Лояльность - это отношение сотрудника к работодателю, основанное на полном доверии и уважении к нему, а также на искренней приверженности корпоративным целям, ценностям и традициям. В этом случае можно рассчитывать, что работник не только сам будет строго соблюдать все установленные работодателем требования, в том числе – в области обеспечения информационной и имущественной безопасности, но и по мере возможности не допустит их нарушения коллегами по работе.
Так как в российской экономике пока не сформирована конкурентная среда, побуждающая собственников, работодателей прилагать необходимые усилия по оценке и укреплению лояльности персонала.

Главным атрибутом нелояльности выступает стремление сотрудника к достижению собственных целей, при полном игнорировании не только корпоративных интересов работодателя, но и ранее принятых перед ним трудовых обязательств. Именно эти цели, т.е. побудительные мотивы и определяют уровень нелояльности сотрудника, следовательно, и характерные для него признаки трудового поведения. Ниже выделены **пять типов** нелояльных сотрудников:

«Прагматик» - не скрывает от работодателя стремление ограничить свои трудовые усилия исключительно рамками трудового договора и должностной инструкции. От прагматиков исходит наименьшая опасность, в большинстве своем они являются квалифицированными специалистами. Их нежелание приносить свои интересы в жертву интересам работодателя, демонстративное игнорирование многих внешних атрибутов лояльности компенсируется добросовестным отношением к исполнению своих служебных обязанностей и высокой личной порядочностью. Реальная ценность таких сотрудников для организации, следовательно – и отношение к ним со стороны работодателя, целиком зависит от уровня квалификации и степени дефицитности их специализации на рынке труда. В случае, если в силу указанных факторов они относятся к категориям «трудно заменимых» или «почти не заменимых» специалистов, работодатель вынужден включать их в состав «кадровой элиты», создавая эксклюзивные условия найма. В противном случае выраженный прагматизм сделает такого сотрудника легким объектом для переманивания конкурентами. Если же «прагматик» относится к категории «середнячков», то с его присутствием в штате работодатель будет

мириться до тех пор, пока не появится более достойная кандидатура на замещение данного рабочего места. Однако, в любом случае, прагматики обычно не рассматриваются в качестве кандидатов на замещение руководящих должностей. Их профессиональная карьера в организации осуществляется по одному из двух направлений - горизонтальные перемещения для исполнителей и вертикальные – для высококвалифицированных специалистов (экспертов). Допуск «прагматика» к конфиденциальной информации или к управлению высоколиквидными активами обычно нежелателен, но на практике часто необходим в силу его высокого профессионализма.

Признаки трудового поведения «прагматика»:
- готовность к оперативному и полному исполнению общих трудовых обязательств, принятых перед работодателем, равно как и наилучшим образом выполнять его задания - но только в рамках своего трудового до-говора и должностной инструкции;
- честность по отношению к работодателю;
- недопущение публичной критики работодателя;
- демонстративное игнорирование любых конфликтов в организации;
- демонстративный отказ идти на жертвы ради достижения целей работодателя;
- не скрываемый от работодателя «нейтралитет» в отношении его целей и ценностей;
- демонстративный отказ от участия в корпоративных ритуалах и игнорирование корпоративных традиций, в случае, если они вступают в противоречие с интересами самого работника;
- не скрываемое от работодателя нежелание предупреждать об угрожающих ему опасностях, в том числе – со стороны нелояльных коллег по работе.

«Имитаторы» более опасны для работодателя в качестве источников угроз имущественной, и особенно – информационной безопасности. Их стремление к минимизации собственных трудовых усилий распространяется на все аспекты профессиональной деятельности, в том числе, непосредствен-но связанные с обеспечением безопасности. В частности, «имитатор» вряд ли станет затруднять себя скрупулезным выполнением всех пунктов инструкции по работе с конфиденциальными документами или электронными базами данных. Поэтому основной угрозой с его стороны выступает нанесение организации имущественного или репутационного ущерба не из-за злого умысла, а в силу общей безответственности и лени. При управлении профессиональной деятельностью рассматриваемой категорией сотрудников соблюдаются несколько простых

правил. Поскольку «имитатор», за редким исключением, не утруждает себя ни текущей работой, ни повышением своей профессиональной квалификации, он никогда не может претендовать на роль менедже-ра или специалиста. Это позволяет работодателю использовать его в качестве рядового исполнителя, причем не допущенного ни к конфиденциальной информации, ни к ответственным технологическим операциям. В отличие от «прагматика» «имитатор» является первым кандидатом на сокращение или на замещение более ответственным сотрудником из числа кандидатов на трудоустройство.

