Успешное функционирование организации в условиях рыночной экономики предполагает обеспечение эффективной системы безопасности, особенно информационной и имущественной. Персонал организации влияет на все аспекты жизнедеятельности организации, а также неразрывно связан с ее информационной и экономической безопасностью.

Прежде чем рассматривать основные виды угроз имущественной и информационной безопасности, которые может нанести нелояльный сотрудник, хотелось бы заострить внимание на понятии лояльность сотрудников.

В переводе с французского языка, лояльность означает верность. Исходя из этого, справедливо предположить, что лояльный сотрудник, значит сотрудник верный своей компании. С точки зрения науки, лояльный сотрудник – это сотрудник, который принимает ценности фирмы как собственные, следует корпоративной культуре, поддерживает тактику действий своего вышестоящего руководства.

В свое время один из топ-менеджеров «General Electric» Джек Уэлч сформулировал это понятие так: «Лояльный персонал — это команда единомышленников, приверженных целям и ценностям моего предприятия и готовых на многое ради его процветания». Естественно, что такое положение является заветной мечтой каждого руководителя. Однако формирование лояльности - длительный и непростой процесс, требующий тщательного подхода.

По моему мнению, чем больше выражен уровень лояльности, тем более надежным является сотрудник. Лояльные работники готовы смириться с временными трудностями компании, принять необходимые организационные перемены. Такие сотрудники дорожат своим рабочим местом именно в этой компании. Они не только сами стремятся как можно лучше выполнить свою работу, но нередко побуждают к этому и своих коллег. Только лояльные сотрудники готовы творчески подходить к решению возникающих проблем, брать на себя ответственность, прикладывать все усилия для достижения целей компании. Можно говорить о нескольких уровнях лояльности, которые можно выделить у работников. Каждый последующий уровень обеспечивает более высокую степень преданности компании:

- **Лояльность на уровне атрибутики**, которая свидетельствует о принадлежности к компании. Это формальный уровень, который говорит только об ожидаемом поведении человека, владеющего или использующего тот или иной атрибут компании.
- **Лояльность на уровне поведения**. Подразумевает выполнение определенных норм, правил, регламентирующих такие поступки сотрудников, как, например, обязательное обсуждение организационных событий прошедшего дня во время утреннего перекура или коллективное поздравление начальника отдела с вручением ценного подарка.
- **Лояльность на уровне способностей**. Подразумевает более выраженную приверженность компании, нежели на предыдущих уровнях. Во многом лояльность зависит от того, насколько компетентно подобран персонал. Лояльность на уровне способностей подразумевает, что человек обладает соответствующими целям и требованиям организации навыками и умениями, придерживается определенных принципов и поэтому может воспроизводить ожидаемое и требуемое поведение. Сотрудник, лояльный на уровне способностей, ценен для организации. Он всегда хорошо ориентируется в происходящих изменениях, инициативен, так как обладает необходимыми знаниями и заинтересован в достижении целей компании. От него можно ожидать эффективных инновационных предложений, его взгляд всегда нацелен на перспективу достижений компании.

Лояльность на уровне убеждений и лояльность на уровне идентичности. Лояльность на уровне убеждений подразумевает полное принятие убеждений и принципов организации. Ценности организации становятся личными ценностями работника, поэтому устойчивость этих позиций наиболее высока. Формальное послушание и следование правилам здесь сменяет открытая приверженность. Таким уровнем лояльности обладают руководители, работники, занимающие высшие и ключевые должности в организации, работники, удовлетворенные своей работой, оплатой, условиями, а также имеющие большой стаж работы на данном месте. Лояльность на уровне идентичности в наивысшей степени демонстрирует сам владелец компании. Он вкладывает все свои силы, сбережения и время в то, чтобы добиться совершенства и развития компании. Тем более, если он стоял у самых истоков и первые шаги становления своего дела осуществлял главным образом самостоятельно. Эта верность компании уже не просто безусловна - она является сама собой разумеющейся.

