УДК 004.056

ПРОВЕРКА БЛАГОНАДЕЖНОСТИ СОТРУДНИКА ПРИ ПРИЕМЕ НА РАБОТУ: ПРАВОВЫЕ ОГРАНИЧЕСНИЯ И ПРАКТИЧЕСКИЕ ВОЗМОЖНОСТИ

Котанджян А.В.
кандидат экономических наук,
Вятский государственный университет,
Киров, Россия

Валова Н.А.
студент 4 курса,
Вятский государственный университет,
Киров, Россия

Опарина Э.Н.
студент 4 курса,
Вятский государственный университет,
Киров, Россия

Прозорова С.С.
студент 4 курса,
Вятский государственный университет,
Киров, Россия

Аннотация

В статье исследуются правовые и организационные аспекты проверки благонадёжности сотрудников при приёме на работу в контексте обеспечения информационной безопасности хозяйствующего субъекта. Целью работы является систематизация разрешённых и запрещённых методов сбора

информации о кандидате, а также разработка практического алгоритма, позволяющего минимизировать инсайдерские риски без нарушения законодательства о персональных данных. Продемонстрировано, что, несмотря на ограничения Трудового кодекса и Федерального закона №152-ФЗ, работодатель располагает набором легальных инструментов. Выявлены методы, находящиеся под прямым запретом. Сделан вывод, что эффективная оценка благонадёжности достигается не за счёт нарушения закона, а благодаря последовательному применению пошагового алгоритма, что позволяет снизить риск приёма инсайдеров и одновременно служит доказательством добросовестности работодателя при возможных судебных разбирательствах.

Ключевые слова: благонадёжность сотрудника, инсайдерские угрозы, персональные данные, проверка кандидатов, трудовое законодательство, кадровая безопасность.

EMPLOYEE TRUSTWORTHINESS CHECK WHEN APPLYING FOR A JOB: LEGAL CONSTRAINTS AND PRACTICAL POSSIBILITIES

Kotanjyan A.V.
Candidate of Economic Sciences
Vyatka State University,
Kirov, Russia

Valova N.A.
4th year student,
Vyatka State University,
Kirov, Russia

Oparina E.N.
4th year student,

Vyatka State University,
Kirov, Russia

Prozorova S.S.
4th year student,
Vyatka State University,
Kirov, Russia

Abstract

The article examines the legal and organizational aspects of employee trustworthiness verification when applying for a job in the context of ensuring the information security of an economic entity. The aim of the work is to systematize the permitted and prohibited methods of collecting information about a candidate, as well as to develop a practical algorithm that minimizes insider risks without violating the legislation on personal data. It has been demonstrated that, despite the limitations of the Labor Code and Federal Law No. 152-FZ, the employer has a set of legal tools. Methods that are directly prohibited have been identified. It is concluded that an effective assessment of trustworthiness is achieved not by violating the law, but by consistently applying a step-by-step algorithm, which reduces the risk of receiving insiders and at the same time serves as proof of the employer's integrity in possible court proceedings.

Keywords: employee trustworthiness, insider threats, personal data, candidate verification, labor legislation, personnel security.

Современная организация любой отрасли сталкивается с проблемой внутренних угроз информационной безопасности. По данным аналитических отчётов, от 60 до 80% инцидентов, связанных с утечкой конфиденциальных данных, происходят при участии сотрудников – как умышленно, так и по

неосторожности. Как отмечает А.В. Поляков, персонал организации одновременно выступает и основным ресурсом, и главным источником угроз информационной безопасности [12]. Особенно уязвимыми становятся компании в моменты приёма нового персонала, когда ещё не сформировано доверие, а доступ к корпоративным ресурсам уже требуется для выполнения должностных обязанностей. Т.Н. Виноградова подчёркивает, что подбор благонадёжных сотрудников – ключевая задача кадровой безопасности предприятия [6]. В этих условиях закономерно возникает запрос на предварительную оценку благонадёжности кандидата: отсутствие судимостей за экономические преступления, отрицательных рекомендаций с предыдущих мест работы, связей с конкурентами или криминальными структурами. И.В. Мешкова также указывает, что кадровая безопасность является важнейшим элементом национальной безопасности [10], а коллектив авторов под руководством А.В. Ивашкиной выделяет инсайдерские угрозы как наиболее опасные для организаций [8].

