Дата поступления рукописи в редакцию: 01.10.2026 г. DOI: 10.24412/2224-9133-2026-10-642-646
Дата принятия рукописи в печать: 10.11.2026 г.

ЗАКИРОВА Альфия Резавановна,
профессор кафедры «Техносферная безопасность» Уральского государственного университета путей сообщения, доктор технических наук, доцент,
e-mail: AZakirova@usurt.ru

ПРАВОВАЯ БАЗА КАК ОСНОВА РЕГУЛИРОВАНИЯ ЭЛЕКТРОБЕЗОПАСНОСТИ ПЕРСОНАЛА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Аннотация. *В статье рассматривается нормативно-правовая база, регулирующая электробезопасность персонала, занятого в сфере информационных технологий. Раскрывается проблема правовой квалификации ИТ-специалистов – отнесения их к электротехническому, электротехнологическому или неэлектротехническому персоналу – и вытекающие из этого последствия для обучения, допуска и ответственности. Анализируются применимые нормативные акты, частноправовые аспекты (трудовой договор, удалённая работа, гражданско-правовые договоры), а также организационные механизмы на уровне предприятия. Отдельное внимание уделено современным подходам к решению проблем: цифровизации документооборота, применению искусственного интеллекта для предиктивной аналитики, актуализации нормативной базы и риск-ориентированному надзору.*

Ключевые слова: *электробезопасность, ИТ-персонал, системный администратор, электротехнологический персонал, серверное оборудование, дистанционные работники, цифровизация охраны труда.*

Для цитирования: *Закирова А. Р. Правовая база как основа регулирования электробезопасности персонала информационных технологий // Право и управление. 2026. № 10. С. 642–646.*

ZAKIROVA Alfiya Rezavanovna,
Professor at the Department of Technospheric Safety, Ural State University of Railway Transport, Doctor of Technical Sciences, Associate Professor

THE LEGAL FRAMEWORK AS THE BASIS FOR REGULATING ELECTRICAL SAFETY OF IT PERSONNEL

Annotation. *The article examines the regulatory and legal framework governing electrical safety for personnel working in the information technology sector. It addresses the problem of the legal classification of IT specialists — namely, their attribution to electrical, electrotechnological, or non-electrical personnel — and the resulting implications for training, authorization, and liability. The paper analyses applicable regulations, private-law aspects (employment contracts, remote work, civil-law agreements), as well as organisational mechanisms at the enterprise level. Special attention is given to modern approaches to solving these problems: digitalisation of document management, the use of artificial intelligence for predictive analytics, updating the regulatory framework, and risk-based supervision.*

Key words: *electrical safety, IT personnel, system administrator, electrotechnological personnel, server equipment, remote workers, digitalisation of occupational safety.*

For citation: *Zakirova A. R. The legal framework as the basis for regulating electrical safety of it personnel. Law and administration. 2026;(10):642–646. (In Russ.).*

Специфика ИТ персонала в системе электробезопасности. Сотрудники информационных технологий занимают особое положение в системе регулирования электробезопасности. Традиционно ИТ специалистов не относят к электротехническому персоналу, однако их повседневная деятельность неразрывно связана с эксплуатацией оборудования, подпадающего под действие нормативных документов в сфере электробезопасности: серверных стоек, источников бесперебойного питания (ИБП), телекоммуникационных шкафов, кабельных трасс, систем охлаждения и электропитания.

Ключевая правовая проблема состоит в определении категории, к которой относится тот или иной работник. Согласно Правилам по охране труда при эксплуатации электроустановок, утверждённым приказом Минтруда России от 15.12.2020 № 903н, весь персонал подразделяется на три группы: неэлектротехнический, электротехнический и электротехнологический. Решение об отнесении конкретного ИТ сотрудника к той или иной категории принимает руководитель организации, опираясь на характер выполняемых работ и положения нормативных актов. Это порождает зону правовой неопределённости: одни работодатели классифицируют системных администраторов как неэлектротехнический персонал (I группа), другие — как электротехнологический (II–III группы), что напрямую определяет требования к обучению, допуску и уровню ответственности. По сути, определяющим фактором служит не должность, а реальное содержание трудовой функции.

I группа — разработчики, тестировщики, дизайнеры, менеджеры и иные сотрудники, взаимодействующие с офисной техникой (компьютеры, принтеры, мониторы). Группа присваивается по итогам ежегодного инструктажа; удостоверение не оформляется, запись вносится в специальный журнал.

