**УДК 349.2**
**DOI 10.26118/9933.2025.89.62.019**

# Безопасность и этические аспекты использования цифровых профилей персонала в машиностроительной отрасли

**Життеев Тимур Юрьевич**
Московский государственный технический университет
**Старожук Евгений Андреевич**
Московский государственный технический университет

**Аннотация.** Внедрение цифровых профилей сотрудников на предприятиях машиностроения, основанных на анализе данных из HR-систем, производственных платформ и инженерных сред, открывает новые возможности для управления персоналом, повышения производительности и безопасности труда, но одновременно порождает риски, связанные с защитой персональных данных, киберугрозами и этическими вопросами. В данной статье рассматриваются ключевые угрозы информационной безопасности, правовые аспекты обработки и хранения данных работников, а также этические дилеммы, возникающие при цифровизации HR-процессов и внедрении аналитических и автоматизированных решений. Предлагаются практические рекомендации по обеспечению конфиденциальности информации о сотрудниках, снижению внешних и внутренних рисков, выстраиванию прозрачных правил использования цифровых профилей сотрудников, позволяющих соблюдать баланс между эффективностью управления, производственной безопасностью и правами работников.

**Ключевые слова:** цифровой профиль, персональные данные, этика, машиностроение, конфиденциальность.

**Zhitteev Timur Yurievich**
Bauman Moscow State Technical University
**Starozhuk Evgeny Andreevich**
Bauman Moscow State Technical University

# Safety and ethical aspects of using digital personnel profiles in the engineering industry

**Abstract.** The introduction of digital employee profiles in engineering enterprises based on the analysis of data from HR systems, production platforms and engineering environments opens up new opportunities for personnel management, improving productivity and occupational safety, but at the same time creates risks related to personal data protection, cyber threats and ethical issues. This article examines the key threats to information security, the legal aspects of processing and storing employee data, as well as the ethical dilemmas that arise during the digitalization of HR processes and the introduction of analytical and automated solutions. Practical recommendations are offered on ensuring the confidentiality of information about employees, reducing external and internal risks, and building transparent rules for using digital employee profiles to maintain a balance between management efficiency, industrial safety, and employee rights.

**Keywords:** digital profile, personal data, ethics, engineering, confidentiality.

Цифровизация машиностроения заметно меняет практики работы с персоналом и требования к управлению трудовыми ресурсами. На предприятиях отрасли всё шире применяются цифровые инструменты, в том числе системы, формирующие электронные профили сотрудников, где аккумулируются сведения о личных данных, профессиональной подготовке, уровнях допуска и опыте работы. Использование таких решений упрощает

кадровое планирование, позволяет системно отслеживать соответствие квалификации требованиям производства и повышает уровень охраны труда. Для машиностроительных организаций, ориентированных на сложные технологические процессы и высокую ответственность персонала, цифровые профили становятся удобным инструментом подбора, обучения и оценки работников. Вместе с тем их внедрение связано с рядом существенных вызовов: некорректная обработка информации снижает доверие сотрудников, алгоритмические перекосы могут приводить к несправедливым управленческим решениям, а утечки данных и неправомерный доступ создают предпосылки для злоупотреблений и промышленного шпионажа.

Под цифровым профилем понимается структурированный набор персональных и около персональных данных о сотруднике, формируемый из корпоративных источников и дополненный аналитикой — от оценки и матриц компетенций до прогноза рисков инцидентов. Цифровые профили сотрудников могут включать биометрические данные, сведения о производительности, медицинские показатели и даже поведенческие паттерны. С одной стороны, это повышает эффективность производства, с другой — создает угрозы приватности и автономии работников. В условиях ужесточающегося регулирования и растущего внимания к корпоративной социальной ответственности (КСО), компаниям необходимо находить баланс между технологическим прогрессом и защитой прав персонала. Сбор, хранение и анализ персональных данных сопряжены с серьезными вызовами:

- Юридические риски (несоблюдение 152-ФЗ и других норм);
- Угрозы кибербезопасности (утечки данных, хакерские атаки);
- Этические конфликты (снижение доверия сотрудников, дискриминация на основе данных).

