**Конспект лекций по дисциплине: Управление кадровой безопасностью организации**

Раздел 1. Основы управления кадровой безопасностью в организации

Тема 1. Система кадровой безопасности. Понятие, место, принципы и основные задачи кадровой безопасности в системе безопасности организации. Методы противодействия угрозам кадровой безопасности организации. Нормативно-правовые и методические основы кадровой безопасности.

Тема 2. Кадровые риски и угрозы. Типы, источники возникновения, методы анализа и оценки кадровых рисков и угроз. Социальные и личностные индикаторы кадровых рисков и угроз.

Тема3. Кадровая безопасность в системе управления персоналом. Принципы, инструменты и правовые основы обеспечения кадровой безопасности в процессах управления персоналом. Основные регламенты компании по кадровой безопасности.

Раздел 2. Обеспечение кадровой безопасности компании

Тема 4. Противодействие угрозам кадровой безопасности в процессах управления персоналом. Подбор и найм: исследование информации о кандидате (группы риска), оценка благонадежности, защита персональных данных. Противодействие угрозе переманивания персонала. Безопасное увольнение сотрудников. Информационная безопасность, защита персональных данных.

Тема 5. Предупреждение и противодействие противоправным и недобросовестным действиям персонала. Способы и инструменты обеспечения имущественной, финансовой и информационной безопасности организации (мошенничество, воровство, неблагонадежность и т.д.). Нормативноправовые основы проведения внутренних расследований и применения санкций к сотрудникам.

Тема 6. Социально-психологические аспекты кадровой безопасности. Мотивационные факторы благонадежности и лояльности персонала. Корпоративная этика как инструмент кадровой безопасности. Методика оценки лояльности/ благонадежности персонала.

**Тема 1.**

Созданию службы безопасности обычно предшествуют два события:

1 Как реакция на внезапно возникшие реальные угрозы имуществу, физической расправы с персоналом и т.д.

2 Неудовлетворительное состояние безопасности предприятия

В первом случае – служба безопасности:

− создаётся поспешно;

− способна лишь в некоторой степени отразить угрозы;

− способна в дальнейшем реагировать на появление кадровых угроз.

Таким образом реализуется принцип работы: «угроза – отражение». Понятно, что такая работа службы безопасности аварийная и не всегда способна вовремя, либо качественно отразить уже наступившее негативное событие. Остаётся риск рецидива преступлений, причём частота повторения кадровых угроз может нарастать.

Во втором случае, при неудовлетворительном состоянии безопасности предприятия проводится детальное изучение ситуации, чаще всего с привлечением сторонних специалистов, поскольку своих безопасников на предприятии не оказалось. В результате – формируется «реальное представление» о системе безопасности предприятия. И уже предпринимаются необходимые меры по выравниванию/оздоровлению ситуации на местах.

В качестве нормативно-правовой базы регулирования кадровых угроз на предприятии существует ряд законодательных норм, отраженных в федеральных законах. Приведём лишь некоторые из них:

− Указ Президента РФ № 361 «О борьбе с коррупцией в системе государственной службы».

− Федеральный закон РФ № 2446-1 «О безопасности».

− Федеральный закон «Об информации, информационных технологиях и защите информации».

− Закон РФ «О частной детективной и охранной деятельности в РФ».

− Федеральный закон РФ № 98-ФЗ «О коммерческой тайне».

− Федеральный закон РФ № 122-ФЗ «О контроле за соответствием расходов лиц, замещающих государственные должности, и иных лиц их доходам».

− Федеральный закон РФ № 230-ФЗ «О профессиональных стандартах».

− Федеральный закон РФ № 273-ФЗ «О противодействии коррупции».

− Федеральный закон РФ № 238-ФЗ «О независимой оценке компетенций».

− Федеральный закон РФ № 152-ФЗ «О персональных данных».

− Постановление Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

− Гражданский кодекс РФ №51-ФЗ (с изм. и доп.).

− Уголовный кодекс РФ № 63-ФЗ (с изм. и доп.).

Благодаря этим законам можно раскрыть сущность безопасности, в том числе, кадровой, описать элементы системы кадровой безопасности. Термин «безопасность» определяется в ст. 1 ФЗ

«О безопасности» от 5 марта 1992 года как «состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз».

Сущность безопасности напрямую связана с понятием «развитие» и «устойчивость». ***Безопасность*** – это способность к устойчивости (самовыживанию) и развитию в условиях внутренних и внешних угроз, действий непредсказуемых и трудно прогнозируемых факторов.

Исходя из данного определения, становятся понятными и функции безопасности, а именно: выявление, предупреждение, снижение, ослабление, нейтрализация, пресечение, локализация, отражение и устранение угроз.

***Система безопасности организации*** – это комплекс организационно-управленческих, экономически-правовых, социально-психологических, профилактических, пропагандистских, режимных и инженерно-технических мер и мероприятий, направленных на обеспечение безопасности организации и ее персонала.

Вся ***система кадровой безопасности*** представлена четырьмя элементами. В неё входит:

1 Научная теория безопасности.

2 Политика и стратегия безопасности.

3 Средства и методы обеспечения безопасности.

4 Концепция безопасности предприятия.

Раскроем эти элементы.

***Научная теория безопасности***

Ни одна, даже хорошо развитая и стабильно действующая организация, не застрахована от неожиданностей, способных привести к серьёзным негативным последствиям. Такие события способны внести хаос в работу и дестабилизировать налаженные процессы в управлении персоналом, создать угрозу кадровой безопасности в организации. С точки зрения безопасности предприятия, угроза – это потенциальное или реально возможное событие, действие, процесс или явление, которое способно нарушить устойчивость и развитие компании и/или привести к остановке его деятельности. Кадровых угроз для предприятия большое множество.

Угрозы кадровой безопасности негативно сказываются на деятельности. Кадровая безопасность включает в себя широкий спектр угроз. По направленности воздействия различают угрозы, при которых объектом кадровой безопасности может выступать как сама организация, так и её персонал. Со стороны организации угрозой может стать, например, незаконное увольнение сотрудника, либо перевод его на другую должность без согласия работника. В таких случаях приходится защищать права работника с привлечением третьей стороны. Нередко дело доходит до суда. Вместе с тем и сам персонал часто грешит незаконными действиями, которые способны нанести серьезный ущерб организации. В данном случае речь идет о несанкционированном разглашении конфиденциальной информации, о приписках в финансовых документах, об использовании своего положения в должности для выполнения незаконных сделок. Отдельные сотрудники подвергаются психологическим манипуляциям и вербовке со стороны третьих лиц. В результате, они оказываются втянутыми в такие социально-трудовые отношения, где есть место не только неприятным случайностям (ошибкам), но также преднамеренным злостным нарушениям. И если ошибочные действия можно списать на некомпетентность работников, чрезмерную доверчивость или даже на недобросовестность, то подлоги, «слив» информации, использование в корыстных целях или добыча незаконными методами конфиденциальной информации – все это свидетельствует о целенаправленном подрыве устоев организации, возникновении кадровых угроз для экономической безопасности организации.

Термином «риск», как правило, характеризуют возможность возникновения нештатной ситуации или неблагоприятных последствий какого-либо события. Рисковые ситуации формируют уязвимость работника и коллектива, создают кадровые угрозы в организациях.

Ситуации риска отличаются некоторыми особенностями. Прежде всего, это связано с неопределенностью момента возникновения риска, характером и последствиями развития нештатной ситуации, а также с дефицитом времени и недостаточностью поступающей информации, определяющих последующее функциональное поведение работника, оказавшегося в данной ситуации.