Признаки трудового поведения «имитатора»:
- не только полное отсутствие публичной критики работодателя, но и регулярные публичные его восхваления;
- постоянная демонстрация личной преданности вышестоящему руководителю;
- готовность сообщить работодателю о любых нарушениях со стороны коллег по работе, включая и ложные доносы;
- активное участие в корпоративных ритуалах;
- готовность выступать в роли постоянного организатора различных корпоративных мероприятий, не связанных с работой;
- скрытое участие в трудовых и межличностных конфликтах, склонность к интригам.

«Борцы за справедливость» представляют прямую угрозу безопасности организации одновременно по двум направлениям. Во-первых, при наличии в деятельности работодателя любых, даже незначительных прегрешений перед законом, именно они выступят в роли «идейного разоблачителя» перед контролирующими инстанциями государства, прикрывая свое предательство ссылкой на «активную гражданскую и социальную позицию». Во-вторых, выступая в качестве постоянных «возмутителей спокойствия» в своих трудовых коллективах, такие «борцы» активно способствуют ухудшению в них состояния психологического климата. Одним из наиболее распространенных поводов для критики руководства со стороны рассматриваемой категории нелояльных сотрудников является обвинение в наличии «любимчиков», которым в ущерб остальным работникам и достаются повышения в должности, крупные премии, дополнительные социальные льготы. Если в таком подразделении по-настоящему лояльные сотрудники не составляют большинства, подобная критика найдет многих «благодарных слушателей». В результате вокруг элитных работников подразделения неизбежно возникнет «стена отчуждения», что может спровоцировать их инициативное увольнение. Рассмотренные выше угрозы делают

недопустимым пребывание «борцов за справедливость» в штате любой коммерческой организации. Лучшим способом профилактики выступает их отсев еще на стадии трудоустройства. При необходимости же избавиться от уже присутствующего в штате работника данного типа, работодателю необходимо скрупулезно выполнять соответствующие требования трудового законодательства. В противном случае почти неизбежным становится продолжительное судебное разбирательство по иску уволенного сотрудника, «несправедливо репрессированного за свои социальные убеждения».

Признаки трудового поведения «борца за справедливость»:

- жесткая и публичная критика кадровой политики работодателя и деятельности непосредственного руководителя;
- постоянные публичные насмешки над корпоративными ценностями и ритуалами;
- демонстративное игнорирование корпоративных традиций;
- регулярное провоцирование конфликтов;
- постоянные официальные жалобы в различные государственные инстанции с критикой работодателя.

«Саботажники – мстители» - в обычных условиях их трудовое поведение соответствует первым трем уровням лояльности. Несоответствие четвертому и пятому уровням (в силу отсутствия необходимых морально-этических норм и, тем более, желания отождествлять себя с работодателем) обычно успешно скрывается от руководителя и коллег по работе. Однако в случае, если работодатель или непосредственный руководитель чем-то серьезно обидел сотрудника («обошел» в повышении, лишил премии, объявил публичный выговор и т.п.), у него немедленно срабатывают такие негативные личностные качества как злопамятность, отсутствие самокритичности, мстительность. В дальнейшем «саботажник-мститель» психологически уже готов использовать любой подходящий момент для «сведения счетов» с работодателем. Особая опасность его действий заключается в том, что, планируя свою месть, он обычно не задумывается о тяжести последствий от ее реализации не только для работодателя, но и для своих коллег. В результате уничтожение саботажником компьютерной базы данных или порча особо ценного оборудования способна парализовать работу подразделения на дли-тельный срок и, как следствие, вызвать массовое сокращение его сотрудников или длительный неоплачиваемый отпуск. Противодействие саботажнику затрудняет тот факт, что он обычно никогда не афиширует свою обиду, а свою месть осуществляет так, что выявить конкретного виновника традиционными методами расследования весьма затруднительно.

Признаки трудового поведения «саботажника-мстителя»:

- наличие негативных с позиции работодателя личностных качеств (злопамятность, обидчивость, мстительность), определяющие в некоторых ситуациях проявление нелояльности;
- отсутствие чувства солидарности с интересами не только работодателя, но и коллег по работе;
- неспособность сотрудника объективно оценить адекватность нанесенной ему обиды и ущерба работодателя от реализованной мести;
- умение длительное время скрывать от работодателя и коллег по работе свое желание отомстить.