Существует ряд угроз безопасности цифровых профилей сотрудников, которые могут привести к нарушению прав работников и финансовым потерям предприятий. Опасность идёт как снаружи (фишинг, хакерские атаки), так и изнутри (халатность сотрудников). В итоге цифровой профиль становится не просто набором сведений и данных, а потенциальным доступом к людям и процессам, где любая уязвимость в процессах безопасности быстро вырастает до инцидента уровня предприятия. Рассмотрим ключевые из возможных угроз в Таблице 1.

*Таблица 1. Угрозы безопасности цифровых профилей сотрудников*

| **Наименование** | **Описание** | **Примеры** |
|---|---|---|
| *Внешние киберугрозы* | | |
| 1. Хакерские атаки и утечка данных | Цифровые профили содержат персональные данные сотрудников (такие как паспорта, медицинские записи, биометрию и тд.). Все это может стать мишенью для хакеров в целях фишинга и целевых атак на системы предприятий. | В 2019 году у компании «РЖД» произошла утечка персональных данных более 700 тыс. сотрудников. В результате хакерской атаки в открытом доступе оказались телефонные номера, должности, снимки СНИЛС сотрудников. [10] |
| 2. Промышленный шпионаж | Цифровые профили могут содержать информацию, представляющую собой коммерческую или служебную тайну. | В 2019 году компания «Tesla» обвинила своего бывшего инженера Цао Гуанчжи в передаче файлов, которые касались работы |

| | | |
|---|---|---|
| | Компании-конкуренты могут незаконно завладеть данной информацией посредством взлома информационной системы предприятия, вербовки персонала или других методов недобросовестной конкуренции. [8] | автопилота электрокара компании, китайскому производителю «Xiaopeng Motors». [11] |
| 3. Рансомварь | Рансомварь — это вредоносная программа, которая шифрует и блокирует файлы и системы с целью получения вознаграждением создателем такой программы. [13] | Более 15 компаний, входящие в агрохолдинг, «Мираторг» пострадали от вредоносной программы, зашифровавшей данные компаний. [15] |
| *Внутренние угрозы* | | |
| 4. Злоупотребление доступом | Сотрудники компании могут продавать данные, взятые из цифровых профилей, различным заинтересованным лицам. | В 2019 году у ПАО «Сбербанк» произошла утечка данных клиентов и сотрудников. Компания заподозрила в хищении сведений своих сотрудников. [12] |
| 5. Халатность при обращении с информацией | Сотрудники компании в силу невнимательности и пренебрежения правилами могут непреднамеренно стать причиной утечки, искажения или уничтожения данных | Шведская страховая компания «Trygg-Hansa» была оштрафована на 3 миллиона долларов США из-за утечки персональных данных клиентов. Утечка произошла из-за халатности при установке аутентификации баз данных. [14] |
| 6. Дискриминация на основе данных | Анализ данных о здоровье или возрасте может привести к негласному отказу в допуске перспективных сотрудников к новым проектам или обучению из-за страха компании перед возможными рисками. | ПАО «Аэрофлот» снизила надбавки к заработной плате своей бортпроводнице из-за «не соответствия по требованиям к физическим данным в части установленного диапазона размера одежды». [7] |

В целях предотвращения потенциальных угроз необходимы строгая минимизация и сегментация данных в профилях, прозрачные цели обработки с запретом «скрытой» смены назначения, ограниченные сроки хранения, управление доступами по принципу наименьших прав и регулярный их пересмотр. Не менее важно закрепить «право на объяснение» решений систем, каналы оспаривания и участие сотрудников в определении границ наблюдения. Только сочетание технической гигиены, правовых гарантий и подотчётности в использовании цифровых профилей позволяет извлечь пользу для эффективности и безопасности без превращения машиностроительного предприятия в непрозрачную систему тотального контроля, уязвимую для внешних и внутренних угроз.