Психологи рассматривают риск как «сознательно-волевую деятельность субъекта, связанную с преодолением неопределенности в ситуации неизбежного выбора из нескольких альтернатив, в процессе которого есть возможность определить вероятность достижения поставленной цели» [А.П. Альгин, 1989; 1990]. То есть, ситуация кадрового риска формирует у работника активное восприятие действительности. В этом случае личный опыт и психологическая готовность конкретного работника в разрешении чрезвычайной и/или нестандартной ситуации формируют уникальную модель поведения. Это объясняет, почему в идентичных ситуациях каждый сотрудник поступает особым для него образом.

Почему один работник способен и готов идти на сговор, преступление, способствовать разглашению конфиденциальной информации и коммерческой тайны, заниматься промышленным шпионажем и прочими неблаговидными и преступными действиями, а другой – нет [И.Н. Махмудова, 2020].

Таким образом, речь идет не о мотивационном факторе, как это принято считать в научной литературе, а о сформированном шаблоне мышления и поведения, если оно являлось положительным опытом в жизни конкретного человека. Именно поэтому важно всячески обеспечивать контроль ситуации и не допускать возможности совершения неблаговидного выбора сотрудника, оказавшегося в нестандартной ситуации. Для этого параллельно с мерами контроля необходимо проводить профилактическое информирование персонала о возможностях и последующих угрозах как для самого работника, так и для организации, в случае нарушения кодекса и норм корпоративной этики, правил поведения в организации.

Потребуется отрабатывать некоторые оперативные действия, чтобы избежать наступления нештатной ситуации. Важным источником угроз является недостаток информации, спонтанные (неожиданные, бесконтрольные) действия других субъектов и уникальность самой ситуации. В.А. Петровский в своих исследованиях надситуативной активности выявил два основных типа риска: мотивированный и немотивированный. Он связывает мотивированный риск с расчетом шансов на успех [Петровский В.А., 1992]. Это значит, что человек в ситуации выбора склонен идти на сближение с опасностью ради реализации наиболее предпочтительных (для себя или для конкретной специфичной ситуации, определяемой обстоятельствами жизни человека) целей и достижения желаемых результатов. Иногда такую форму риска называют оправданной.

Эту идею подтверждают исследования зарубежных и российских социальных психологов [Кленова М.А., 2010]. Однако, наряду с данной формой существует и другая, особая форма риска – «риск ради риска». Такая ситуация сближения с опасностью не имеет какой-либо внешней необходимости, а выполняется ради испытания остроты ощущений. Она не просто не оправданна, но и опасна для организации с точки зрения формирования кадровых угроз. Ситуация бесконтрольна, выполняется на уровне осознанного выбора работника, который получает эмоциональное наслаждение. А это, как известно, самые стойкие эмоции, которые человек стремится раз за разом возобновлять. Это и есть мотивированный риск.

Данный выбор позволяет максимально реализовать скрытые потенциальные человеческие возможности. Просчитать их заблаговременно не представляется никакой возможности. Можно лишь локализовать данные потенциальные угрозы системой профилактических мероприятий, повышающих лояльность персонала организации и формирующих эмоциональную устойчивость личности. В качестве мероприятий этому могут способствовать методы, повышающие самооценку личности и уровень его самоконтроля.

***Показатели надёжности системы безопасности.***

***Политика и стратегия безопасности.***

Надежность и эффективность системы безопасности предприятия оценивается на

основе одного критерия – степени отсутствия или наличия нанесенного ему материального ущерба и морального вреда.

Содержание этого критерия раскрывается через ряд показателей:

1) недопущение фактов утечки (разглашения) конфиденциальных сведений;

2) предупреждение или пресечение противоправных действий

со стороны персонала предприятия, его посетителей, клиентов;

3) сохранность имущества и интеллектуальной собственности

предприятия;

4) предупреждение чрезвычайных ситуаций;

5) пресечение насильственных преступлений в отношении

отдельных (специально выделенных) сотрудников и групп сотрудников предприятия;

*Политика и стратегия безопасности* – это общие ориентиры для действий и принятия решений, которые облегчают достижение целей.

Такими целями могут быть:

1 Укрепление дисциплины труда и повышение его производительности.

2 Защита законных прав и интересов персонала.

3 Укрепление интеллектуального потенциала предприятия.

4 Сохранение и приумножение собственности.

5 Повышение конкурентоспособности производимой продукции.

6 Максимально полное информационное обеспечение деятельности предприятия и повышение его эффективности.

7 Ориентация на мировые стандарты и лидерство в разработке и освоении новой технологии и выпускаемой продукции.

8 Выполнение производственных программ.

9 Оказание содействия управленческим структурам в достижении целей предприятия.

10 Недопущение зависимости от случайных и недобросовестных деловых партнеров.

Общие ориентиры для действий и принятия решений:

− сохранение и наращивание ресурсного потенциала;

− проведение комплекса превентивных мероприятий по повышению уровня защищенности собственности и персонала предприятия;

− включение в деятельность по обеспечению безопасности

предприятия всех его сотрудников;

− профессионализм и специализация персонала предприятия;

− приоритетность не силовых методов предотвращения и нейтрализации угроз.

Для успешного выполнения этой политики необходимо реализовать стратегию безопасности, под которой понимается совокупность наиболее значимых решений, направленных на обеспечение приемлемого уровня безопасности функционирования предприятия.

***Выделяют три типа стратегий безопасности***:

1 Ориентированные на предотвращение возникновения возможных угроз.

2 Нацеленные на предотвращение воздействия существующих или возможных угроз на предмет безопасности.

3 Направленные на восстановление (компенсацию) наносимого ущерба.

***Концепция безопасности предприятия, сущность, её структура и составные элементы***

Определяющим и изначальным звеном при формировании системы безопасности является концепция безопасности организации.

Концепция – это официально утверждённый документ, в котором отражена система взглядов, требований и условий организации мер безопасности персонала и собственности предприятия. Концепция – это свод основных документов, касающихся:

− политики безопасности;

− стратегии безопасности;

− основных направлений;

− средств и методов ее обеспечения.

Выделяют некоторые требования к концепции безопасности:

− Конструктивность – добиться исходного состояния объекта при использовании необходимых и остаточных средств в достижении цели;

− Вписываемость в единую систему объектов;

− Открытость – давать возможность в её рамках реагировать на изменение условий реализации концепции и вносить коррективы в реализацию в случае их необходимости.

Структура концепции безопасности включает в себя три части:

1 Описание проблемной ситуации в сфере безопасности

− Перечень потенциальных и реальных угроз безопасности,

их классификация и ранжирование.

− Причины и факторы зарождения угроз.

− Негативные последствия угроз для предприятия.

2 Механизм обеспечения безопасности:

− Определение объекта и предмета безопасности предприятия

− Формулирование политики и стратегии безопасности.

− Принципы обеспечения безопасности.

− Цели обеспечения безопасности.

− Задачи обеспечения безопасности.

− Критерии и показатели безопасности предприятия.

− Создание оргструктуры по управлению системой безопасности предприятия.

3 Мероприятия по реализации мер безопасности:

− Формирование подсистем общей системы безопасности предприятия.

− Определение субъектов безопасности предприятия и их роли.

− Расчет средств и определение методов обеспечения безопасности.

− Контроль и оценка процесса реализации концепции.

Структура концепции безопасности примерная, однако, она предусматривает все необходимые направления деятельности для обеспечения системы безопасности на объекте.