В общем же смысле можно выделить следующие проявления лояльности сотрудников в профессиональной деятельности:

- искренняя заинтересованность в деятельности компании;
- любовь к своей работе, к своему делу;
- стремление повысить свой профессиональный уровень;
- творческий подход к предложениям, поступающим от начальства;
- проявление инициативы, которая должна привести к улучшению работы компании;
- готовность отстаивать свою позицию, если есть уверенность в том, что она верна;
- отношение к интересам фирмы, как к собственным интересам;
- понимание того, что процветание организации - это процветание каждого сотрудника.

Соответственно, нелояльный сотрудник – это сотрудник по каким-то причинам намеренно неэффективно работающий в организации, который считает, что он никому ничего не должен и работает либо в четких рамках своей должностной инструкции, либо, даже не выполняет свои обязанности, прописанные в должностной инструкции. Так же такой сотрудник может саботировать других сотрудников на такое же поведение, подрывать авторитет руководства компании.

На самом деле, форм проявления нелояльности очень много. Своим поведением, сотрудник так или иначе наносит ущерб для организации-работодателя. В рамках данной темы, рассмотрим два варианта угроз, которые могут исходить от такого сотрудника, это угроза информационной безопасности и угроза имущественной безопасности.

В современном мире, информации – это самое главное конкурентное преимущество любой организации. Потеря конфиденциальной, строго - конфиденциальной, ценной информации может нанести урон, вплоть до закрытия компании.

Информация обладает следующими свойствами:

- аутентичность - свойство информации, позволяющей идентифицировать источник ее происхождения (устанавливать авторство)
- конфиденциальность - свойство информации быть защищенной от несанкционированного ознакомления;
- целостность - свойство информации быть защищенной от несанкционированного искажения, разрушения или уничтожения;

- доступность - свойство информации быть защищенной от несанкционированной блокировки.

Чаще всего нелояльный сотрудник будет проявлять интерес к конфиденциальной информации. Относительно определения понятия «конфиденциальная информация», следует отметить, что лексическим значением слова «конфиденциальный» является такое понятие: «не подлежащий разглашению, доверительный, тайный». На мой взгляд, конфиденциальной информацией может быть любая информация с ограниченным доступом, не отнесенная действующим законодательством к государственной тайне.

Конфиденциальность понимается как предотвращение возможности использования информации лицами, которые к ней не причастны.

К конфиденциальной информации относится информация, доступ к которой ограничивается с целью защиты коммерческой или клиентской тайны, а также иные данные, разглашение которых по тем или иным причинам нежелательно для конкретной организации.

Основными видами конфиденциальной информации являются:

- клиентская тайна - разновидность конфиденциальной информации, находящейся в распоряжении организации, разглашение которой способно нанести имущественный или неимущественный ущерб ее клиентам или партнерам по хозяйственной деятельности;
- банковская тайна - конфиденциальные сведения о финансовой и коммерческой деятельности клиентов финансово-кредитной организации, которыми банк располагает как их доверенное лицо;
- коммерческая тайна - разновидность конфиденциальной информации, находящейся в распоряжении организации, разглашение которой способно нанести ей имущественный или неимущественный ущерб как хозяйствующему субъекту.

Нанести угрозу информационной безопасности нелояльный сотрудник может различными способами и выражается это может тоже по разному, рассмотрим, по каким признакам можно разделить угрозу информационной безопасности:

- по критериям информационной безопасности (угрозы конфиденциальности данных и программ; угрозы целостности данных, программ, аппаратуры; угрозы доступности данных; угрозы отказа от выполнения операций);

- по компонентам информационных систем, на которые нацелены угрозы (информационные ресурсы и услуги, персональные данные, ноу-хау, программные средства, аппаратные средства, программно-аппаратные средства);
- по способу осуществления (случайные, умышленные, действия природного и техногенного характера);
- по расположению источника угроз (внутренние и внешние).

Существует много причин, по которой может произойти утечка информации, самая опасная причина, это действия (умышленные или неумышленные) нелояльного сотрудника.