Использование цифровых профилей сотрудников в РФ на предприятиях регулируется комплексом нормативно-правовых актов, которые устанавливают требования к обработке персональных данных, защите конфиденциальной информации и правам работников, которые работодатель обязан соблюдать. Юридические аспекты и вызовы цифровизации затрагивают не только охрану личной информации, но и вопросы цифрового суверенитета, правовой ясности и справедливости. [9]. Основными законодательными актами, формирующие правовой фундамент для обработки любых персональных данных в РФ, являются:

*Таблица 2. Перечень нормативно-правовых актов, регулирующие использование персональных данных в РФ*

| **Наименование** | **Содержание** |
|---|---|
| 1. Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных" | • Определение персональных данных: любая информация, относящаяся к прямо или косвенно определенному физическому лицу.<br>• Требования к обработке: обязательное получение письменного согласия работника на обработку персональных данных, за исключением случаев, предусмотренных законом.<br>• Права субъектов: работник имеет право на доступ к своим персональным данным, их уточнение и блокирование. [2] |
| 2. Трудовой кодекс Российской Федерации (ст. 85–90) | • Обработка персональных данных работника: должна осуществляться исключительно для целей обеспечения соблюдения законов и иных нормативных правовых актов.<br>• Хранение и использование: работодатель обязан обеспечивать защиту персональных данных от неправомерного использования;<br>• Передача данных: ограниченность сведений и данных о сотрудниках, которые возможны к передаче. [1] |
| 3. Федеральный закон от 29.07.2004 № 98-ФЗ "О коммерческой тайне" | • Защита конфиденциальной информации: регулирует вопросы защиты служебной и коммерческой тайны, включая данные о сотрудниках. [3] |

| | |
|---|---|
| 4. Приказ Роскомнадзора от 05.09.2013 № 996 "Об утверждении требований и методов по обезличиванию персональных данных" | • Обезличивание данных: устанавливаются методы и требования к обезличиванию персональных данных для их использования в статистических и аналитических целях. [5] |
| 5. Постановление Правительства РФ от 15.09.2008 № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации" | • Обработка без автоматизации: регулирует порядок обработки персональных данных неавтоматизированными способами. [4] |
| 6. Отраслевые стандарты и рекомендации (Приказы ФСТЭК России, методические рекомендации Роскомнадзора и др.) | • Устанавливают требования к защите информации в информационных системах персональных данных; [6]<br>• Разъясняют порядок применения законодательства о персональных данных. |

В итоге нормативно-правовая рамка вокруг использования персональных данных задаёт для цифровых профилей в машиностроении чёткие границы допустимого: обработка должна быть необходимой, соразмерной цели и прозрачной для сотрудника, с опорой на законное основание (легитимный интерес работодателя, исполнение трудовых и охранных обязательств). Национальные законы труда ограничивают поведенческую аналитику и автоматизированные решения, требуют минимизации, разграничения доступов, сроков хранения и надлежащих договоров с обработчиками, а при трансграничной передаче — адекватных гарантий и договорных инструментов. Параллельно с этим, отраслевые стандарты переводят эти принципы в проверяемые меры — от сегментации ИТ -контуров до регулярных аудитов. Ключевым остаётся баланс: защита коммерческой тайны и безопасности производства не оправдывает «тотального наблюдения» — работники сохраняют права на доступ, исправление, ограничение, оспаривание автоматизированных решений, а участие профсоюзов или других представительных органов при внедрении систем наблюдения снижает правовые и репутационные риски. Соблюдение этих принципов законности и подотчётности превращает цифровые профили из источника рисков в управляемый инструмент эффективности и безопасности.

