

## **ПРИМЕНЕНИЕ МЕЖДУНАРОДНОГО ОПЫТА В РАБОТЕ С КАДРАМИ КАК ОСНОВНОЙ СПОСОБ СОХРАНЕНИЯ КОММЕРЧЕСКОЙ ТАЙНЫ В ИТ-КОМПАНИИ**

**И. В. Шоломицкая,**  
юрисконсульт ООО «Дейлорент»  
магистр юридических наук

1. Современные тенденции мирового развития связаны с переходом общества к постиндустриальной стадии развития экономики, главную роль в которой играют информационные технологии. В развитых странах 80 – 95 % прироста ВВП приходится на долю новых знаний, воплощенных в технике и технологиях.

Подъем ИТ-отрасли наблюдается не только в западных странах, но и в Республике Беларусь. Оборот отрасли производства ИТ-услуг в Беларуси давно превысил 1 млрд USD и вырос в 20 раз за 10 лет. Принята Государственная программа развития цифровой экономики и информационного общества на 2016 – 2020 годы, успешная реализация которой направлена на привлечение эффективных инвестиций и ускоренное развитие инновационных секторов экономики [1].

Благодаря сильной технической школе, высококвалифицированным кадрам, низким издержкам в секторе, ценовой конкурентоспособности белорусских ИТ-компаний, а также вовремя предоставленным льготам (в первую очередь – резидентам Парка высоких технологий (далее – ПВТ) в Республике Беларусь развивается не только экспортная модель разработки программного обеспечения, но и продуктовая. В сфере разработки программного обеспечения вопросы защиты интеллектуальной собственности стоят очень остро. Разглашение коммерческой тайны может привести к значительным финансовым потерям и потерям ключевых клиентов, может вызвать ухудшение отношений с инвесторами и кредиторами, а также несет огромные риски для репутации компании.

2. Случаи увольнения или совершения сотрудниками других неправомерных действий часто влекут для компаний значительные экономические издержки. Нередки случаи, когда компании создаются собственниками исключительно под разработку конкретных программных продуктов и утрата исходного кода равносильна банкротству. В подобных условиях использование

режима коммерческой тайны в качестве одного из правовых механизмов защиты интеллектуальной собственности является обязательным условием эффективного развития бизнеса [2, с. 172].

В области IT-технологий в настоящее время наиболее развитыми системами разработок и защиты прав собственности являются США, страны Евросоюза, Китай, Индия, Япония и ряд других. При этом основную роль в обеспечении сохранности коммерческой тайны играют сами фирмы, а не государственные органы [3, с. 69].

Следует отметить, что японский бизнес менее всего страдает от утечки информации. Это связано с присущей этой стране системой «пожизненного найма» и воспитанием у сотрудников чувства патернализма, когда они считают себя членами одной семьи. Известный основатель и руководитель фирмы Sony Акио Морита утверждал, что когда нет преданности, которая приходит с долгосрочной занятостью, то нет возможности положить конец утечке информации и воровству, от которых повседневно страдает бизнес на Западе [4, с. 7].

Обязанность неразглашения коммерческой тайны организации предусмотрена рядом конвенций МОТ (например, в ст. 19 Конвенции № 155).

Руководители служб безопасности отмечают, что по статистике 85 – 90 % ущерба, наносимого компании, – «заслуга» персонала, внешние факторы влияют не более чем на 15 % [5, с. 48].

Поэтому главное место в организации надежной защиты секретной информации должно отводиться работе с кадрами. Специалисты считают, что сохранность секретов компании на 80 % зависит от правильного подбора, расстановки и воспитания кадров. И эта работа должна начинаться со дня приема человека на работу [4, с. 24, 25].

3. Первым направлением в работе с кадрами является правильный подбор персонала, который целесообразно проводить с полной проверкой каждого кандидата посредством проведения нескольких этапов собеседования, получения информации с предыдущих мест работы, применения технических средств психологического тестирования и т. д.

Подбор персонала с применением полиграфа – одна из самых распространенных современных методик работы с кадрами, осо-

бенно в США, Европе и России. В Беларуси ситуация несколько иная. Полиграф применяется редко и только крупным частным бизнесом. В частности, полиграф применялся на конечном этапе собеседования на должность финансового директора крупной металлургической компании [6].

Важно отметить, что законного основания применения полиграфа при трудоустройстве не существует, поэтому соискатель имеет полное право отказаться от подобной проверки.