***Субъекты безопасности предприятия, их элементы***

Субъекты безопасности предприятия делятся на две группы



Рис. 1 Субъекты безопасности предприятия

К первой группе относятся:

Специализированные субъекты (совет или комитет безопасности предприятия, служба безопасности, пожарная часть, строительная служба и т.д.), основным предназначением которых является постоянная профессиональная деятельность по обеспечению безопасности предприятия (в рамках своей компетентности).

Полуспециализированные, т.к. часть функций этих субъектов предназначена для обеспечения безопасности предприятия (медицинская часть, юридический отдел и т.д.). Весь остальной персонал и подразделения предприятия, которые в рамках своих должностных инструкций и положений о подразделениях обязаны принимать меры к обеспечению безопасности.

Ко второй группе относятся:

Законодательные органы – законы составляют правовую основу деятельности по обеспечению безопасности предприятия.

Органы исполнительной власти – принятые на уровне этих органов подзаконные акты во многом дополняют, уточняют, детализируют требования закона.

Суды. Судебные органы обеспечивают соблюдение законных прав и интересов предприятия, в том числе в сфере кадровой безопасности.

Правоохранительные органы. Они осуществляют борьбу с правонарушениями, которые негативно влияют на состояние безопасности предприятия.

Научно-образовательные учреждения (для подготовки частных охранников и детективов) – они призваны обеспечить научно-методическую проработку проблем безопасности предприятия и подготовку соответствующих специалистов в сфере безопасности предприятия.

***Тема 2.***

Кадровые угрозы можно классифицировать по разным основаниям:

По степени вероятности – невероятные, маловероятные, вероятные, весьма вероятные, вполне вероятные.

По степени удалённости – непосредственные, близкие (до 1 года), далёкие (свыше 1 года).

По степени развития – выделяют этап возникновения, экспансии, стабилизации и ликвидации.

По степени отдалённости угрозы в пространстве – это территория предприятия, прилегающая к предприятию территория, территория региона, страны, зарубежная территория.

По темпам нарастания – угрозы измеряются по месяцам,кварталам и годам.

По напряжённости – угрозы подразделяются на две группы:

а) нормальные, повышенные, близкие к пределу (порогу), избыточные;

б) определяют рост, стабильность или снижение.

По природе возникновения – бывают:

а) естественные/объективные, т.е. вызванные стихийными природными явлениями, не зависящими от человека, например, в результате наводнений, землетрясений, ураганов и проч.;

б) искусственные/субъективные, т.е. вызванные деятельностью человека, непреднамеренные/неумышленные и преднамеренные/умышленные угрозы.

Приведём пример намеренного создания кадровой угрозы на предприятии. В современной практике кадровую угрозу безопасности организации может создать, например, неумелое использование персоналом информационно-технических средств и специального оборудования, подвергающееся хакерским атакам, взлому криптоключей и запуском шпионских программ и вредоносных ПО. Такие действия извне отличаются своей непредсказуемостью и масштабностью урона для организации.

В настоящее время появился новый термин – «кибертерроризм», с которым ведётся целенаправленная борьба во всем мире. Однако, пока безрезультатно.

Кибертерроризм (это даже не хакерские атаки) вынуждает организации увеличивать финансовые вливания в создание защитных барьеров. С этой целью закупается дорогостоящее оборудование, вкладываются средства в закупку и установку новейших программных пакетов для отражения вирусных атак, в наём и обучение собственного персонала работе со специальными программами.

Но реальность такова, что злоумышленники пока идут на шаг впереди, втягивая организации в процесс саморазрушения, в незапланированные финансовые расходы. Также выделяют различные виды угроз: экономические, информационные, социальные, экологические, правовые, технические, организационные и криминальные. Постановка проблемы формирования кадровых угроз и рисков в организации. Самоконтроль часто идентифицируют как стрессоустойчивость.

Однако, это не совсем правильно. Самоконтроль позволяет успешно действовать в условиях риска, достигать положительного результата с учетом приоритета правил, требований, взятых на себя обязательств и специфики самой ситуации. Это навязанная, натренированная, внешняя эмоциональная устойчивость, внешний локус-контроль. Стрессоустойчивость, в большей степени, раскрывает специфику физиологии человека, его способность переносить повышенные нагрузки на нервную систему. Соответственно, это внутренняя эмоциональная устойчивость или внутренний локус-контроль.

Результаты научных исследований свидетельствуют о том, что у лиц с внутренним локусом контроля лучше развито умение использовать информацию в неопределенной ситуации, чем у лиц с внешним локусом контролем [Кочетков В.В., Скотникова И.Г.,1993; Рапохин Н.П., 1981].

Описанные выше исследования позволяют объяснить возникновение проблемной ситуации в области формирования кадровых угроз, а также способствуют постановке задачи об оценке вероятности наступления возможных рисков в организации. Кроме того, важно определить не просто готовность к риску специалистов службы безопасности, но и соответствие специалиста своей должности.

Готовность к риску специалистов службы безопасности (методы). Благосклонность к рисковому поведению, как мы выяснили, определяется ситуационными, мотивационными и личностными факторами, а также субъективным отношением человека. Однако, неопределенность возникновения рискованной проблемной ситуации диктует необходимость предоставить некие гарантии, что специалисты службы безопасности готовы демонстрировать способность принимать качественные управленческие решения и транслировать адекватное ситуации поведение для локализации и нейтрализации угроз в организации. Готовность к риску обычно сопровождается низкой мотивацией к избеганию неудач, и прямо пропорциональна числу допущенных ошибок.

Кроме того, интересными представляются результаты психологических исследований, которые зафиксировали тенденцию снижения готовности к риску в соответствии с увеличением возраста и опыта специалистов. То есть, наиболее опытные работники менее готовы к риску, чем молодые сотрудники [Кленова М.А.,2010].

Для диагностики личности на мотивацию к избеганию неудач, а также для оценки зависимости уровня готовности специалиста к риску от его возраста, можно использовать следующие инструменты анализа:

− методику Т. Элерса в сочетании с диагностикой степени готовности к риску по методике А.М. Шуберта;

− опросник «Ценностные ориентации» М. Рокича;

− тест-опросник Н. Когана и М. Уоллаха;

− факторный анализ по различиям средних величин, определяемых с помощью t-критерия Стьюдента.

Чтобы минимизировать вероятность наступления опасных событий и сократить случаи угроз кадровой безопасности, необходимо вовремя диагностировать потенциально опасные ситуации, регламентировать порядок оперативных мероприятий по выходу из опасных ситуаций. Кадровая безопасность организации как объект управления. Виды кадровой безопасности и кадровых угроз:

Угроза кадровой безопасности организации – это событие, действие или явление, которое посредством воздействия на персонал, финансовые, материальные ценности и информацию может привести к нанесению вреда здоровью работников и ущерба организации, нарушению или приостановке её функционирования.

Обеспечение безопасности организации – это деятельность её должностных лиц, персонала, специального подразделения по безопасности, государственных правоохранительных органов и иных структур, направленная на предотвращение возможного нарушения её нормального функционирования.

*Раскроем сущность видов кадровой безопасности.*

Физическая безопасность объекта – это охрана материальных и финансовых ресурсов от чрезвычайных обстоятельств (пожар, терроризм, стихийное бедствие) и от несанкционированного проникновения на территорию (вандализм, кража, хищение и т.д.).

Этот вид безопасности объекта обеспечивается деятельностью сотрудников службы охраны путём соблюдения пропускного объектового и внутриобъектового режимов с применением соответствующих охранных технических средств и систем.

К техническим и инженерно-техническим охранным средствам и системам относятся:

− Периметральные охранные системы.

− Системы охранной сигнализации.