II группа — системные администраторы, DevOps инженеры, выполняющие работы с серверным оборудованием, коммутационными шкафами, ИБП. Подтверждается проверкой знаний в комиссии предприятия.

III группа и выше — специалисты, обслуживающие оборудование напряжением свыше 1000 В либо выполняющие работы, предполагающие право единоличного осмотра электроустановок.

Нормативные документы, применимые к ИТ сфере. Правовое регулирование электробезопасности ИТ персонала опирается на комплекс нормативных актов:

Трудовой кодекс РФ — закрепляет обязанности работодателя по обеспечению безопасных условий труда (ст. 212, 214) [1].

ПТЭЭП, утверждённые приказом Минэнерго России от 12.08.2022 № 811, — устанавливают требования к организации эксплуатации, назначению ответственных лиц, подготовке персонала. Документ распространяется на юридических лиц, индивидуальных предпринимателей и физических лиц, владеющих электроустановками [2].

Правила по охране труда при эксплуатации электроустановок (приказ Минтруда России от 15.12.2020 № 903н) — определяют категории персонала, требования к группам по электробезопасности, порядок оформления нарядов допусков [3].

ГОСТ IEC 60950 1 2014 «Оборудование информационных технологий. Требования безопасности» — устанавливает требования к защите пользователей и обслуживающего персонала от поражения электрическим током, разделяя доступ к оборудованию на зоны для пользователей и зоны ограниченного доступа для обслуживающего персонала [4].

ГОСТ IEC 62040 1 2024 «Системы бесперебойного энергоснабжения (UPS). Требования безопасности» — регламентирует безопасность ИБП, включая требования к квалифицированному и неквалифицированному персоналу. Стандарт введён в действие с 1 апреля 2026 года с правом досрочного применения. [5]

ПУЭ (7 е издание) — нормы проектирования и монтажа, влияющие на безопасность эксплуатации [6].

Серверное оборудование может классифицироваться как электротехнологическое, что автоматически распространяет на него требования ПТЭЭП. ИТ специалистов, выполняющих работы в серверной, целесообразно относить к оперативному электротехнологическому персоналу, занятому техническим обслуживанием оборудования, с составлением перечня работ, выполняемых в порядке текущей эксплуатации.

Частноправовые аспекты применительно к ИТ персоналу. С позиций частноправовых наук регулирование электробезопасности ИТ персонала затрагивает несколько аспектов.

Трудовой договор и должностная инструкция. В трудовом договоре с системным администратором, инженером эксплуатации центра обработки данных (ЦОД), DevOps специалистом должны быть чётко определены обязанности, связанные с работой в электроустановках. Отсутствие в должностной инструкции указания на работу с электрооборудованием не освобождает работодателя от ответственности, но порождает правовую неопределённость при расследовании несчастных случаев.

Дистанционные работники. Острая проблема — электробезопасность удалённых ИТ сотрудников. ПТЭЭП в редакции 2022 года распространил требования и на физических лиц, ис-

пользующих электроустановки в рабочих целях, включая удалённых работников. Работодатель обязан провести инструктаж и зафиксировать факт ознакомления, однако присвоение I группы по электробезопасности дистанционным работникам пока не оформляется в электронной форме с использованием КЭДО — журналы должны подписываться собственноручно [7].

Гражданско правовые договоры (подряд, аутсорсинг). При привлечении внешних ИТ подрядчиков для обслуживания серверной стороны распределяют риски через условия договора: требования к квалификации персонала, наличию групп по электробезопасности, использованию средств защиты. Однако гражданско правовая квалификация договора не освобождает заказчика от обязанности обеспечить безопасные условия на своей территории.

Организационно правовые механизмы для ИТ подразделений

На уровне предприятия регулирование реализуется через следующие инструменты:

Приказ о назначении ответственного за электрохозяйство. Для организаций с электроустановками до 1000 В ответственный должен иметь группу не ниже IV. Если в штате нет квалифицированного специалиста, допускается заключение договора со специализированной организацией.

Перечень должностей и работ. Руководитель приказом утверждает перечень должностей электротехнического и электротехнологического персонала, которым необходимо иметь соответствующую группу по электробезопасности. ИТ должности включаются в перечень на основе анализа фактических обязанностей.

Обучение и проверка знаний. ИТ специалисты со II группой и выше проходят проверку знаний в комиссии предприятия (не реже 1 раза в год для оперативного персонала и 1 раза в 3 года для административно технического).