Нейтрализация выявленных угроз и рисков возможна лишь при комплексном подходе, который сочетает технические средства защиты с продуманными организационными процедурами и регулярным повышением осведомлённости сотрудников. Снижение уязвимостей в работе с цифровыми профилями требует построения многоуровневой системы безопасности, опирающейся на ряд базовых практик, среди которых ключевыми являются следующие:

1) Предоставление сотрудникам прав доступа строго в пределах их функциональных обязанностей, что позволяет ограничить распространение чувствительной информации и снизить потенциальный ущерб при компрометации учётной записи;

2) Обязательное внедрение многофакторной аутентификации для доступа к критически важным системам, что особенно важно в контексте действующих регуляторных требований и растущего числа атак с применением украденных учётных данных;

3) Для защиты данных при передаче и хранении использование сквозного шифрования. Вся информация, включая персональные данные сотрудников, техническую документацию и коммерческие тайны, шифруются как при передаче по сетям, так и при хранении на серверах и конечных устройствах;

4) Разработка и внедрение четких политик информационной безопасности является фундаментом организационных мер. Эти политики детально регламентируют порядок работы с цифровыми профилями, определяют уровни доступа для различных категорий сотрудников и устанавливают процедуры обработки инцидентов;

5) Создание системы инцидент-менеджмента позволяет оперативно реагировать на нарушения. Четкие процедуры включают идентификацию инцидента, его изоляцию, устранение последствий и проведение расследования для предотвращения подобных случаев в будущем;

6) Проведите разделение доменов данных. Хранение персональных, кадровых и производственных метрик должно вестись обособленно друг от друга;

7) Обеспечение прозрачности и информированного согласия является ключевым этическим требованием. Сотрудники должны быть полностью проинформированы о том, какие данные собираются, как они обрабатываются и с какой целью. Сбор и обработка данных осуществляются только с добровольного и информированного согласия работников;

8) Соблюдение принципа соразмерности и минимальной достаточности гарантирует, что собираются только те данные, которые действительно необходимы для заявленных целей. Необходимо сформировать перечень законных целей профилирования (матрицы компетенций, охрана труда и др.) и привязать к каждой цели строго необходимый перечень атрибутов и характеристик, отражающих её. Объем и детализация собираемой информации должны быть минимально необходимыми для достижения поставленных целей;

9) Обязательное наличие резервных профилей и данных. В результате различных технических сбоев в деятельности предприятия существует вероятность повреждения или утраты части данных профилей. Поэтому во избежание потенциальных проблем в работе цифровых профилей на предприятии, вызванных повреждением данных, необходимо производить регулярные бэкапы своих систем и баз данных.

Использование цифровых профилей персонала в машиностроительной отрасли представляет собой мощный инструмент повышения эффективности и безопасности производственных процессов. Однако, его успешное внедрение требует сбалансированного подхода, сочетающего технические меры защиты, организационные процедуры и этические принципы. Технические меры бессильны без этики и подотчётности: работник должен понимать, какие выводы делает система, иметь право их оспорить и влиять на границы их наблюдения. Соблюдение требований законодательства, реализация многоуровневой системы безопасности и формирование культуры ответственного обращения с данными позволят максимально использовать преимущества цифровизации при минимизации сопутствующих рисков, обеспечивая устойчивое развитие предприятий в условиях цифровой экономики. Компании, которые стабильно совмещают правовые требования, техническую гигиену и участие людей, получают конкурентное преимущество: они извлекают пользу из аналитики, не превращая производство в поле «тотального контроля» и не подвергая бизнес утечкам и регуляторным санкциям.

**Список источников**

1. Российская Федерация. Законы. Трудовой кодекс Российской Федерации: ТК РФ N 197-ФЗ : текст в редакции от 29.09.2025 [принят Государственной Думой 21 декабря 2001 года : одобрен Советом Федерации 26 декабря 2001 года] — Москва. — 2001. — 244 с. — Текст: непосредственный.

2. Российская Федерация. Законы. О персональных данных: Федеральный закон N 152-ФЗ : текст в редакции от 24.06.2025 : [принят Государственной Думой 8 июля 2006 года : одобрен Советом Федерации 14 июля 2006 года] — Москва. — 2006. — 46 с. — Текст: непосредственный.

