

ПРИКАЗ БЮРО ЗАЩИТЫ ДАННЫХ И ТРУДОВОГО БЮРО НЕО-СИТИ

№ 523

"О порядке использования биометрических данных для контроля доступа на рабочих местах"

г. Нео-Сити

25 сентября 2089 года

В целях регулирования использования биометрических данных как специальной категории (статья 4.2 КЗД) в трудовых отношениях и обеспечения баланса интересов работодателей и работников в соответствии со статьёй 2.1 Трудового регламента Нео-Сити, Бюро защиты данных совместно с Трудовым бюро

ПРИКАЗЫВАЮТ:

1. Общие положения

1.1. Настоящий Приказ устанавливает требования к использованию биометрических данных работников для целей контроля доступа на территорию работодателя и к информационным системам.

1.2. Для целей настоящего Приказа:

- а) *биометрические данные* — данные, раскрывающие физиологические или поведенческие характеристики человека, позволяющие его идентифицировать (статья 4.2 КЗД);
- б) *система биометрического контроля доступа (СКУД)* — программно-аппаратный комплекс для идентификации или верификации личности по биометрическим данным;
- в) *идентификация* — установление личности путём сравнения биометрических данных с базой данных (1:N);
- г) *верификация* — подтверждение личности путём сравнения биометрических данных с образцом конкретного лица (1:1);
- д) *биометрический шаблон* — математическое представление биометрических характеристик.

1.3. Действие настоящего Приказа распространяется на:

- а) всех работодателей, использующих биометрические системы контроля доступа;
- б) организации, обрабатывающие биометрические данные работников по договору;
- в) поставщиков биометрических систем.

2. Допустимые цели использования биометрии

2.1. Использование биометрических данных работников допускается для следующих целей:

- а) контроль физического доступа на территорию организации;
- б) контроль доступа в помещения с ограниченным доступом;
- в) контроль доступа к информационным системам;
- г) учёт рабочего времени;
- д) обеспечение безопасности на опасных производственных объектах.

2.2. Запрещённые цели:

- а) мониторинг эмоционального состояния работников;
- б) оценка производительности на основе биометрических показателей;
- в) выявление состояния здоровья (кроме случаев, прямо предусмотренных законом);
- г) скрытое наблюдение за работниками;
- д) передача биометрических данных третьим лицам без согласия работника.

2.3. Работодатель обязан документально обосновать необходимость использования биометрии и невозможность достижения тех же целей менее инвазивными методами.

3. Виды биометрических данных

3.1. Допустимые виды биометрических данных для контроля доступа:

- а) отпечатки пальцев;
- б) изображение лица (2D или 3D);
- в) рисунок радужной оболочки глаза;
- г) геометрия руки;
- д) рисунок вен ладони.

3.2. Ограниченные виды (требуют дополнительного обоснования):

- а) голос (только для телефонных систем);
- б) походка и динамика движений;
- в) рисунок сетчатки глаза.

3.3. Запрещённые виды для целей контроля доступа:

- а) генетические данные;
- б) нейробиометрия (ЭЭГ, активность мозга);
- в) данные о состоянии здоровья.

3.4. Работодатель не вправе собирать биометрические данные видов, не предусмотренных для заявленных целей.

4. Требования к согласию работника

4.1. В соответствии со статьёй 4.2 КЗД (специальные категории данных) и статьёй 21.2 КЗД (явное согласие) использование биометрических данных требует явного согласия работника.

4.2. Согласие должно быть:

- а) добровольным — не может быть условием приёма на работу (за исключением случаев, указанных в пункте 4.5);
- б) конкретным — на определённые цели использования;
- в) информированным — работник должен понимать, как будут использоваться его данные;
- г) документально подтверждённым — в письменной форме.

4.3. Содержание согласия:

- а) наименование работодателя;
- б) виды собираемых биометрических данных;
- в) цели использования;
- г) срок хранения;
- д) права работника;
- е) возможность отзыва согласия;
- ж) последствия отзыва.

4.4. Работник вправе отозвать согласие в любой момент. Отзыв не влияет на законность обработки до момента отзыва.

4.5. Исключения из требования о добровольности. Биометрическая идентификация может быть обязательным условием работы для:

- а) сотрудников, имеющих доступ к государственной тайне;
- б) сотрудников критической инфраструктуры (по перечню, утверждённому Советом Нео-Сити);
- в) сотрудников финансовых организаций, имеющих доступ к клиентским средствам.

4.6. При отказе работника от биометрической идентификации (кроме случаев пункта 4.5)

работодатель обязан предоставить альтернативный способ контроля доступа.

5. Альтернативные способы идентификации

5.1. Работодатель обязан обеспечить альтернативу биометрической идентификации:

- а) пропуск или карта доступа;
- б) PIN-код или пароль;
- в) токен или ключ;
- г) комбинация указанных методов.

5.2. Альтернативный способ:

- а) должен обеспечивать сопоставимый уровень безопасности;
- б) не должен создавать существенных неудобств работнику;
- в) не должен влечь дополнительных затрат для работника;
- г) не должен приводить к дискриминации.

5.3. Работодатель не вправе:

- а) создавать преимущества для работников, использующих биометрию;
- б) фиксировать факт отказа от биометрии в личном деле;
- в) учитывать отказ при принятии кадровых решений.