Понятие «благонадёжность сотрудника» не имеет единого закреплённого определения. В широком смысле, как отмечает М. А. Молчанов, кадровая безопасность — это состояние защищённости персонала от внутренних и внешних угроз, а благонадёжность выступает интегральной характеристикой лояльности и добросовестности работника [11].

В контексте информационной безопасности С. В. Глухарева определяет уровень благонадёжности сотрудника как уровень владения компетенциями, отражающими все аспекты его деятельности [7]. Благонадёжный сотрудник — это не только лояльный работник, но и профессионал, чьи знания, навыки и поведенческие установки соответствуют требованиям должности и политике информационной безопасности. А.В. Ивашкина и У.П. Лебедева предлагают методы профилактики кадровых угроз, включая проверку благонадёжности [9].

Таким образом, благонадёжность в контексте ИБ можно определить как интегральную характеристику сотрудника, отражающую его способность и

готовность соблюдать правила работы с информацией и не допускать действий, ведущих к её утечке или компрометации.

Однако в Российской Федерации право на информацию о соискателе ограничено. Конституция Российской Федерации гарантирует каждому право на неприкосновенность частной жизни, что накладывает ограничения на сбор данных о кандидатах [1]. Трудовой кодекс (ст. 86–90) [2] и Федеральный закон «О персональных данных» (№152-ФЗ) [3] устанавливают чёткие рамки: работодатель может собирать только те сведения, которые непосредственно относятся к профессиональным качествам и необходимы для принятия решения о приёме. Любые действия, выходящие за эти пределы (запрос справок о судимости без законного основания, сбор биометрических данных без отдельного согласия, негласный мониторинг социальных сетей с нарушением приватности), грозят административными штрафами и судебными исками о дискриминации [4] . Сложность заключается в том, что многие руководители и HR-специалисты либо пренебрегают проверками из-за правовых рисков, либо, наоборот, нарушают закон, пытаясь защитить компанию. В результате нивелируется сам смысл оценки благонадёжности, а реальные инсайдеры попадают в штат незамеченными.

И всё же закон оставляет работодателю несколько легальных способов получить информацию о кандидате. Первый и самый очевидный из них – изучение открытых источников. Работодатель вправе изучать общедоступные сведения о кандидате – те, которые тот разместил самостоятельно без ограничений доступа. Это могут быть профили в социальных сетях (ВКонтакте, Telegram, профессиональное сообщество на Habr), публикации в СМИ, комментарии на форумах, а также данные из государственных реестров: ЕГРЮЛ, ЕГРИП, картотека арбитражных дел, Федеральный ресурс сведений о банкротстве. Например, если кандидат значится учредителем компании-конкурента или фигурирует в судебных спорах о присвоении имущества – эта информация легально доступна и может быть использована для принятия

решения. Единственное ограничение: нельзя пытаться получить доступ к закрытым постам или личным сообщениям, взламывать аккаунты или использовать данные, которые человек скрыл в настройках приватности. Такие действия уже попадают под статью 138 УК РФ (нарушение тайны переписки).

От открытых источников логично перейти к информации, которую можно получить напрямую от предыдущих работодателей. Здесь ключевую роль играет письменное согласие самого кандидата. Статья 86 ТК РФ разрешает направлять запросы на прошлые места работы – но только если соискатель подписал добровольное согласие [2] . В таком запросе можно уточнить: период работы, должность, причину увольнения, а главное – были ли зафиксированы факты разглашения конфиденциальных данных или дисциплинарные взыскания за нарушение ИБ. Однако запрашивать медицинские данные, сведения о личной жизни или семейном положении запрещено даже при наличии согласия – такая информация считается избыточной.

Помимо характеристик, стоит убедиться в подлинности документов об образовании – и здесь закон также предоставляет легальный инструмент. Федеральная информационная система «Федеральный реестр сведений о документах об образовании» (ФИС ФРДО) позволяет любому работодателю проверить диплом. Формально это не требует отдельного согласия, так как сведения об образовании не относятся к категории «персональные данные ограниченного доступа». Тем не менее, лучшей практикой считается включить пункт о проверке диплома в общее согласие на обработку данных – это исключит даже гипотетические претензии.

