] (далее — Закон № 99), установивший правовые основы обработки персональных данных граждан и ответственность за ее нарушение, а также определивший права и обязанности субъектов и операторов персональных данных. В 2021 г. в части реализации Указа Президента Республики Беларусь от 28 октября 2021 г. № 422 «О мерах по совершенствованию защиты персональных данных» создан Национальный центр защиты персональных данных, который контролирует соблюдение этого законодательства [2].

Статья 19 Закона № 99 гласит, что лица, виновные в нарушении законодательства в части защиты персональных данных, несут ответственность, предусмотренную другими правовыми актами, в том числе и дисциплинарную, установленную в Трудовом кодексе Республики Беларусь (далее — ТК) [3]. Так, согласно ст. 197 ТК, дисциплинарная ответственность наступает за «противоправное, виновное неисполнение или ненадлежащее исполнение работником своих трудовых обязанностей». Отметим, что важной новацией стало введение специального основания для увольнения за нарушение порядка обработки персональных данных: «нарушение работником порядка сбора, систематизации, хранения, изменения, использования, обезличивания, блокирования, распространения, предоставления, удаления персональных данных» (п. 10 ч. 1 ст. 47 ТК) [3]. Из этого следует, что нарушение законодательства о защите персональных данных признается самостоятельным дисциплинарным проступком и при доказанной виновности работника за несоблюдение этой нормы может явиться основанием для его увольнения.

Однако при практической реализации данной нормы ТК правоприменитель сталкивается с тем, что она может быть применена только к ограниченному кругу лиц, в частности только к тем работникам, на которых возложена обязанность по обработке персональных данных, что на практике означает невозможность привлечь к дисциплинарной ответственности за нарушение правил по защите персональных данных административный персонал (например, менеджеров) без прямых обязанностей по защите такого рода информации. Кроме того, трудовое законодательство исходит из презумпции невиновности работника, и поэтому обязанность доказать его вину в совершенном дисциплинарном проступке ложится на нанимателя. При этом увольнение по основанию, предусмотренному ч. 1 ст. 47 ТК, возможно лишь при доказанном умысле или небрежности работника [3]. В то же время на практике представляется затруднительным определить, кто конкретно и в чем виновен при утечке данных: это мог быть технический сбой или некорректный инструктаж руководства в части защиты персональных данных, что затрудняет применение дисциплинарного взыскания.

Помимо всего прочего, единственной мерой дисциплинарной ответственности за нарушение правил по защите персональных данных является только увольнение, что может вызывать споры о соразмерности наказания: может ли увольнение как наиболее суровая мера дисциплинарного взыскания применяться к работникам, совершившим случайную ошибку. Поэтому было бы целесообразно рассмотреть возможность определить и другие меры дисциплинарных взысканий за нарушение норм по защите персональных данных, в частности за проступки, совершенные по неосторожности, что позволит варьировать наказания в зависимости от степени вины сотрудника.

Кроме того, приведение локальных актов организации (должностных инструкций, положений об обработке персональных данных и других внутренних документов) в соответствие с законодательством о защите персональных данных позволит четко закрепить обязанности сотрудников, ответственных за защиту таких данных. Также нельзя сбрасывать со счетов обучение и информирование персонала, так как проведение регулярных тренингов по защите персональных данных поможет снизить число нарушений в этой сфере. Но помимо человеческого фактора, усиление мер технической защиты, таких как шифрование, контроль доступа, аудит журналов и других как программных, так и аппаратных средств, также позволит предотвратить риск утечек информации.

Таким образом, для повышения эффективности режима ответственности за нарушения в сфере защиты и обработки персональных данных необходимо сочетать ужесточение законодательства с развитием внутренних

корпоративных механизмов (обучение, инструкции, аудит). В перспективе законодатель может уточнить отдельные нормы (например, расширить круг лиц для применения мер дисциплинарного взыскания), а правоприменители — выработать «прецедентные» подходы, ориентированные на справедливость и защиту интересов как субъектов защиты персональных данных, так и работников, ответственных за обработку и хранение такой информации. При этом важно, чтобы все применяемые к работнику меры учитывали баланс между эффективностью контроля и защитой прав работников.

1. О защите персональных данных [Электронный ресурс] : Закон Респ. Беларусь от 7 мая 2021 г. № 99-З : в ред. от 1 июня 2022 г. № 175-З. Доступ из информ.-поисковой системы «ЭТАЛОН». Вернуться к статье

2. О мерах по совершенствованию защиты персональных данных [Электронный ресурс] : Указ Президента Республики Беларусь от 28 окт. 2021 г. № 422 : в ред. от 24 марта 2025 г. № 113. Доступ из информ.-поисковой системы «ЭТАЛОН». Вернуться к статье

3. Трудовой кодекс Республики Беларусь [Электронный ресурс] : 26 июля 1999 г. № 296-З : принят Палатой представителей 8 июня 1999 г. : одобр. Советом Респ. 30 июня 1999 г. : в ред. от 8 июля 2024 г. № 25-З. Доступ из информ.-поисковой системы «ЭТАЛОН». Вернуться к статье