Практика показывает, что лучше предусмотреть неприятные ситуации во взаимоотношениях нанимателя и работника и подписать все необходимые документы по обеспечению режима коммерческой тайны при приеме на работу. Обычно при приеме на работу человек готов подписать любые документы, в то время как при увольнении это сделать гораздо сложнее.

4. Вторым по важности мероприятием должно быть ограничение доступа к секретной информации и мониторинг за деятельностью сотрудников. В организации должен быть грамотно введен и эффективно поддерживаться режим коммерческой тайны. Работа должна быть организована таким образом, чтобы каждый сотрудник имел доступ только к той информации, которая необходима ему в процессе выполнения прямых служебных обязанностей. Эта мера не сможет сама по себе полностью защитить от возможной ее утечки, но позволит свести возможный ущерб к минимуму.

Как показывает практика, значительная утечка коммерческой информации происходит в ходе ведения переговоров. Сотрудник должен четко знать, какую информацию он имеет право сообщить партнеру по переговорам, а какую – нет. Сотрудник должен понимать, что от успешно проведенных переговоров зависит не только процветание фирмы, но и его личное благополучие [4, с. 25, 26].

В профессиональной среде распространено мнение, что использование сотрудниками интернета стоит запрещать, в том числе и с личных мобильных устройств. Однако очевидно, что в IT-сфере это просто невозможно, поскольку интернет и соцсети часто выступают в качестве «орудия труда».

Для контроля своих сотрудников наниматель может использовать технические средства контроля. При этом важно помнить, что любое негласное применение технических средств контроля, во-первых, противоречит ст. 28 Конституции Респу-

блики Беларусь. Во-вторых, ответственность за подобные действия предусмотрена в ст. ст. 179 и 203 Уголовного кодекса Республики Беларусь. Негласный контроль за личной перепиской сотрудников, мониторинг открытых веб-сайтов, перехват сообщений мессенджеров в целях охраны коммерческой тайны является незаконным и может быть расценен как вмешательство в личную жизнь сотрудника, посягательство на тайну его корреспонденции.

Вместе с тем полагаем, что, если наниматель в целях соблюдения коммерческой тайны решит применить технические средства контроля, такие, например, как видеонаблюдение либо анализ истории посещений интернет-сайтов со служебного компьютера, данные меры следует рассматривать как законные в случае, если работник будет уведомлен об этом. Порядок и цели применения таких средств могут быть описаны в Положении о коммерческой тайне и других локальных правовых актах, с которыми работник также должен быть ознакомлен.

В случае обнаружения нарушения сотрудником режима коммерческой тайны посредством электронной переписки и признания ее в качестве допустимого доказательства распечатку скриншота с экрана или простую распечатку лучше нотариально заверить, составив у нотариуса протокол осмотра интернет-страницы.

5. Третьим направлением в работе с персоналом является проведение воспитательной работы и обучение сотрудников сохранности коммерческой информации. Вместе с тем сотрудник, нарушивший правила работы с секретной информацией, должен знать, что у него будут серьезные неприятности и он будет строго наказан руководством [4, с. 25, 26].

6. Четвертым направлением в работе с персоналом является правильный порядок расторжения трудовых отношений с работниками.

Самым элементарным шагом при увольнении сотрудника является смена паролей и порядка доступа к рабочим программам. На практике это делают редко в то время, когда это одно из обязательных требований, обеспечивающих функциональность режима коммерческой тайны.

На сегодняшний день в белорусском законодательстве нет нормы, по которой бы уволившемуся сотруднику можно было бы запретить работать у конкурента, а также заключать договоры

с клиентами компании в течение определенного периода времени. То же касается и создания экс-работником собственной компании, где бы емугодились навыки, приобретенные у нанимателя. То есть по общему правилу условие трудового договора, предусматривающее так называемую «оговорку о неконкуренции», будет являться ничтожным.

Однако согласно подпункту 5.5 п. 5 Декрета Президента Республики Беларусь от 21 декабря 2017 г. № 8 «О развитии цифровой экономики» (далее – Декрет № 8), резидентам ПВТ предоставлено право заключать между собой и/или с третьими лицами соглашение, предусматривающее обязанность одной стороны возместить другой стороне по ее требованию убытки и/или уплатить предусмотренную таким соглашением неустойку в случае совершения одной стороной или ее аффилированным лицом действий, имевших результатом прекращение трудовых отношений между другой стороной и ее работником (работниками) и установление трудовых отношений между таким работником (такими работниками) и первой стороной или ее аффилированным лицом [7].