Когда документальные подтверждения собраны, наступает этап живого общения – собеседования с участием специалиста по информационной безопасности. Закон не запрещает задавать вопросы о понимании ответственности за разглашение тайны, о знании фишинга, социальной инженерии, правил работы с паролями. Как отмечает Т.Н. Виноградова, на этом этапе эффективно использование психологических методов для выявления

личностных качеств кандидата [6]. Но важно помнить о запрете на дискриминацию (ст. 3 ТК РФ): нельзя спрашивать о религии, политике, беременности или членстве в профсоюзах. Такие вопросы – прямой путь к судебному иску.

Собеседование даёт качественную оценку, а количественные данные о связях кандидата можно получить через коммерческие сервисы проверки контрагентов. Системы СПАРК, Контур.Фокус или СБИС аккумулируют открытые данные из реестров. С их помощью легко выяснить, является ли соискатель действующим руководителем или учредителем других юрлиц, есть ли у этих фирм долги, банкротства, признаки «однодневок». Поскольку информация общедоступна, дополнительных разрешений не требуется, но добросовестный работодатель всё равно фиксирует этот пункт в согласии.

Наконец, самый узкий и осторожный метод – проверка судимости. Закон разрешает требовать справку о судимости только для должностей, прямо перечисленных в федеральных актах: педагоги, госслужащие, лица, получающие допуск к гостайне или работающие на критической информационной инфраструктуре (КИИ) [5]. Для обычного менеджера или программиста такой запрос – грубое нарушение, которое грозит штрафом и гарантированным судебным иском. Поэтому к этому методу следует прибегать исключительно в случаях, когда должность подпадает под законодательные исключения.

Таким образом, разрешённые методы позволяют получить информацию законно. Однако существуют методы, применение которых независимо от целей признаётся правонарушением.

Начнём с самого распространённого нарушения – сбора биометрических данных без отдельного согласия. Отпечатки пальцев, рисунок радужки, голос, фотографии для систем распознавания лиц (при автоматизированной обработке) – всё это биометрия. Статья 11 закона №152-ФЗ требует письменного согласия на каждую такую операцию, причём согласие должно

быть отдельным документом, а не пунктом в общей анкете [3] . Штраф по ст. 13.11 КоАП достигает 500 тыс. рублей [4] .

Не менее опасен метод негласного наблюдения – когда работодатель пытается следить за кандидатом скрытно. Наём частного детектива без лицензии, прослушивание разговоров, чтение переписки (даже если соискатель сам оставил телефон на столе) – всё это попадает под статью 138 УК РФ «Нарушение тайны переписки, телефонных переговоров и иных сообщений». Максимальное наказание – до двух лет лишения свободы, но даже в менее тяжких случаях слежка ведёт к крупным штрафам и дискредитации компании.

Ещё один спорный, но часто используемый метод – полиграф. Трудовой кодекс прямо его не запрещает, но требует абсолютной добровольности. Соискатель должен дать письменное согласие, причём с подробным перечнем вопросов, а также иметь право отказаться в любой момент. Если работодатель принуждает к тестированию или отказывает в приёме из-за отказа пройти «детектор лжи» – это дискриминация (ст. 3, 64 ТК РФ) [2] , подтверждённая десятками судебных решений. Штраф может достигать 50 тыс. рублей плюс компенсация морального вреда кандидату.

Похожая ситуация с медицинскими справками – психиатра, нарколога, о ВИЧ-статусе. Запрашивать их можно только для профессий, где это прямо предписано федеральным законом: водители, лётчики, некоторые производственные рабочие, сотрудники детских учреждений. Для офисного сотрудника, даже с доступом к коммерческой тайне, требовать психиатрическое освидетельствование – грубое нарушение ст. 88 ТК РФ (запрет на избыточные персональные данные) [2] . Штраф для юрлица – до 100 тыс. рублей [4] .

И наконец, проверка кредитной истории – абсолютное табу для любого работодателя. Кредитные истории охраняются специальным законом, и даже с согласия кандидата организация не имеет права делать запрос в БКИ – такие сведения предоставляются только самому гражданину или госорганам.

Единственный легальный способ – попросить соискателя самостоятельно принести выписку, но отказ в приёме из-за «плохой кредитной истории» будет признан дискриминацией, ведь долги не относятся к профессиональным качествам. Санкции: возмещение убытков кандидату и штраф до 200 тыс. рублей.

Таким образом, законодательство оставляет работодателю широкое поле для законной проверки (открытые источники, рекомендации, реестры, собеседования), но устанавливает жесткие запреты на биометрию, слежку, принудительный полиграф, избыточные медсправки и кредитные истории. Нарушение этих запретов – не просто риск, а почти гарантированные финансовые и репутационные потери. Для наглядности основные запреты и их последствия сведены в таблицу (таблица 1).