− Системы пожарной сигнализации, пожаротушения и оповещения.

− Системы ограничения доступа.

− Системы управления доступом.

− Средства связи.

− Защитные инженерные средства (решетки, жалюзи, броне-стёкла и др.).

Экономическая безопасность объекта – это состояние защищенности экономических интересов организации от внутренних и внешних угроз посредством минимизации коммерческих рисков, системы мер экономического, правового и организационного характера, разработанных администрацией организации. Экономическая безопасность характеризуется совокупностью качественных и количественных показателей и включает в себя следующие функциональные составляющие: финансовую, имущественную, валютную, кредитную, политико-правовую и др. Экономическая безопасность выступает материальной основой решения практически всех задач, связанных с функционированием организации.

Информационная безопасность – это охрана каналов поступления, хранения, обработки и передачи информации, защита любых информационных ресурсов по уровням доступа. Защите подлежит любая документационная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу. Режим защиты информации устанавливается в отношении конфиденциальной документационной информации собственником информационных ресурсов, т.е. самой организацией. Результатами реализации угроз информации могут быть:

− утрата (разрушение, уничтожение);

− утечка (извлечение, копирование, подслушивание);

− искажение (модификация, подделка);

− блокирование.

Существует два основных принципа защиты информации:

− разделение обязанностей;

− минимизация привилегий.

Принцип разделения обязанностей предписывает так распределять роли и ответственность, чтобы один человек не смог нарушить критически важный для предприятия процесс. Принцип минимизации привилегий предписывает выделять пользователям только те права доступа, которые необходимы им для выполнении служебных обязанностей.

Юридическая безопасность – это охрана прав, порядка и условий осуществления конкурентной предпринимательской деятельности организации в рамках законодательства Российской Федерации. Выделяют три основных направления юридической безопасности:

1 Взаимоотношения с органами государственной власти.

2 Защита от действий недобросовестных партнёров, заказчиков или контрагентов.

3 Создание условий для успешной производственной деятельности организации.

Интеллектуальная безопасность – это охрана прав на научные труды, промышленные образцы, товарные знаки, коммерческие наименования. Гражданский кодекс РФ (ст. 138) «признает исключительное право (интеллектуальную собственность) ... юридического лица на результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации. Использование результатов интеллектуальной деятельности и средств индивидуализации может осуществляться третьими лицами только с согласия правообладателя».

Экологическая безопасность включает охрану окружающей среды, обеспечение безопасной работы экологически опасных объектов предприятия, предотвращение экологических катастроф.

Кадровая безопасность – это процесс предотвращения негативных воздействий на экономическую безопасность предприятия за счет:

− рисков и угроз, связанных с персоналом;

− его интеллектуальным потенциалом;

− трудовыми отношениями в целом.

Виды угроз со стороны персонала могут выражаться в следующем:

1 Хищение имущества предприятия.

2 Использование ресурсов предприятия в собственных целях.

3 Умышленная порча и уничтожение имущества предприятия.

4 Получение заработной платы за невыполняемую работу.

5 Шантаж компетентностью (я – незаменимый работник).

6 Шантаж полномочиями (концентрация полномочий в од-

них руках).

7 Торговля коммерческими секретами.

8 Дисциплинарные нарушения.

9 Создание в коллективе невыносимого морально-психологического климата.

Кадровая безопасность включает обеспечение физической

безопасности персонала. Физическая безопасность включает:

1 Личную безопасность руководителя.

2 Личную безопасность ведущих специалистов.

3 Безопасность всего персонала в целом.

Охрана первых двух категорий объектов регулируется Законом РФ «О частной детективной и охранной деятельности». Сюда относят физическую охрану руководителей и ведущих специалистов организации, а также охрану их жилья и средств передвижения и членов их семей. Личная безопасность обеспечивается целым комплексом оперативных и технических мер по охране лица как в обычных повседневных, так и в экстремальных условиях.

Охрана третьей категории объекта регламентируется Трудовым кодексом РФ (разд. X), Законом РФ «Об основах охраны труда в Российской Федерации» и нормативными правовыми актами по охране труда. Это система охраны труда и техники безопасности в организации на основе производственной санитарии и психологии деловых отношений. Безопасные и здоровые условия труда в организации обеспечиваются комплексным взаимодействием как руководства организации, так и, не в последнюю очередь, усилиями самого персонала организации.

Кадровую безопасность в организации рассматривают с позиций:

− процесса обеспечения текущей и потенциальной защищенности персонала от разнообразных угроз со стороны организации, в трудовых отношениях (основным источником угроз выступает работодатель, грубо нарушающий права и гарантии работников);

− с точки зрения активной защиты, в которой нуждается сама организация.

Речь идет об экономической безопасности, имидже и устойчивом развитии внутренних бизнес-процессов, об угрозах, создаваемых несанкционированными сознательными или неосознанными действиями персонала данной организации, которые могут вступать в сомнительные с точки зрения закона трудовые отношения. В эту группу включим: коррупционную деятельность чиновников и лиц, принимающих решение, злоупотребляющих своим положением; сговор, передачу секретной информации третьим лицам или использование её не по прямому назначению; вербовку редких специалистов, переманивание их в конкурирующие организации; рейдерские захваты, другие виды насильственных действий, физическую расправу.

Как видно, кадровую безопасность составляют риски со стороны персонала, которые возникают всегда и на всех этапах работы. Главный инструмент работы службы кадровой безопасности – тотальный контроль на всех участках работы персонала. Для этого применяют специальные средства, такие как видеонаблюдение, прослушивание телефонных разговоров, контроль доступа и работы компьютера, контроль использования рабочего и свободного времени сотрудников, контроль перемещений.

Важно также выстраивать качественное взаимодействие со службами управления персоналом в организации, начиная с этапа подбора и найма кадров. Список «опасных» кандидатов – это люди, чья работа в организации или их последующее увольнение может вызвать различные проблемы.

Что касается методов и техник – они самые разнообразные и очень специфичные, законные, и не очень:

− традиционный headhunting («хэдхантинг);

− talent raiding («кадровые налеты»);

− talent poaching («кадровое браконьерство»);

− executive search – «переманивание» лиц, принимающих решение;

− «агрессивный» или «партизанский» рекрутинг.

В применении методов и техник необходимо разграничивать функции HR-структур и служб безопасности. Если менеджеры в большей степени связаны с оценкой деловых и профессиональных качеств кандидатов (например, при подборе кадров), то службы безопасности применяют в большей степени силовые методы, используют повышенный уровень секретности. А для обнаружения хищений применяется ТОП-5 методов безопасности:

1 Электронный контроль – видеокамеры, мониторинг трафика в сети.

2 Технические средства защиты – сигнализация, электронный доступ, турникеты.

3 Внезапные ревизии.

4 Беседы с работниками.

5 Наблюдение за действиями сотрудников и технологическими процессами.

***Тема3.***

Под объектом безопасности предприятия понимают:

− степень устойчивости и развития предприятия;

− его способность противостоять угрозам.

В объекте безопасности предприятия можно выделить:

− различные структурные подразделения или группы сотрудников либо владельцы акций предприятия;

− ресурсы предприятия (информационные, кадровые, материально-технические, информационные, интеллектуальные и финансовые);

− различные виды деятельности (управленческая, производственная, снабженческая и т.д.).

Целью обеспечения безопасности предприятия является комплексное воздействие на потенциальные и реальные угрозы, поз воляющее ему успешно функционировать в нестабильных условиях внешней и внутренней среды.