«Конспираторы» представляют наибольшую угрозу с позиции обеспечения кадровой безопасности организации.
Их морально-этические установки (точнее – полное их отсутствие) изначально нацеливают на нанесение работодателю любого ущерба, сопряженного с приобретением таким сотрудником малейшей личной выгоды. Именно представители рассматриваемой группы нелояльных работников являются наиболее привлекательными объектами для вербовки конкурентами, криминальными структурами, индивидуально действующими злоумышленниками. При наличии хотя бы минимальных гарантий личной безопасности «конспиратор» с легкостью идет на соучастие в краже, дает «наводку» на ограбление, принимает взятку за злоупотребление своими служебными полномочиями, продает конкуренту конфиденциальную информацию. С таким же успехом он может действовать и по собственной инициативе, если задуманное преступление не предполагает необходимость наличия соучастников. В отличие от «борца за справедливость», «конспиратор» всегда умело скрывает свое истинное отношение к работодателю, внешне демонстрируя ему полную лояльность. Это затрудняет выявление таких сотрудников в коллективе организации, особенно крупной. Поэтому наиболее эффективным методом борьбы с появлением «конспираторов» в штате конкретного работодателя является эффективная процедура отбора кандидатов на трудоустройство. При неудачном решении данной задачи, выявление и увольнение представителей данной группы нелояльных сотрудников осуществляется обычно уже по результатам проведенных служебных расследований причин реализованных угроз.

Признаки трудового поведения «конспиратора»:
- готовность внешне подчиняться всем требованиям и пожеланиям работодателя в области лояльности персонала;

- неучастие в коллективных конфликтах;
- полное отсутствие морально-этических обязательств перед работодателем;
- постоянная готовность принести в жертву своим интересам интересы работодателя;
- в случае возможности извлечения существенной личной выгоды – готовность создать ситуацию, при которой работодателю будет нанесен любой по масштабам ущерб;
- отказ от публичной критики работодателя в сочетании с постоянной готовностью предать его при наличии малейшей личной выгоды.

По данным отечественных и зарубежных исследований, количество утечек информации от работников организации составляет от 60 до 80%. При этом доля так называемых квалифицированных утечек, т.е. когда работники умышленно осуществляют хищение информации или создают утечку, колеблется от 15 до 30%. Высокий процент умышленных утечек (в России порядка 25%) является следствием отсутствия либо недостаточной проработанности системы управления лояльностью персонала.

Для компании очень важно выявить нелояльного сотрудника еще на этапе прохождения собеседования. К сожалению, в настоящее время не существует точных вопросов, отвечая на которые, новый сотрудник может указать на свою нелояльность. Однако есть ряд вопросов, благодаря которым можно сделать близкие к реальности выводы. В первую очередь нужно задавать больше вопросов, не касающихся работы. Если сотрудник отвечает быстро и четко, а главное, правдиво, это означает, что ему нечего скрывать. Именно такие вопросы помогают создать портрет нового сотрудника как человека, а не только сотрудника, исполняющего обязанности. Другой разговор, если опрашиваемый отвечает на вопросы уклончиво – в такой ситуации стоит задуматься о том, стоит ли принимать его на работу. Однако чаще всего то, что требуется узнать для менеджера по подбору персонала, лежит на поверхности. Понять, лоялен ли сотрудник, можно по резюме. На этот вопрос помогут ответить следующие пункты:

•должности, которые он занимал;

•период, в течение которого он проработал на предыдущей работе;

•количество мест, которые он сменил, перед тем как прийти именно в эту компанию и т. д.

Если у компании есть возможность проверить факты, указанные в резюме или сказанные во время собеседования, то лучше это сделать. Намеренная ложь сразу указывает на нелояльность нового сотрудника. Сюда относится и утаивание каких-либо фактов или скрытый шантаж. Это касается случаев, когда сотрудник, к примеру, говорит о предложениях конкурентов с целью повысить свою зарплату. Способами диагностики на данном этапе могут быть: анкетирование, ответы на вопросы в анкете, которую заполняет кандидат перед собеседованием, или опросная беседа в ходе самого собеседования. В случае опросной беседы можно проводить ее видеозапись (с предварительного письменного согласия), чтобы в последующем имеющийся в штате специалист по безинструментальной детекции лжи (сотрудник службы безопасности) мог ее просмотреть и дать соответствующее заключение.

Кроме того, в ряде организаций практикуются опросные беседы с использованием полиграфа. Хотя, по мнению автора, применение методов инструментальной диагностики на этапе собеседования нежелательно в силу, во-первых, достаточно трудоемкой предварительной подготовки, во-вторых, возможного негативного отношения квалифицированных специалистов к указанной процедуре и, как следствие, потери достойного кандидата. Использование полиграфа допустимо лишь при принятии на работу в организации, работающие с государственной тайной или осуществляющие конфиденциальные (секретные) научно-технические разработки, а также при расследовании инцидентов.

1. Анкетирование. Принципы применения указанного метода аналогичны описанным выше. Вся разница будет лишь в вопросах, включенных в анкету. В указанную анкету, по мнению автора, целесообразно включать балльную оценку удовлетворенности сотрудников следующими аспектами работы: организацией труда, содержанием труда, условиями труда, размером заработной платы, системой материального и нематериального стимулирования, отношениями с коллегами и руководителем, удовлетворенность стилем руководства менеджеров, перспективам карьерного роста. При анкетировании персонала целесообразно включать в анкеты вопрос, направленный на расчет такого показателя, как индекс чистой лояльности работника – eNPS (анг. Employee Net Promoter Score). Данный индекс был первоначально использован при оценке лояльности клиентов компаний, а затем адаптирован в сферу управления персоналом. Для расчета указанного индекса достаточно включить в анкету следующий вопрос: с какой вероятностью вы порекомендуете свою компанию друзьям и знакомым? (нужно поставить балл от 1 до 10). На основании анализа указанного показателя можно

прогнозировать текучесть кадров, их результативность и выявлять возможные группы риска.