Основные угрозы информационной безопасности организации, которые может нанести нелояльный сотрудник:

- противоправный сбор и использование информации;
- нарушение технологии обработки и хранения информации;
- внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;
- разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;
- вывод из строя, повреждение или разрушение средств и систем обработки информации, телекоммуникации и связи;
- влияние на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации;
- утечка информации по техническим каналам;
- утечка информации по личным каналам;
- внедрение электронных устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения органов государственной власти, предприятий, учреждений и организаций всех форм собственности;
- уничтожение, повреждение, разрушение или хищение печатных, аудио-, видео-, электронных и других носителей информации;
- перехват информации в сетях передачи данных и линиях связи, дешифрование этой информации;
- навязывание недостоверной и ложной информации;
- распространение информации, способной нанести ущерб репутации организации;

- использование не сертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации;
- несанкционированный доступ к информации, находящейся в банках и базах данных;
- нарушение законных ограничений на конфиденциальность и распространение информации.

В общем смысле нелояльный сотрудник может уничтожить, переделать, передать (слить) или предоставить прямой доступ третьему лицу (н-р. конкурентам) к информации организации. Что может повлечь за собой: снижение прибыли компании, потерю конкурентного преимущества, снижение доли рынка, проблемы с государственными органами, разлад рабочего коллектива, «вербовку» или создание таких же нелояльных сотрудников, увольнение кадровой элиты, потерю имиджа «достойного работодателя» на рынке труда.

Что касается имущественной безопасности, то, по моему мнению, данная угроза менее опасна, так как она не наносит урон имиджу организации, но в значительной степени наносит урон материальному состоянию организации.

В общем смысле, имущество предприятия – это материальные ценности, используемые предприятием в производственной деятельности. Имущество предприятия включает все виды имущества, которые необходимы для осуществления хозяйственной деятельности.

Так же как с информацией, порча имущества может произойти по многим факторам, природные явления, срок эксплуатации и так далее, но самым опасным является нелояльный сотрудник.

Основные угрозы имущественной безопасности организации, которые может нанести нелояльный сотрудник:

- мелкие хищения товарно-материальных ценностей организации (от канцтоваров до относительно дешевой готовой продукции);
- крупные хищения товарно-материальных ценностей организации (от дорогостоящей готовой продукции до производственного оборудования), совершаемые обычно в сговоре с коллегами или сторонними злоумышленниками;
- хищения наличных денежных средств;

- хищения наличных и безналичных денежных средств путем фальсификации финансовых документов;
- хищение денежных средств с использованием информационных технологий;
- нанесение организации ущерба в результате коррупции при заключении хозяйственных договоров и контрактов;
- умышленное повреждение или уничтожение имущества организации (саботаж);
- неумышленное повреждение или уничтожение имущества организации (преступная небрежность).

По моему мнению, вышеперечисленные факторы являются основными, если говорить об имущественной безопасности. Такие действия со стороны нелояльных сотрудников могут привести к таким последствиям как: увеличение расходов на обслуживание оборудования, увеличение расходов на обновление оборудования и материалов, снижение уровня лояльности у всех сотрудников организации (по принципу «как не придешь, вечно ничего не работает, как работать на таком оборудовании»), срыв рабочих процессов, уменьшение прибыли.

Рассмотрев основные угрозы информационной и имущественной безопасности со стороны нелояльных сотрудников, хочется отметить, что важно отбирать, принимать на работу лояльных сотрудников, а также сохранять эту лояльность на протяжении всего времени работы сотрудника в компании. Моя точка зрения заключается в том, что лучший поддержания лояльности персонала – это мотивация.

В литературе чаще всего выделяются следующие основные методы мотивации сотрудников, которые в свою очередь ведут к повышению лояльности персонала к организации.