3. Российская Федерация. Законы. О коммерческой тайне: Федеральный закон N 98-ФЗ : текст в редакции от 08.08.2024 [принят Государственной Думой 9 июля 2004 года :

одобрен Советом Федерации 15 июля 2004 года] — Москва. — 2004. — 7 с. — Текст: непосредственный.

4. Российская Федерация. Постановления Правительства. Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации : Постановление Правительства РФ № 687 — Москва — 2008. — 3 с. — Текст: непосредственный.

5. Приказ Роскомнадзора : Об утверждении требований и методов по обезличиванию персональных данных : Приказ № 140 от 19.06.2025 : [зарегистрировано в Минюсте России 31.07.2025 N 83110] — Москва. — 2025. — 5 с. — Текст: непосредственный.

6. Приказ ФСТЭК : Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных : Приказ N 21 : текст в редакции от 14.05.2020 : [зарегистрировано в Минюсте России 14.05.2013 N 28375] — Москва. — 2013. — 15 с. — Текст: непосредственный.

7. Апелляционное определение Московского городского суда от 06.09.2017 N 33-33167/2017 — Москва, 2017 — URL: https://mos-gorsud.ru/mgs/cases/docs/content/ba917112-8d49-427f-a66e-a54e00a3b10f (дата обращения: 11.11.2025). — Текст: электронный.

8. Воробьева, М. А. Промышленный шпионаж как угроза экономической безопасности предприятия / М. А. Воробьева. — Текст: непосредственный // Молодой ученый. — 2019. — № 48 (286). — С. 353-356. — URL: https://moluch.ru/archive/286/64528/ (дата обращения: 07.11.2025).

9. Давудова С.Я., Рагимханова К.Т. Практика использования цифрового профиля: правовые риски и вызовы / — Текст: непосредственный // Закон и право — 2025. — №8. — URL: https://cyberleninka.ru/article/n/praktika-ispolzovaniya-tsifrovogo-profilya-pravovye-riski-i-vyzovy (дата обращения: 11.11.2025). — Текст: электронный.

10. РБК: информационный портал [сайт]. – Москва, 2019 – URL: https://www.rbc.ru/business/27/08/2019/5d6544519a79475d51ee7532?from=share (дата обращения: 07.11.2025). – Текст: электронный.

11. ТАСС: информационное агентство России: [сайт]. — Москва, 2019 — URL: https://tass.ru/ekonomika/6658004 (дата обращения: 10.11.2025). — Текст: электронный.

12. ТАСС: информационное агентство России: [сайт]. — Москва, 2019 — URL: https://tass.ru/ekonomika/6957393?ysclid=mfqlrl5al456435280) (дата обращения: 11.11.2025). — Текст: электронный.

13. Kuzmin A., Kuligina N. Research of the work of ransomware malware based on INTEL SGX // Norwegian Journal of Development of the International Science. — 2022. — №78-1. — URL: https://cyberleninka.ru/article/n/research-of-the-work-of-ransomware-malware-based-on-intel-sgx (дата обращения: 10.11.2025).

14. SecurityLab.ru: информационный портал: [сайт] — Москва, 2023 — URL: https://www.securitylab.ru/news/541485.php?ysclid=mfmdfczzki24640665 (дата обращения: 11.11.2025). — Текст: электронный.

15. SecurityLab.ru: информационный портал: [сайт] — Москва, 2022 — URL: https://www.securitylab.ru/news/530695.php (дата обращения: 10.11.2025). — Текст: электронный.

## Сведения об авторах

**Життеев Тимур Юрьевич,** аспирант, Московский государственный технический университет имени Н.Э. Баумана, Москва, Россия.

**Старожук Евгений Андреевич**, к.э.н., доцент, зав. каф. «Менеджмент», Московский государственный технический университет имени Н.Э. Баумана, Москва, Россия.

## Information about the authors

**Zhitteev Timur Yuryevich,** Postgraduate Student, Bauman Moscow State Technical University, Moscow, Russia.

**Evgeny Andreevich Starozhuk,** PhD in Economics, Associate Professor, Head of the Department of Management, Bauman Moscow State Technical University, Moscow, Russia.