Таблица 1 – Запрещенные методы проверки и их последствия

Запрещённый метод	Нормативный акт	Типичное наказание
Сбор биометрии без отдельного согласия	ст. 11 152-ФЗ, ст. 13.11 КоАП	штраф до 500 000 руб.
Негласное наблюдение (слежка) без лицензии	ст. 138 УК РФ, закон о частном сыске	уголовная ответственность (до 2 лет лишения свободы)
Принудительный полиграф	ст. 3, 64 ТК РФ (дискриминация)	компенсация морального вреда + штраф до 50 000 руб.
Запрос избыточных медицинских справок	ст. 88 ТК РФ, ст. 13.11 КоАП	штраф на юрлицо до 100 000 руб.
Проверка кредитной истории без согласия	закон «О кредитных историях»	возмещение убытков + штраф до 200 000 руб.

Изложенные выше законодательные нормы создают формальную основу, но сами по себе не дают ответа на вопрос: как именно организовать проверку кандидата, чтобы она была одновременно законной и результативной? Для решения этой задачи предлагается пошаговый алгоритм, апробированный в

ряде организаций и учитывающий как правовые ограничения, так и реальные потребности службы безопасности.

Шаг первый – определение перечня должностей, подлежащих углублённой проверке. Не всех сотрудников имеет смысл проверять с одинаковой тщательностью. Критериями отбора выступают: доступ к персональным данным клиентов (CRM, 1С), доступ к коммерческой тайне или конструкторской документации, право подписи финансовых документов, а также участие в обслуживании критической информационной инфраструктуры [5] . Целесообразно закрепить этот перечень во внутреннем локальном акте, например в «Положении о порядке допуска сотрудников к конфиденциальной информации». Такой документ позволит избежать обвинений в выборочном или дискриминационном подходе.

После того как перечень должностей утверждён, следующим шагом становится разработка и подписание с кандидатом «Согласия на сбор и обработку персональных данных для целей проверки». Этот документ должен включать конкретные источники информации, которые работодатель намерен использовать: открытые социальные сети, государственные реестры, запросы на предыдущие места работы, а также проверку через коммерческие сервисы (СПАРК, Контур.Фокус). Важно, чтобы согласие не было «безразмерным» – в нём следует перечислить только те действия, которые действительно необходимы. Без такого согласия любой сбор информации о кандидате, за исключением общедоступных сведений, считается незаконным [2] .

Следующий этап – сбор и анализ информации из открытых источников, причём исключительно в рамках полученного согласия. Практические действия включают: просмотр публичных профилей в социальных сетях и профессиональных сообществах, поиск упоминаний кандидата в средствах массовой информации, а также проверку через системы «Контур.Фокус» или «СПАРК» на предмет регистрации в качестве индивидуального предпринимателя или учредителя юридических лиц. Дополнительно

проверяется картотека арбитражных дел (наличие судебных споров, связанных с присвоением имущества или разглашением тайны) и реестр дисквалифицированных лиц. Все результаты фиксируются в отчёте с указанием даты проверки – это необходимо для подтверждения законности действий при возможных претензиях. Как отмечает С.В. Глухарева с соавторами, использование таких открытых данных является неотъемлемой частью модели оценки благонадежности сотрудника [14] .

После завершения «кабинетной» проверки целесообразно перейти к сбору данных через предыдущих работодателей. Для этого на основании подписанного согласия готовится письменный запрос по форме, содержащей вопросы о периоде работы, должности, причине увольнения, а также – ключевой блок – о наличии дисциплинарных взысканий, связанных с разглашением конфиденциальной информации или нарушением правил работы с данными. А.В. Ивашкина и У.П. Лебедева включают этот метод в перечень основных при профилактике кадровых угроз [9] . Запрос направляется заказным письмом или через официальный электронный документооборот. Ответы на такие запросы не являются обязательными, но их отсутствие само по себе может служить косвенным признаком нежелания предыдущего работодателя давать рекомендации.