Журналы и документация. Журнал учёта присвоения I группы, журнал инструктажей по охране труда, протоколы проверки знаний, удостоверения о проверке знаний — обязательный минимум для ИТ компаний.

Перечень работ в порядке текущей эксплуатации. Для ИТ специалистов, обслуживающих серверное оборудование, составляется перечень работ, выполняемых без наряда допуска (осмотр, регулировка, замена модулей с отключением питания).

Проблемы правоприменения в ИТ сфере. Анализ практики позволяет выделить специфические проблемы:

Правовая неопределённость статуса ИТ персонала. Отсутствие прямого указания в нормативных документах на отнесение системных администраторов к электротехнологическому персоналу создаёт риск различной трактовки надзорными органами.

Формальный подход к инструктажам. В малых ИТ компаниях инструктажи по электробезопасности нередко проводятся номинально, без учёта реальных опасностей серверной.

Отсутствие ответственного за электрохозяйство. Во многих ИТ компаниях эта должность не назначена или существует лишь «на бумаге», что является прямым нарушением ПТЭЭП.

Дистанционные работники. Неурегулированность процедуры инструктажа удалённого ИТ персонала в электронной форме создаёт юридический риск для работодателей.

Сложность адаптации требований к современным технологиям. Стандарты ГОСТ IEC 60950 1 2014 и ГОСТ IEC 62040 1 2024 устанавливают требования к оборудованию, но не регулируют порядок работы персонала с этим оборудованием, что формирует разрыв между техническими нормами и организационными требованиями.

Современные способы решения проблем. Проблемы правового регулирования электробезопасности ИТ персонала сегодня получают новые решения — технологические, организационные и нормативные.

Цифровизация документооборота и контроля. С 1 марта 2026 года надзорные органы в сфере охраны труда перешли на цифровые формы контроля через Единую цифровую платформу надзора (ЕЦПН). Бумажные проверки отменены, электронный документооборот стал обязательным. Для ИТ компаний доступны специализированные программные решения: модули электробезопасности в системах 1С:EHS и «Охрана труда для 1С» (ОТ Софт) ведут учёт оборудования, планируют проверки и обучение персонала, формируют приказы, удостоверения, протоколы и чек листы Ростехнадзора. Автоматизированные системы еженедельно формируют отчёты с цветовой индикацией сроков аттестации, исключая пропуск или просрочку проверки знаний. Важно учитывать правовую границу: инструктажи по электробезопасности (присвоение I группы) пока не допускается оформлять в системе КЭДО с электронной подписью — журналы должны подписываться собственноручно. Однако приказы, инструкции, перечни должностей можно вести в электронном виде [8].

ИИ системы предиктивной аналитики и мониторинга. Интеллектуальные системы мониторинга на базе IoT датчиков и алгоритмов машинного обучения непрерывно собирают данные о состоянии ИБП, серверного оборудования, кабельных линий — температуру, уровень изоляции, параметры тока и напряжения. Системы выявляют аномалии, которые человек не замечает, и

предсказывают аварии за часы и дни до их возникновения. Для ИТ инфраструктуры это особенно актуально: ИБП с аккумуляторными батареями представляет один из наиболее опасных узлов с точки зрения электробезопасности.

Актуализация нормативной базы. ПТЭЭП в редакции 2022 года расширил сферу применения требований, включив физических лиц, использующих электроустановки в рабочих целях, в том числе удалённых работников. С 1 марта 2026 года действуют новые требования Ростехнадзора по электробезопасности — обновлённые группы, требования к теоретическим и практическим тестам, порядок формирования комиссий. Федеральным законом № 304 ФЗ расширен перечень случаев, когда проверку знаний проводит комиссия Ростехнадзора. Цифровая маркировка средств индивидуальной защиты в системе «Честный знак» становится обязательной, закупка немаркированных СИЗ запрещена. Профилактические визиты заменяют плановые проверки для низкорисковых объектов — новая форма надзора, направленная на предупреждение нарушений без штрафных санкций [9].

Риск ориентированный подход и непрерывный контроль. Современная модель управления электробезопасностью ИТ персонала строится на переходе от бумажной отчётности к непрерывному цифровому контролю. Автоматизированный расчёт риска травмирования персонала предприятий на основе данных о несчастных случаях, условиях труда, прохождении обучения позволяет надзорным органам определять категории риска и применять дифференцированный подход. [10].