1. Материальный метод. Способы материального стимулирования сотрудников включают в себя:
    - премии
    - проценты
    - участие в прибыли компании
    - опционы
    - предоставление займов
    - льготное кредитование
    - корпоративное пенсионное обеспечение
    - накопительную премию по результатам работы за год

- частичную или полную оплату обучения, тренингов
- социальный пакет, в том числе медицинское страхование
- оплату услуг мобильной связи и фитнес-центров
- поездки за границу и т. д.

Среди руководителей нет единого мнения о том, имеет ли смысл предлагать сотрудникам максимально широкий спектр вышеперечисленных возможностей, из которых, скорее всего, не все будут реально использоваться. Здесь важно разграничивать социальные программы и другие виды материального стимулирования.

Недостатком метода материального стимулирования является то, что постоянное повышение уровня оплаты не способствует ни поддержанию на должном уровне трудовой активности, ни росту производительности труда. Применение этого метода может быть полезным лишь для достижения кратковременных подъемов эффективности деятельности сотрудников. В конечном итоге происходит привыкание к данному виду воздействия и постоянное повышение производительности труда в подобных случаях нереально. Данный метод не дает возможности удовлетворить нематериальные потребности, связанные с профессиональной деятельностью персонала.

2. Целевой метод. Этот метод заключается в регулировании деятельности сотрудников по средствам постановки взаимовыгодных профессиональных целей. Никакие установленные извне цели не вызывают заинтересованности человека и активизации усилий до тех пор, пока они не станут его «внутренней» целью и не перейдут во «внутренний» план действия. Мотивация работников в контексте данного метода, по мнению М. И. Магуры и М. Б. Курбатовой, зависит от четырех основных характеристик целей:

- конкретность (определяет вероятность того, что работник поймет, как и когда сотрудник должен достичь поставленной цели);
- сложность (степень, в которой работник рассматривает цели как трудные, перспективные и бросающие вызов его возможностям, но достижимые);
- приемлемость (степень, с которой работник принимает цели и хочет их достичь);
- активное участие в постановке целей (формирует личную ответственность за успешность достижения целей в будущем).

Подводя итог вышесказанному, хочется отметить, что нелояльный сотрудник может представлять большую опасность для организации.

Причины появления таких сотрудников могут быть следующими:

- неэффективные методы отбора персонала
- некомпетентные действия непосредственного руководителя сотрудника
- некорректные действия управляющих компанией;
- вербовка сотрудника со стороны конкурентов
- менталитет сотрудника
- неэффективная система мотивации и развития персонала и др.

По моему мнению лучше проводить профилактические действия по «выращиванию» лояльных сотрудников, нежели бороться уже с нелояльными сотрудниками, активно проявляющими свою позицию. Я считаю, что каждая организация обязана выстроить такую кадровую политику, чтоб сотрудники даже не задумывались о каком-либо проявлении нелояльности. В качестве примера хочу привести одну историю: «В 1996 году никому не известная горничная крупного английского отеля Линда Хилп стала победительницей национальной лотереи, выиграв первый приз в размере двух миллионов фунтов стерлингов. После этого она в соответствии с новыми возможностями улучшила жилищные условия (приобретя небольшой замок), совершила кругосветный круиз и… осталась трудиться на прежнем месте. «Я слишком люблю свою компанию, свою работу. Без нее моя жизнь будет неполной», — объясняла счастливица в многочисленных интервью.»

К сожалению такая история является лишь трогательным исключением из правил. На самом же деле, я не думаю, что дело лишь в главной героини истории, ключевую роль играет та кадровая политика, которую выбрала (разработала) для себя организация и которой она придерживается.

Природа лояльности кроется в признании и уважении авторитета фирмы и ее руководителей. Причем эти чувства основаны на вполне конкретных надеждах и убеждениях персонала. Сотрудники должны быть уверены, что их лояльность будет по достоинству оценена сверху. Иными словами, достаток, социальная защита и карьерные перспективы персонала должны быть адекватны уровню его ответственности и уважения к фирме и тогда компания может быть практически на 95% уверенна в своей информационной и имущественной безопасности.