Параллельно или после получения ответов от прежних нанимателей проводится собеседование с участием специалиста по информационной безопасности. Его цель – не столько проверка формальных знаний, сколько выявление установок и ценностного отношения кандидата к вопросам защиты информации. Рекомендуемые вопросы: «Как вы понимаете ответственность за разглашение сведений, ставших известными вам на рабочем месте?», «Приходилось ли вам сталкиваться с фишинговыми атаками и как вы на них реагировали?», «Опишите случай, когда вы замечали нарушение правил ИБ со стороны коллег – как вы поступили?». Обработка ответов позволяет выделить так называемые «поведенческие маркеры»: оправдание нарушений, агрессию

на вопросы о безопасности, непонимание базовых угроз. С.В. Глухарева (2022 г.) предлагает оценивать благонадежность именно через компетенции, что включает и поведенческие аспекты [7] . В работе 2024 года этот подход детализирован с использованием весовых коэффициентов [13] . Такие признаки повышают риски и могут служить основанием для решения о нецелесообразности приёма на должность, связанную с доступом к конфиденциальной информации.

Итогом всех перечисленных шагов становится подготовка письменного заключения о благонадёжности кандидата. В нём выделяются три возможных решения:

- рекомендован – по всем проверкам замечаний нет, риски минимальны;
- условно рекомендован – выявлены незначительные риски (например, частые смены работы без объяснения причин, отсутствие рекомендаций); такому кандидату может быть установлен испытательный срок с ограниченным доступом к наиболее чувствительным данным;
- не рекомендован – обнаружены факты сокрытия информации, отрицательные рекомендации, участие в судебных спорах о разглашении тайны или аффилированность с конкурентами.

  А.В. Поляков подчёркивает, что системная работа с персоналом, включая оценку при приёме, позволяет снизить долю инцидентов, связанных с человеческим фактором [12] .

Заключение носит рекомендательный характер; окончательное решение о приёме остаётся за руководителем организации или уполномоченным должностным лицом. Однако документированная процедура проверки существенно снижает риск принятия на работу потенциального инсайдера и одновременно служит доказательством добросовестности работодателя в случае судебных разбирательств.

Таким образом, предложенный алгоритм (определение круга должностей → получение согласия → проверка открытых источников → запрос

рекомендаций → профильное собеседование → оформление заключения) позволяет проводить оценку благонадёжности в полном соответствии с законодательством и при этом получать информацию, достаточную для обоснованного кадрового решения. Как показывают исследования С.В. Глухаревой и коллег, внедрение подобных методик на предприятиях критической информационной инфраструктуры подтверждает их эффективность [7, 13, 14] .

Библиографический список:

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020).
2. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ (ред. от 06.04.2024).
3. Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 06.04.2024) «О персональных данных».
4. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (ред. от 22.04.2024).
5. Постановление Правительства РФ от 12.10.2020 № 1495 «О требованиях к обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».
6. Виноградова Т.Н. Обеспечение информационной безопасности предприятия при работе с персоналом // Научный журнал. — 2023.
7. Глухарева С.В. Метод оценки уровня благонадежности сотрудников в системе кадровой безопасности предприятия (на примере предприятий критической информационной инфраструктуры (КИИ) // Доклады ТУСУР. 2022. №2.

8. Ивашкина А.В. [и др.] Оценка инсайдерских угроз в системе кадровой безопасности организации // Экономическая безопасность. — 2022. — № 4. — С. 36–40.
9. Ивашкина А.В., Лебедева У.П. Угрозы в кадровой безопасности и методы по их предотвращению // Евразийский союз ученых. — 2018. — № 4-6(49). — С. 71–77.
10. Мешкова И.В. Кадровая безопасность в системе национальной безопасности России // Миссия конфессий. — 2021. — Т. 10. — № 8(57). — С. 907–913.
11. Молчанов М.А. Кадровая безопасность как элемент экономической безопасности предприятий производственных отраслей // Мир современной науки. — 2014. — № 3(25). — С. 71–73.
12. Поляков А.В. Место и роль персонала в информационной безопасности организации // Вестник МГТУ «Станкин». — 2013. — № 2. — С. 112–116.
13. Глухарева С.В., Немирович-Данченко М.М., Шелупанов А.А. Выбор весовых коэффициентов для модели оценки уровня благонадежности сотрудников в системе кадровой безопасности на предприятиях критической информационной инфраструктуры (КИИ) // Известия ВУЗов ЭФиУП. 2024. №3 (61).
14. Шелупанов А.А., Глухарева С.В. Немирович-Данченко М.М. Оценка благонадежности сотрудника в системе кадровой безопасности предприятия // Доклады ТУСУР. 2021. №4.