В связи с этим имеет место законодательное закрепление соглашения о запрете переманивания сотрудников, одной из сторон которого должен быть резидент ПВТ. Основной и взаимной обязанностью сторон соглашения о непереманивании сотрудников является обязательство не трудоустраивать у себя работников сторон по соглашению (не проводить рекрутинг, не приглашать работников контрагента на работу, не рассматривать на свои вакансии кандидатов из компаний-контрагентов).

В случае нарушения обязанности сторон воздержаться от реализации своего права на поиск и наем сотрудников другой стороне предоставлено право потребовать от стороны, допустившей нарушение, прекратить переговоры с кандидатом (отозвать направленное ранее предложение о работе) или возместить убытки и/или уплатить неустойку.

Однако требовать увольнения работника, который перешел на работу в другую компанию, в связи с нарушением соглашения о непереманивании сотрудников незаконно, поскольку законодательством не закреплено такое основание увольнения, как нарушение нанимателем договоренности (соглашения) о непереманивании сотрудников. Также отказ кандидату в приеме на

работу по причине заключения соглашения о непереманивании сотрудников является незаконным, так как Декрет № 8 не расширяет перечень причин (обстоятельств), по которым работнику можно обоснованно отказать в приеме на работу. Компания (наиматель) вправе отказать в приеме на работу бывшему сотруднику своего контрагента, только если кандидат не соответствует требованиям, предъявляемым к конкретной должности.

В связи с вышеизложенным, можно говорить, что Декрет № 8 легализует и регламентирует новые гражданско-правовые отношения между организациями о запрете переманивания сотрудников, но не отношения в трудовой сфере. Отношения между работником и организацией в части соглашения о неконкуренции также регулируются только в гражданско-правовой плоскости, при этом не устанавливаются нововведения в сфере трудовых отношений.

7. Наконец, пятым направлением в работе с IT-специалистами, обеспечивающими личную заинтересованность сотрудников в сохранении коммерческой тайны, для резидентов ПВТ являются опционы, предусмотренные Декретом № 8.

Опционы с работниками – это общепринятая мировая практика в IT-компаниях, когда ключевых участников команды стимулируют не только высоким вознаграждением, но и долей от прибыли компании, участием в доле прибыли от сделки по продаже стартапа. Более того, как раз стартапам инструмент опциона помогает привлечь квалифицированные кадры. Обычно, не имея возможности «сорить» деньгами инвесторов и платить выше рынка, стартапы готовы при этом делить прибыль с ключевыми работниками в случае своего будущего успеха.

Таким образом, на сегодняшний день опционы с работниками – один из самых успешных мотиваторов для наемного IT-работника, так как предоставляет ему часть прав акционера. Этот же инструмент представляется нам самым эффективным в сохранении режима коммерческой тайны, поскольку предусматривает личную материальную заинтересованность сотрудников. Представляется возможным законодательное закрепление возможности использования опционов IT-компаниям, не входящим в ПВТ.

### Список использованных источников

1. Об утверждении Государственной программы развития цифровой экономики и информационного общества на 2016 – 2020 годы [Электронный ресурс] : постановление Совета Министров Респ. Беларусь, 23 марта 2016 г., № 235 // Консультант Плюс: Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2019.
2. Шоломицкая, И. В. Введение режима коммерческой тайны в IT-компаниях / И. В. Шоломицкая // Магистерский вестник : сб. науч. работ магистрантов и аспирантов : в 3 ч. / редкол.: М. Г. Жилинский [и др.]. – Минск : ИВЦ Минфина, 2018. – Ч. 3. – С. 172–176.
3. Токарев, Р. Б. Патентные стратегии IT-компаний / Р. Б. Токарев // Маркетинг. – 2015. – № 5 (144). – С. 64–78.
4. Соловьев, Э. Я. Коммерческая тайна и ее защита / Э. Я. Соловьев. – М. : Изд-во «Ось-89», 2001. – 128 с.
5. Николаева, О. В. Как правильно нанять персонал / О. В. Николаева // Директор. – 2018. – № 2. – С. 48, 49.
6. Саврук, М. А. Полиграф при приеме на работу. Как работает и зачем нужен [Электронный ресурс] / М. А. Саврук // Куку. – Режим доступа: <https://kyku.org/money/poligraf-pri-prieme-na-rabotu-kak-rabotaet-i-zachem-nuzhen>. – Дата доступа: 28.08.2019.
7. О развитии цифровой экономики [Электронный ресурс] : Декрет Президента Респ. Беларусь, 21 дек. 2017 г., № 8 // Консультант Плюс: Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2019.