Цель определяет насущные задачи её достижения:

− выявление угроз для стабильности и развития предприятия и выработка мер по их противодействию;

− обеспечение защиты технологических процессов;

− реализация мер противодействия всех видов шпионажа (промышленного, и т.д.);

− своевременное информирование руководства предприятия о фактах нарушения законодательства со стороны государственных и муниципальных органов, коммерческих и некоммерческих организаций, затрагивающих интересы предприятия;

− предупреждение переманивания сотрудников предприятия, обладающих конфиденциальной информацией;

− всестороннее изучение деловых партнеров;

− своевременное выявление и адекватное реагирование на дезинформационные мероприятия;

− разработка и совершенствование локальных правовых актов, направленных на обеспечение безопасности предприятия;

− реализация мер по защите коммерческой и иной информации;

− организация мероприятий по противодействию недобросовестной конкуренции;

− реализация мер по защите интеллектуальной собственности;

− организация и проведение мер по предотвращению чрезвычайных ситуаций;

− выявление негативных тенденций среди персонала предприятия, информирование о них руководства предприятия и разработка соответствующих рекомендаций;

− организация взаимодействия с правоохранительными и контрольными органами в целях предупреждения и пресечения правонарушений, направленных против интересов предприятия;

− разработка и реализация мер по предупреждению угроз физической безопасности имуществу предприятия и его персоналу;

− возмещение материального и морального ущерба, нанесенного предприятию в результате неправомерных действий организаций и отдельных физических лиц, обеспечение защиты всех видов ресурсов предприятия.

В рамках научной теории необходимо обозначит принципы построения системы безопасности предприятия. Принципы – это правила, которым нужно неукоснительно следовать или соблюдать. Выделяют следующие принципы:

1 Приоритет мер предупреждения – своевременное выявление тенденций и предпосылок, способствующих развитию угроз, на основе которых вырабатываются соответствующие профилактические меры по недопущению возникновения реальных угроз.

2 Принцип законности – меры безопасности предприятия разрабатываются на основе и в рамках действующих правовых актов. Локальные правовые акты предприятия не должны противоречить законам и подзаконным актам.

3 Комплексное использование сил и средств – для обеспечения безопасности используются все имеющиеся в распоряжении предприятия силы и средства. Каждый сотрудник должен в рамках своей компетенции участвовать в обеспечении безопасности предприятия. Организационной формой комплексного использования сил и средств является программа обеспечения безопасности предприятия.

4 Координация и взаимодействие внутри и вне предприятия – осуществляются на основе взаимодействия и скоординированности усилий всех подразделений, служб предприятия, а также установления необходимых контактов с внешними организациями, способными оказать необходимое содействие в обеспечении безопасности предприятия. Организовать координацию и взаимодействие внутри и вне предприятия может комитет (группа, совет и т.д.) безопасности предприятия.

5 Сочетание гласности с конспирацией. Доведение до сведения персонала предприятия и общественности в допустимых пределах мер безопасности выполняет важнейшую роль – предотвращение потенциальных и реальных угроз. Такая гласность, однако, должна непременно дополняться в оправданных случаях мерами конспиративного характера.

6 Компетентность. Сотрудники и группы сотрудников должны решать вопросы обеспечения безопасности на профессиональном уровне, а в необходимых случаях специализироваться по основным его направлениям.

7 Плановая основа деятельности – деятельность на основе комплексной программы обеспечения безопасности предприятия, подпрограмм обеспечения безопасности по основным его видам (экономическая, научно-техническая, экологическая, технологическая и т.д.) и разрабатываемых для их исполнения планов работы подразделений предприятия и отдельных сотрудников.

8 Принцип системности – означает учёт всех факторов, оказывающих влияние на безопасность предприятия, включение в деятельность по его обеспечению всех сотрудников подразделений, использование в этой деятельности всех сил и средств.

9 Принцип экономической целесообразности. Стоимость финансовых затрат на обеспечение безопасности не должна превышать тот оптимальный уровень, при котором теряется экономический смысл их применения.

***Тема 4.***

***Средства и методы обеспечения безопасности***

Все средства обеспечения безопасности предприятия подразделяются на семь групп. Среди них: технические, организационные, финансовые, информационные, правовые, кадровые и интеллектуальные. Применять данные средства обеспечения безопасности следует комплексно. Причем следует соблюдать этапы их применения. Так на первом этапе – используют исключительно финансовые средства. Важно понимать, что недостаточность именно этих средств обеспечивает всю дальнейшую работу по обеспечению безопасности на предприятии. Если данных средств будет недостаточно, то не будет никакой гарантии безопасности от кадровых и другого рода угроз. Среди принципов использования финансовых средств выделяют: их достаточность, целенаправленность и высокую отдачу применения (эффективность).

На втором этапе подключают формирование кадровых и организационных средств. Это значит, что должно быть достаточно кадров, занимающихся вопросами обеспечения безопасности; имеющиеся в наличии кадры должны отвечать высокому профессиональному уровню, который регулярно оттачивается и повышается. Что же касается организационных средств, то создаются специализированные оргструктурные формирования, обеспечивающие безопасность предприятия.

На третьем этапе – осуществляется разработка системы правовых средств. С одной стороны, используются уже изданные вышестоящими органами власти законы и подзаконные акты. С другой стороны, разрабатываются собственные, локальные правовые акты по вопросам обеспечения кадровой безопасности.

Наконец, на четвёртом этапе привлекаются всевозможные технические, информационные и интеллектуальные средства. Таким образом можно отметит понятность и последовательности логики применения всех имеющихся средств обеспечения безопасности в организации.

Методы воздействия на персонал в службе безопасности:

− методы диагностики угроз кадровой безопасности как со стороны внешних, так и внутренних факторов воздействия;

− методы, противостоящие потенциальной и/или реальной кадровой угрозе для организации.

Приведем классификацию методов диагностики кадровой

безопасности (рисунок)



***Методы и алгоритм приема персонала на работу***

Отбо­р будущих сотрудников организации. Содержание этого этапа во мно­гом зависит от традиций, культуры организации, а также характера долж­ности, на которую подбирается кандидат, однако в самом общем виде этот этап может быть представлен следующей схемой, включающей прак­тически все возможные этапы:

Первичный отбор начинается с анализа списка подобранных канди­датов с точки зрения их соответствия требованиям организации к буду­щему сотруднику. Основная цель первичного отбора состоит в отсеива­нии кандидатов, не обладающих минимальным набором характеристик, необходимых для занятия вакантной должности. Естественно, что этот минимальный набор является различным для разных специальностей и организаций.

Методы первичного отбора зависят от бюджета, стратегии, культу­ры компании и относительной важности данной должности для организации. Наиболее распространенными в настоящее время методами являются: анализ анкетных данных, тестирование, экспертиза почерка, тестирование на полиграфе.

Анализ анкетных данных (или анализ биографических данных) предполагает, что биография человека является достаточно надежным инди­катором его потенциала успешно выполнять определенные производствен­ные функции. При использовании этого метода отдел человеческих ресур­сов проводит анализ информации, содержащейся в заполненных кандидатами анкетах, сравнивая фактические данные с собственной моделью. Наличие такой модели (четко определенных критериев отбора) является необходи­мым условием проведения справедливого для кандидатов и эффективного для организации первичного отбора. Отсутствие четких критериев значи­тельно снижает эффективность отбора, поскольку решение принимается на основе субъективного мнения сотрудника, обрабатывающего анкеты, часто не обладающего достаточным знанием специфики данного вида деятельно­сти и, соответственно, предъявляемых к кандидату требований.