Кроме того, можно использовать анкеты-опросники, составленные по методикам оценки лояльности персонала Л.Г. Почебут – О.Е. Королевой и Д. Мейера – Н. Аллен.

2. Метод проективных вопросов. Достаточно трудоемкий и требующий специальных знаний в области психологии. Суть данного метода в том, что сотруднику предлагают ответить на так называемые открытые вопросы, например "Какими качествами должен обладать хороший руководитель?", "Какие условия должны быть созданы для эффективной работы?". Указанные вопросы предполагают развернутый ответ, интерпретация которого позволит определить, насколько лоялен работник организации и какие меры можно предпринять для повышения его лояльности.

3. Интервью. Также достаточно трудоемкий метод. Его использование целесообразно для оценки лояльности управленцев или высококвалифицированных работников, ценных для организации. При проведении интервью целесообразно применять как открытые, так и закрытые вопросы, примеры которых приведены выше.

4. Систематический мониторинг рабочей активности. Индикаторами низкой лояльности работников могут быть выявленные факты нарушения трудовой дисциплины и инциденты информационной безопасности. Так, например, для выявления фактов опозданий и ранних уходов с рабочего места можно использовать журналы системы контроля доступа в помещение работодателя. Для выявления различных групп инсайдеров в настоящее время существуют два типа систем мониторинга и защиты информации – DataLoss (Leak) Protection (Prevention) (DLP) и Use randentity behavior analytics UEBA.

DLP-системы в настоящее время являются одним из популярных решений по контролю за персоналом, используемых руководителями служб как информационной, так и экономической безопасности. Большинство существующих на рынке систем данного класса дает возможность обеспечить не только мониторинг и блокировку электронных каналов коммуникации, но и мониторинг активности пользователей, позволяющий выявлять сотрудников, нерационально использующих рабочее время: опаздывают на работу и уходят раньше, сидят в социальных сетях, играют в компьютерные игры, работают "на себя".

Системы UEBA предназначены для анализа поведения пользователей, построения их профилей и выявления поведения, отклоняющегося от нормы, которое может свидетельствовать о снижении лояльности.

5. Анализ активности пользователей в социальных сетях. В настоящее время практически у каждого работника имеется профиль в социальной сети, а зачастую в нескольких. Анализ профиля в социальной сети позволяет выявлять нелояльных работников путем оценки их высказываний об организации, коллегах и руководстве в комментариях или публикуемых постах, фиксации времени активности в сети, членстве в группах (например, группы по поиску работы).

Завершение диагностики лояльности работника, по мнению автора, должно осуществляться на этапе его увольнения из организации. Оценка лояльности на указанном этапе направлена на прогнозирование причинения вреда интересам организации ее бывшим работником после увольнения. Методы проведения – анкетирование или опрос. К примеру, автор в обязательном порядке проводит с увольняющимися работниками беседу перед подписанием так называемых обходных листов с целью выявления настроя бывшего работника к организации, а также мотивов увольнения (позитивные или негативные).

Разумеется, не стоит ожидать преданности от всего коллектива, так как это невозможно. Однако на ключевые должности стоит назначать именно лояльных сотрудников, тех, на кого действительно можно положиться в сложной ситуации. Именно с такими работниками компания способна покорять новые вершины. Только при совместной работе возможна дорога вверх. Влияние нелояльных сотрудников на конкурентные позиции организации – работодателя не требует специального рассмотрения. Оно просто «полярно» по механизму своего действия, механизму влияния лояльных сотрудников. Конкурентные преимущества автоматически превращаются в недостатки. Именно поэтому задачей любого работодателя в области обеспечения кадровой безопасности выступает увеличение удельного веса лояльных сотрудников с одновременным сокращением нелояльного персонала. Работа по оценке лояльности персонала должна проводиться сотрудниками служб безопасности совместно с кадровыми подразделениями, а для обеспечения эффективной работы, направленной на предупреждение противоправной активности инсайдеров, необходимо формировать в организации систему управления лояльностью персонала.

1. Алавердов А.Р. «Технологии управления лояльностью персонала». 2017 г.
2. Саматов К. «Способы диагностики и оценки лояльности персонала как составляющей кадровой безопасности организации» Интернет-ресурс. Режим

доступа: http://information-security.ru/articles2/job/sposoby-diagnostiki-i-otsenki-loyalnosti-personala