6. Технические требования к системам

6.1. Системы биометрического контроля доступа должны соответствовать требованиям:

6.1.1. Безопасность хранения:

- а) биометрические шаблоны хранятся в зашифрованном виде;
- б) исходные биометрические образцы (фото, сканы) удаляются после создания шаблона;
- в) шаблоны хранятся отдельно от идентификационных данных работника;
- г) доступ к базе шаблонов ограничен.

6.1.2. Защита при обработке:

- а) сравнение биометрических данных производится локально где возможно;
- б) при передаче данных используется шифрование;
- в) результаты сравнения не раскрывают биометрические данные.

6.1.3. Точность и надёжность:

- а) ложное отклонение (FRR) — не более 1%;
- б) ложное принятие (FAR) — не более 0.01%;
- в) система должна работать в условиях реальной эксплуатации;
- г) регулярная калибровка и тестирование.

6.2. Предпочтительные архитектуры:

- а) хранение шаблона на карте работника (match-on-card);
- б) децентрализованное хранение;
- в) использование необратимых преобразований.

6.3. Запрещается:

- а) хранение биометрических данных в облачных сервисах за пределами Нео-Сити;
- б) использование биометрических данных для целей, не указанных в согласии;
- в) объединение баз биометрических данных разных работодателей.

7. Сроки хранения биометрических данных

7.1. Биометрические данные работника хранятся:

- а) в период трудовых отношений;
- б) не более 30 дней после прекращения трудовых отношений.

7.2. По истечении срока биометрические данные подлежат безвозвратному удалению:

- а) шаблоны удаляются из всех систем;
- б) резервные копии уничтожаются;
- в) составляется акт об удалении.

7.3. Работник вправе потребовать удаления биометрических данных:

- а) при отзыве согласия;
- б) при переходе на альтернативный способ идентификации;
- в) при прекращении трудовых отношений.

7.4. Исключения из сроков хранения:

- а) при расследовании инцидентов безопасности — до завершения расследования;
- б) по требованию правоохранительных органов — в соответствии с решением суда.

8. Права работников

8.1. Работник имеет право:

- а) знать, какие биометрические данные о нём собраны;
- б) получить копию своих данных в машиночитаемом формате;
- в) требовать исправления неточных данных;
- г) требовать удаления данных;
- д) отозвать согласие;
- е) использовать альтернативный способ идентификации.

8.2. Работник имеет право на информацию о:

- а) целях использования биометрии;
- б) сроках хранения;
- в) лицах, имеющих доступ к данным;
- г) мерах безопасности;
- д) порядке отзыва согласия.

8.3. Работодатель обязан:

- а) предоставить информацию в течение 14 дней;
- б) удалить данные в течение 30 дней после требования;
- в) уведомить работника об утечке биометрических данных незамедлительно.

9. Обязанности работодателя

9.1. Работодатель обязан:

9.1.1. До внедрения системы:

- а) провести оценку воздействия на защиту данных (статья 24 КЗД);
- б) обосновать необходимость биометрии;
- в) разработать политику использования биометрии;
- г) обеспечить альтернативный способ идентификации;

д) провести консультации с представителями работников.

9.1.2. При эксплуатации:

- а) обеспечить безопасность системы;
- б) вести журнал доступа к биометрическим данным;
- в) проводить регулярный аудит;
- г) обучить персонал, имеющий доступ к данным;
- д) назначить ответственного за защиту биометрических данных.

9.1.3. При инцидентах:

- а) уведомить Бюро защиты данных в течение 24 часов;
- б) уведомить затронутых работников незамедлительно;
- в) провести расследование;
- г) принять меры по предотвращению повторения.

9.2. Работодатель ведёт реестр систем биометрического контроля доступа, включающий:

- а) перечень систем и их назначение;
- б) виды обрабатываемых биометрических данных;
- в) количество работников, использующих систему;
- г) меры безопасности;
- д) результаты аудитов.

10. Ответственность

10.1. За использование биометрии без согласия работника:

- а) штраф 100,000 кредитов за каждого работника;
- б) обязанность удалить данные;
- в) компенсация морального вреда работнику.

10.2. За нарушение требований безопасности:

- а) штраф 500,000-5,000,000 кредитов;
- б) приостановление использования системы.

10.3. За утечку биометрических данных:

- а) штраф до 4% годового оборота;
- б) компенсация ущерба работникам;
- в) уголовная ответственность при умышленных действиях.

10.4. За дискриминацию работников, отказавшихся от биометрии:

- а) штраф 200,000 кредитов;
- б) восстановление нарушенных прав работника;
- в) компенсация.

10.5. Должностные лица работодателя несут персональную ответственность за нарушение требований настоящего Приказа.

11. Переходные положения

11.1. Настоящий Приказ вступает в силу с 01 ноября 2089 года.

11.2. Работодатели, использующие биометрические системы, обязаны:

- а) получить согласия работников до 01 января 2090 года;
- б) привести системы в соответствие до 01 марта 2090 года;

в) обеспечить альтернативные способы идентификации до 01 февраля 2090 года.

11.3. При отказе работника дать согласие работодатель обязан перевести его на альтернативный способ идентификации в течение 30 дней.

11.4. Бюро защиты данных и Трудовое бюро публикуют совместные методические рекомендации до 15 октября 2089 года.

Директор Бюро защиты данных

Е.А. Морозова

Директор Трудового бюро

Н.С. Кадров

Регистрационный номер: НС-БЗД/ТБ-523/09-25

Опубликован: 01 октября 2089 года