Секция «10.5 Компьютерное право и информационная безопасность»

Правовые границы мониторинга сотрудников в целях обеспечения информационной безопасности

Научный руководитель – Чимитдоржиев Нимбу Баирович

Вохмянин С.В.[1], *Теслов М.С.*[2], *Харитонов Т.В.*[3]

1 - Национальный исследовательский университет «Высшая школа экономики», Московский институт электроники и математики им. А.Н. Тихонова, Москва, Россия, *E-mail: stepan040606@gmail.com*; 2 - Национальный исследовательский университет «Высшая школа экономики», Московский институт электроники и математики им. А.Н. Тихонова, Москва, Россия, *E-mail: matveyteslovv@gmail.com*; 3 - Национальный исследовательский университет «Высшая школа экономики», Московский институт электроники и математики им. А.Н. Тихонова, Москва, Россия, *E-mail: tvkharitonov@edu.hse.ru*

Цифровая трансформация труда привела к широкому внедрению средств мониторинга действий сотрудников на корпоративных ресурсах: журналирование событий безопасности, прокси-логирование, DLP/EDR, контроль использования корпоративной почты и мессенджеров. Для работодателя такие меры выступают инструментом управления рисками утечек, инцидентов и нарушений режима коммерческой тайны [7]. Вместе с тем мониторинг неизбежно затрагивает конституционные гарантии неприкосновенности частной жизни и тайны сообщений (ст. 23, 24 Конституции РФ) [2] и влечет обработку персональных данных работника, что повышает риск признания мер незаконными и (практически) снижает доказательственную ценность материалов мониторинга.

Цель исследования - определить правовые пределы допустимого мониторинга цифровых действий сотрудников в целях обеспечения информационной безопасности (ИБ) в Российской Федерации и выявить дефекты действующего регулирования. Задачи: (1) описать типовые практики мониторинга и связанные с ними риски; (2) выделить проблемные зоны и предложить критерии соразмерности и процедурные гарантии.

Нормативная рамка мониторинга носит межотраслевой характер. Трудовое право допускает обработку персональных данных работника, в том числе для контроля количества и качества выполняемой работы и обеспечения сохранности имущества работодателя (ст. 86 ТК РФ) [4], однако требует соблюдения целей обработки и гарантий работника. Закон о персональных данных закрепляет принципы целевого характера и минимизации обработки (ст. 5 152-ФЗ) [9]. Закон об информации устанавливает общие правила обращения с информацией и режимы доступа [8]. При наличии режима коммерческой тайны мониторинг может выступать мерой обеспечения охраны сведений [7]. Для отдельных организаций, являющихся субъектами КИИ, цели ИБ подкрепляются специальными обязанностями по защите значимых объектов [6].

Ключевым является разграничение мониторинга по уровню вмешательства. Постоянное техническое журналирование событий ИБ (метаданные, факты доступа, системные логи) в общем случае в меньшей степени затрагивает содержание сообщений, чем прямой доступ к ним и пользовательским файлам. Позиция Конституционного Суда РФ подчеркивает, что тайна переписки и иных сообщений является самостоятельной конституционной гарантией и ее ограничение допускается только при соблюдении установленных законом процедур; формальные соглашения или "статус владельца сервиса" сами по себе не легитимируют произвольный доступ к содержанию сообщений (Постановление КС РФ от 26.10.2017 № 25-П) [3]. Следовательно, меры, затрагивающие содержание коммуникаций, требуют повышенного обоснования, строгой регламентации и максимальной минимизации объема вмешательства.

С учетом указанной рамки мониторинг в целях ИБ может быть признан допустимым при одновременном соблюдении следующих условий. Во-первых, должна быть сформулирована легитимная и конкретная цель (предотвращение инцидентов, расследование утечек, обеспечение режима коммерческой тайны), а не абсолютный контроль. Во-вторых, меры должны быть соразмерны цели и минимизировать сбор и использование данных (принцип минимизации 152-ФЗ) [9]. В-третьих, необходима предварительная регламентация через локальные нормативные акты и ознакомление работников: состав собираемых данных, сроки хранения, роли доступа, основания "эскалации" от агрегированной аналитики к персонализированному расследованию. В-четвертых, должны быть обеспечены организационные гарантии: ограничение круга лиц, имеющих доступ к результатам мониторинга; фиксация обращений к данным; разграничение доступа по принципу необходимости; разумные сроки хранения.

Дефекты действующего регулирования проявляются в трех зонах. (1) Отсутствует единая, прямо закреплённая градация мер мониторинга по уровню вмешательства, из-за чего меры применяются непропорционально поставленным целям и выходят за пределы необходимого и обоснованного вмешательства. (2) Недостаточно определены процедурные стандарты корпоративного ИБ-расследования: кто, на каком основании и в каком порядке принимает решение о доступе к данным работника; какие уведомления и журналы доступа необходимы; как обеспечивается внутренний контроль и так далее. (3) В условиях удаленной работы и BYOD практики мониторинга нередко выходят за пределы корпоративной инфраструктуры, повышая риск неправомерного вмешательства в частную сферу, что может образовывать как административные риски (ст. 13.11 КоАП РФ) [1], так и уголовно-правовые (ст. 137, 138 УК РФ) [5].

Источники и литература

1) Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (с изм. и доп.) (ст. 13.11).
2) Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с изм. и доп.).
3) Постановление Конституционного Суда Российской Федерации от 26.10.2017 № 25-П (по жалобе гражданина И.П. Сушкова).
4) Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ (с изм. и доп.).
5) Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (с изм. и доп.) (ст. 137, 138).
6) Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (с изм. и доп.).
7) Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» (с изм. и доп.).
8) Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изм. и доп.).
9) Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (с изм. и доп.).