Заключение. Нормативно правовая база электробезопасности ИТ персонала представляет собой многоуровневую систему, сочетающую публично правовые требования и частноправовые обязательства. Специфика ИТ сферы — в правовой неопределённости статуса персонала, что требует от работодателя взвешенного подхода к классификации должностей, оценке рисков и оформлению локальных актов.

Современные способы решения проблем — цифровизация документооборота, ИИ мониторинг, актуализация нормативной базы, риск ориентированный надзор — позволяют перейти от формального выполнения требований к реальному снижению электротравматизма. Для ИТ руководителей и специалистов по охране труда критически важно своевременно определять категории персонала, присваивать соответствующие группы по электробезопасности и поддерживать документацию в актуальном состоянии, учитывая изменения нормативной базы.

Список литературы:

[1] Трудовой кодекс Российской Федерации от 30.12.2001 № 197 ФЗ.

[2] Правила технической эксплуатации электроустановок потребителей электрической энергии, утв. приказом Минэнерго России от 12.08.2022 № 811.

[3] Правила по охране труда при эксплуатации электроустановок, утв. приказом Минтруда России от 15.12.2020 № 903н.

[4] ГОСТ IEC 60950 1 2014. Оборудование информационных технологий. Требования безопасности. Часть 1. Общие требования.

[5] ГОСТ IEC 62040 1 2024. Системы бесперебойного энергоснабжения (UPS). Часть 1. Общие положения и требования безопасности к UPS.

[6] Правила устройства электроустановок (ПУЭ), 7 е издание.

[7] Электронные инструктажи по ОТ: готовимся к изменениям [https://www.ot-soft.ru/articles/yelektronnye-instruktazhi-po-ot-gotovims] // OT-Soft. — URL: (дата обращения: 01.10.2026).

[8] С 1 марта 2026 года органы в сфере охраны труда переходят на цифровые формы контроля [https://kodeks-sib.ru/blog/s_1_marta_2026_goda_organyi_v_sfere_oxranyi_truda_perexodyat_na_czifrovyie_formyi_kontrolya] // Кодекс-Сиб : блог. — URL: (дата обращения: 01.10.2026).

[9] Новый порядок проверки знаний по электробезопасности — 2026 [https://obrprofi.ru/novosti/novyj-poryadok-proverki-znanij-elektrobezopasnost-2026.html] // ОбрПрофи : новости. — URL: (дата обращения: 01.10.2026).

[10] Новый порядок проверки знаний по электробезопасности [https://ohranatruda125.ru/tpost/vtbib6s7g1-novii-poryadok-proverki-znanii-po-elektr] // Охрана труда 125 : публикации. — URL: (дата обращения: 01.10.2026).

References:

[1] Labor Code of the Russian Federation dated 30.12.2001 No. 197 FZ.

[2] Rules for technical operation of electrical installations of electrical energy consumers, approved by Order of the Ministry of Energy of the Russian Federation No. 811 dated 12.08.2022.

[3] Occupational Safety Rules for Operation of Electrical Installations, approved by order of the Ministry of Labor of Russia dated 15.12.2020 No. 903n.

[4] GOST IEC 60950 1 2014. Information technology equipment. Safety requirements. Part 1. General requirements.

[5] GOST IEC 62040 1 2024. Uninterruptible Power Supply (UPS) systems. Part 1. UPS General and Safety Requirements.

[6] Electrical Installation Code (EIC), 7th edition.

[7] EHS e-Briefing: Getting Ready for Change [https://www.ot-soft.ru/articles/yelektronnye-instruktazhi-po-ot-gotovims] // OT-Soft. - URL: (access date: 01.10.2026).

[8] From March 1, 2026, labor protection authorities will switch to digital forms of control [https://kodeks-sib.ru/blog/s_1_marta_2026_goda_organyi_v_sfere_oxranyi_truda_perexodyat_na_czifrovyie_formyi_kontrolya] // Codex-Sib: blog. - URL: (access date: 01.10.2026).

[9] New procedure for testing knowledge on electrical safety - 2026 [https://obrprofi.ru/novosti/novyj-poryadok-proverki-znanij-elektrobezopasnost-2026.html] // ObrProfi: news. - URL: (access date: 01.10.2026).

[10] New procedure for testing electrical safety knowledge [https://ohranatruda125.ru/tpost/vtbib6s7g1-novii-poryadok-proverki-znanii-po-elektr] // Occupational safety 125: publications. - URL: (access date: 01.10.2026).