Анализ анкетных данных (анкеты могут быть самыми разнообраз­ными и содержать от 10 до 100 и более вопросов) является простым, дешевым и достаточно эффективным методом первичного отбора. В случае, когда организация имеет обширный список кандидатов и когда речь идет о специализированных должностях, например, наладчиках лиф­тов, операторах станков с программным управлением, брокерах по цветным металлам, преподавателях древнегреческого языка. В то же время этот метод достаточно приблизителен в оценке потенциала, по­скольку ориентирован исключительно на факты из прошлого кандидата, а не на его сегодняшнее состояние и способность к профессиональному развитию. Человек мог иметь отличные оценки по математике десять лет назад, но быть не в состоянии произвести элементарные вычисления сегодня. В приведенном выше примере Коммерческая школа могла упустить прекрасных потенциальных кандидатов, не имеющих научной степени, однако обладающих опытом руководства профессиональным обучением в крупных организациях. Поэтому при отборе кандидатов на руководящие должности, особенно предполагающие дальнейшее разви­тие и профессиональный рост, нужно быть крайне осмотрительным, используя метод анализа анкет.

Тестирование завоевывает в последнее время все большую попу­лярность среди ведущих организаций развитых стран, его используют не только корпорации, но и государственные учреждения, университеты, общественные организации. Преимущества тестирования состоят в воз­можности оценки сегодняшнего состояния кандидата с учетом особен­ностей организации и будущей должности. Недостатки этого метода первичного отбора – высокие издержки, часто необходимость сторон­ней помощи, условность и ограниченность тестов, не дающих полного представления о кандидате. Каждая организация должна принимать решение об использовании тестов с учетом собственных финансовых возможностей, культурных особенностей, приоритетов развития.

В настоящее время используются следующие тесты:

Методики диагностики интеллекта:

Тест «Домино»

Краткий ориентировочный тест (КОТ)

Методика диагностики социального интеллекта (Дж. Гилфорда, М. Салливена)

Методики диагностики мотивационно-потребностной сферы личности:

Методика Е. Б. Фанталовой «Уровень соотношения ценности и доступности в основных жизненных сферах»

Методика «Ориентированная анкета» (ОА)

Методика диагностики социально-перцептивных особенностей личности:

Методика «Индивидуальный стиль оценивания» (ИСО).

Модификация методики Ф. Фидлера.

Кроме того используются: шестнадцати факторный опросник Кеттелла, MMPI, тест диагностики уровня тревожности Тейлора, методика Айзенка, диагностика межличностных отношении Т. Лири и другие тесты.

«Многопараметрический Миннесотский Персональный опросник»

Словесный (вербальный) тест MMPI

• Содержит 550 утверждений, предъявляемых для выражения «согласен – не согласен».

• Самый надежный и подробный тест личности

• Максимально приближен к американскому прототипу

• Возможно получение дополнительных данных более чем по 200 особенностям личности (для профессионалов)

ЛУЧШЕ ВСЕХ ИЗВЕСТНЫХ ТЕСТОВ ОПИСЫВАЕТ СТАБИЛЬНЫЕ ЧЕРТЫ ЛИЧНОСТИ

• общий тип характера

• эмоциональный тип

• тип реагирования

• тип поведения в различных ситуациях

• тип отношения к окружающим

• отношение к проблемам

• тип мышления

• потребности

• мотивацию поступков

• склонности, в том числе профессиональные

• тип и условия приспособления к людям и работе

Экспертиза почерка, используемая довольно редко, получила особое распространение во Фран­ции. Она является своеобразной разновидностью тестирования, требующей значительно более низких затрат. Этот метод основан на теории, согласно которой почерк человека является достаточно объективным отражением его личности, и, следовательно, с помощью анализа почерка можно оценить различные характеристики человека, в том числе способность выполнять оп­ределенные производственные функции. По почерку человека определяются такие психологические характеристики, как способность к самостоятельному труду, сила воли, степень развития мышления, отношение к себе и окружающим и т.д. Привлекательность анализа по­черка как метода первичного отбора кандидатов заключается в низких издержках, однако он отличается односторонним подходом и содержит в себе высокую степень риска неадекватной оценки потенциала кандидатов. Поэтому он может использоваться в качестве одного из методов первич­ного отбора, не имеющего решающего значения.

Тестирование с помощью полиграфа (детектора лжи).

Существует три основных направления использования полиграфа для работы с персоналом организаций частного бизнеса:

а) при проведении внутренних расследований и разбирательств в связи с конкретными хищениями или другими действиями, нанесшими ущерб фирме;

б) в целях более полного изучения коллектива работников на предмет оценки их надежности, лояльности и выявления среди них «группы риска». Данная работа может проводиться и в интересах формирования резерва выдвижения;

в) для изучения кандидатов на работу, выявления среди них неприемлемых лиц и их недопущения в коммерческую структуру.

Следует отметить, что тестирование на полиграфе, выполняемое в интересах изучения и отбора персонала, существенно отличаются от испытаний, проводимых в ходе служебных расследований, как по степени сложности и арсеналу используемых методических средств, так и по степени точности и надежности, получаемых результатов.

Собеседование с сотрудниками отдела человеческих ресур­сов. Задача первичного отбора состоит в определении ограниченного числа кандидатов, с которыми организация могла бы работать индивиду­ально. На следующем этапе отдел человеческих ресурсов (специалист по подбору персонала) проводит индивидуальные собеседования (часто на­зываемые интервью – от английского interview) с отобранными кандида­тами. Цель этих собеседований заключается в оценке степени соответ­ствия кандидата портрету идеального сотрудника, его способности выполнять требования должностной инструкции, потенциала профессио­нального роста и развития, способности адаптироваться в организации, знакомстве с ожиданиями кандидата в отношении организации, условий работы, ее оплаты и т.д. Важно помнить, что собеседование является двусторонним процессом – не только организация оценивает кандидата, но и кандидат оценивает организацию с точки зрения ее соответствия его собственным интересам и запросам.

Сотрудник отдела человеческих ресурсов, проводящий собеседование, должен предоставить максималь­но объективную и полную информацию об организации, чтобы заинте­ресовать кандидата и одновременно избежать приема на работу тех, чьи ожидания расходятся с возможностями организации – чем раньше по­тенциальный работник и потенциальный работодатель поймут, что они не подходят друг другу, тем лучше для обеих сторон. В то же время собеседование по подбору не должно превращаться в своеобразную попытку «продать» компанию кандидату, проводящий его менеджер должен помнить о главной цели — определить, в какой степени данный кандидат обладает необходимыми для организации компетенциями. За­дачу убедить выбранного кандидата принять предложение нужно решать после того, как такой кандидат найден

***Методы и методики оценки сотрудников***

Проблема экономической безопасности компаний — это кражи, злоупотребления сотрудников, промышленный шпионаж и, как следствие, сотрудники безопасности начинают заниматься вопросами предупреждения утечки информации в частности и укрепления безопасности в целом.

В качестве средства обеспечения безопасности используются в том числе системы допуска, скрытые камеры и другая техника. Но ни один аппарат не избавит вас от риска потерь до тех пор, пока в компании работает хотя бы один неблагонадежный сотрудник.

Для выявления «слабого звена» можно использовать, например, вот такой способ: возьмите чистый лист бумаги. В центре нарисуйте небольшой кружок. Напишите рядом фамилию руководителя. От первого круга нарисуйте стрелки, которые будут изображать потоки информации. Если руководитель отдает распоряжения пяти со­трудникам, значит должно быть пять стрелок, каждая из которых указывает на свой кружок. Подпишите кружки второго уровня и продолжайте рисовать схему информационных потоков вашей компании.

Особый интерес представляют те сотрудники, на которых замыкается максимальное количество стрелок. Далеко не всегда лидером по числу информационных потоков является директор. Чемпионом может быть и диспетчер, и секретарь, и бухгалтер. Здесь нет никакой закономерности, каждая компания уникальна. Потоки информации, документооборот складываются в зависимости от личностей, занима­ющих те или иные должности. Кстати, особый интерес для конкурентов могут представлять тексты инструкций и регламентов, определяющие правила передачи информации внутри компании.

Если тщательно составить схему, то, вероятно, можно увидеть перед собой несколько узлов. Внедрив своего человека на одно из этих мест, конкуренты могут получить весьма значительный контроль над происходящим в компании. Они могут начать и с периферии. Но стремиться будут туда, где есть все, что им надо. Иногда, особенно когда уровень лояльности персонала достаточно высок, конкуренты поступают иначе. Они внедряют своего человека в штат.

Определив ключевые позиции и выбрав цель, конкуренты могут приступить к осуществлению второй части своего плана. Вербовка, как правило, строится на имеющемся противоречии, на имеющейся компрометирующей информации, на воздействии на слабые стороны личности.

***Технологии оценки благонадёжности.***

Технология состоит из нескольких этапов:

1 этап. Вы должны позаботиться о том, чтобы к вам поступило как можно больше информации о том, чем живут ваши коллеги: кто же­нился, кто завел любовника, кто замечен пьяным, кто демонстрирует склонность к риску. Чем больше информации, тем точнее будут ваши прогнозы. Но вы должны знать, что если от вас будет исходить угроза наказания, то информационный канал со временем превратится в бо­лото, а потом и вовсе пересохнет. Добейтесь того, чтобы ни один слух не проходил мимо вас, тогда вы спасете жизнь и свободу не одного человека.

2 этап. Любая полученная информация о сотруднике должна быть подвергнута анализу с точки зрения того, «является ли это признаком неблагонадежности». На втором этапе вы обязаны, в силу своей роли, преувеличивать опасность. Например, следующим образом.

Сотрудник А купил себе машину. Оценим его доходы, отнимем стоимость прожиточного минимума, добавим доходы других членов семьи. И тем не менее образуется разница. Не хватает десяти тысяч долларов. ОТКУДА: Мог ли он их взять в долг? Обращался ли он к кому-то с просьбой дать денег в долг? Го­ворил ли, что копит деньги на новую машину? Каков круг его знако­мых? Предположим худшее: деньги ему дали конкуренты за какую-либо услугу. Что он мог им передать за такую сумму? К каким секре­там у него есть допуск?

3 этап. С помощью воображения можно построить модель, гипотезу. Необходимо следить за тем, чтобы в основе гипотезы лежали достоверные факты.

4 этап. Профилактическая работа. Когда сумма факторов неблагона­дежности превышает некий порог, наступает пора профилактических действий. Вы знаете, что для разных категорий сотрудников может существовать свой критический порог. Для тех, кто работает с деньга­ми и другими ценностями, он традиционно ниже, как и для сотрудни­ков, которые при желании могут нанести наибольший ущерб в силу своих полномочий, доступа к ресурсам, к тайнам и секретам компа­нии. В этом аспекте минимальный порог реагирования у руководите­ля компании. Он, как правило, держит в своих руках большинство нитей управления и в его силах прекратить или нарушить работу ком­пании. К счастью, руководители часто являются и владельцами этой компании либо отличаются высокой степенью лояльности по отно­шению к владельцу.

***Методы профилактики***

Психологические методы.

• Разъяснительная и просвещающая беседа. Человек должен понять, за ним наблюдают, он на особом учете, ему не дадут безнаказанно нанести ущерб компании.

• Коллективное обсуждение факторов неблагонадежности, таких как, например, пьянство.

• Настоятельная рекомендация посетить специалиста для скорейше­го решения личностных проблем.

Организационные методы.

• Ограничение полномочий.

• Введение дополнительного контроля.

• Понижение в должности.

• Ограничение доступа к ресурсам.

• Увольнение как крайняя мера при безвыходном положении.

Рекомендуется начинать с психологических методов. Большинство проблем можно избежать, если руководитель начнет отслеживать появление признаков неблагонадежности и реагировать на них, а не на их последствия.

В заключение этого небольшого раздела необходимо сделать еще два замеча­ния. Технология оценки благонадежности не является карательным инструментом для увольнения неугодных. Использование данной тех­нологии не заменяет, не отменяет и не исключает работу компетент­ных органов, когда в результате того или иного поведения субъект создал им поле для деятельности. Человек, использующий техноло­гию оценки благонадежности, должен в полной мере осознавать свою ответственность за свои выводы и рекомендации. Он выполняет функ­цию желтого сигнала светофора, который сообщает, что впереди опасность, скоро включится красный, и ехать будет нельзя.

***Принципы корректного контроля благонадежности сотрудников***

Принцип ограниченности. Все, что связано с непосредственным ра­бочим процессом и выполнением служебных обязательств и ограниче­но работой, обладает безусловной открытостью для осуществления кон­троля. Работодатель имеет полное право знать, когда сотрудник при­шел на работу, когда ушел домой, кто входил в помещение, как долго он там оставался и т.д. Важным условием является обязательное знаком­ство сотрудника с полным перечнем контролируемых ресурсов. Новый сотрудник должен быть уведомлен о том, что на данном предприятии ведется скрытый контроль, что служебная переписка может быть про­читана, что телефонные разговоры могут быть записаны. Руководство обязано взять с него расписку, в которой сотрудник подтверждает факт ознакомления с этой стороной работы. Вопросы соблюдения режима секретности должны обсуждаться до того, как сотрудник вольно или невольно разгласит ценную информацию.

Принцип соответствия. Чем выше степень влияния конкретного сотрудника на работу компании в целом, тем больше прав у руковод­ства компании на особый контроль. Это звучит угрожающе с точки зрения защитника прав человека, но на деле это вполне оправдано.

Принцип уместности. Проводимые работы должны быть уместны­ми в контексте происходящего. Уместность определяется субъективно лицом, которое отвечает за предотвращение происшествий. Уместно проверять фактически отработанное время для большинства сотрудни­ков. Но как это сделать для тех, у кого свободный график посещения и ненормированный рабочий день? Уместно запрашивать отчет о прове­денной за день переписке по электронной почте, но только у тех, кто располагает этой самой почтой. Компа­нии создают инструкции и правила, жизнь меняется, но правила не все­гда поспевают за новыми реалиями. И тогда случаются курьезы.

Принцип уместности говорит о том, что контроль возможен, если существует риск. Он говорит о том, что чрезмерная перестраховка мо­жет превратить контроль в высшей степени формальное мероприятие.

Принцип актуальности. Проводимые мероприятия должны быть актуальны и своевременны. Профилактика должна опережать пре­ступления.

Принцип уведомления. Этот принцип уже рассматривался нами раньше. Человек должен быть предварительно уведомлен о том, что в компании приняты те или иные способы контроля. Он должен знать, что в помещении, где он работает, установлены камеры наблюдения, прослушивающие устройства, другая спецтехника.

Принцип сохранности информации. Вся полученная информация должна храниться с максимально возможными предосторожностями. Это требование не только нового Трудового кодекса РФ, но и здраво­го смысла. Защита информации — сложная задача. В настоящее вре­мя пишутся целые книги о том, каким образом можно сохранить и можно добыть информацию. Но никогда не будет существовать иде­альной системы защиты информации. Можно сказать, что все тайное рано или поздно станет явным. Именно из этого стоит исходить при планировании систем сохранения информации.

***Увольнение сотрудника***

Увольнение сотрудников может представлять для компании значи­тельную опасность. Это особенно актуально в том случае, когда уволь­няемый сотрудник обладает такими чертами личности, как обидчи­вость, мстительность, агрессивность и т. п.

Если некто считает себя несправедливо уволенным, он может по­пытаться тем или иным способом отомстить бывшему работодателю. Какой может быть эта месть? В некотором смысле, ответ можно пред­положить.

Если увольняемый работник работал программистом, то локаль­ная сеть и компьютеры компании находятся в опасности. Если при­шлось уволить бухгалтера, то опасности подвергается финансовая сфера компании. Если уволен продавец, то ваш конкурент может по­лучить все наработки по привлечению и удержанию клиентов.

Как минимизировать риски, связанные с увольнением сотрудников, по инициативе администрации компании?

Во-первых, нельзя принимать на вакантные должности людей, ко­торые могут создать проблемы своим поведением при выполнении работы или при увольнении. Нельзя принимать на работу мститель­ных, агрессивных сотрудников. Шансы на то, что вам удастся их пере­воспитать, не существуют.

Во-вторых, увольнять сотрудников надо таким образом, чтобы у них не было психологических причин для мести.

В-третьих, необходимо построить технологию предвосхищения про­блем, связанных с увольнением тех или иных специалистов. При этом технология не должна быть привязана к конкретным персонам, она долж­на иметь отношение только к должности. Например, «Технология увольнения программиста», «Технология увольнения секретаря» и т. д.

Зная особенности своей компании, вы можете определить, какие конкретные действия должны подразумевать эти технологии.

В качестве примера можно привести технологическую карту увольнения уже упоминавшегося программиста, администратора баз данных, си­стемного администратора. Приводимая технология запускается в дей­ствие после принятия окончательного решения об увольнении.

1. Анализ имеющихся данных о личности увольняемого сотрудни­ка. При анализе досье сотрудника необходимо понять, есть ли в его характере черты, которые могут толкнуть его на неблаговидные по­ступки после того, как он получит известие об увольнении. Если та­кие черты характера обнаружены, то увольнение должно проводить­ся но жесткому типу:

•       немедленное после подписания приказа об увольнении отстране­ние от работы на компьютере;

•       немедленная смена паролей и регламентов допуска;

• минимально возможные сроки отработки и передачи дел.

Если в характере увольняемого не обнаруживаются опасные чер­ты, то увольнение может проходить по более мягкой схеме. Сотруд­ник отрабатывает оговоренное время, и после его окончательного ухо­да из компании меняются пароли и регламенты доступа к ресурсам.

2. Анализ действий, выполняемых увольняемым сотрудником. Анализируется текущая деятельность сотрудника. Принимается решение о том, какую работу он может выполнять после подписания приказа об увольнении, а от какой работы он должен быть отстранен немед­ленно.

Составляется список других сотрудников, которые должны выпол­нять те или иные обязанности.

3. Анализ допусков и паролей. Если в компании ведется досье, то не  
составит труда вспомнить, какими допусками обладает сотрудник,  
какие пароли он знает, какими ресурсами пользуется.

Необходимо составить список паролей, которые следует сменить немедленно после подписания приказа или после увольнения, в зави­симости от того, какой сценарий будет выбран: жесткий или мягкий.

4. Встреча с сотрудником. Во время личной встречи до сотрудника  
доводятся претензии компании, сообщается, что принято решение о  
его увольнении, сообщается, какую работу он должен прекратить вы­полнять после этого разговора.

Необходимо обсудить порядок, время и условия увольнения.

Во время этого разговора необходимо обратить внимание на при­знаки возможной обиды или мести. Если они есть, то следует более подробно поговорить с сотрудником и убедить его, что увольнение при этом связано с сокращением штатов, говорить словами не затрагивающими профессиональное или личностное самосознание сотрудника. Некоторые компании берут с увольняемого сотрудни­ка расписку, в которой он берет на себя определенную ответствен­ность.

Сознательно не упоминаются другие аспекты увольнения: административных, законодательных, психологических. В данный момент задача — показать опасности, которые связаны с уволь­нением сотрудника. Их истинная причина кроется в невысокой бла­гонадежности. Еще одна задача — показать пути минимизации воз­можных вредных последствий для обеих сторон.

Стоит отметить и метод, используемый в некоторых российских компаниях: при приеме на работу кандидат помимо всех документов подписывает заявление об увольнении по собственному желанию и не проставляет в нем дату. Таким образом, у линейного руководителя всегда есть подписанное заявление, и он может в любой момент уволить сотрудника. Данный метод не является законным, однако иногда используется.

***Тема 5***

***Направления и меры по противодействию кадровым угрозам***

Как противостоять кадровым угрозам и промышленному шпионажу? Как обеспечить экономическую безопасность организации?

Прежде всего, необходимо провести комплекс мероприятий по управлению кадровой безопасностью, начиная с формирования сильной кадровой политики. Чтобы защитить вашу организацию от потенциальных злоумышленников, вам нужно поставить первое препятствие в процессе отбора при приеме на работу. Для этого требуются высокопрофессиональные рекрутеры, способные провести качественную экспресс-диагностику всеми доступными методами оценки как в работе с соискателем, так и с предоставленной ему документацией. Важно перепроверить информацию. При работе с резюме используйте приемы «поиск узких мест», «чтение между строк», при необходимости проведите «контент-анализ».

При проведении интервью используйте приемы «если не секрет», «перехват», задавайте уточняющие вопросы – UCQ (универсальный уточняющий вопрос – «Пожалуйста, поясните, что вы имеете в виду, когда говорите ...») и, главное правило, не продумывайте для соискателя то, что он хочет сказать!

Еще одно направление нейтрализации кадровых угроз для обеспечения безопасности организации – это работа с существующим персоналом. И в этом направлении необходимо обеспечить проведение качественного инструктажа, подкрепленного регулярным мониторингом эффективности. Также необходимо регулярно информировать персонал о понимании того, какая информация не представляет угрозы безопасности, а какая является строго конфиденциальной и не подлежит разглашению. Вплоть до подписания документов о неразглашении коммерческой тайны. Именно на этом этапе важна четкая работа службы безопасности. Хорошо продуманная система мотивации персонала может сыграть свою роль. При этом важно добиться не только полного удовлетворения сотрудников работой и результатами работы (читай – справедливой оплаты труда), но и дать возможность открыто «высказаться» (система обратной связи), не опасаясь за свое положение и угрозы увольнения. Потому что всегда есть «доброжелатель» («случайный собеседник»), готовый выслушать все секреты и использовать полученную информацию для развала организации.

Поскольку сегодня электронный документооборот осуществляется повсеместно, создаются электронные хранилища с базами данных (необходимые для успешной и эффективной работы предприятия), важным направлением обеспечения безопасности организации в части хранения и передачи информации является формирование мощного ИТ-сервиса, способного противостоять разного рода техническим сбоям и хакерским атакам. В октябре 2018 года Корпорация по управлению доменными именами и IP-адресами (ICANN) осуществила первую в истории замену криптографических ключей, защищающих систему доменных имен (DNS) в Интернете (RG.RU, 2018). Этот ключ для подписи (KSK) необходим любому пользователю Интернета. Он повышает уровень информационной безопасности. А в организациях в рамках обеспечения системы безопасности также рекомендуется время от времени с определенной регулярностью контролировать смену паролей на персональных компьютерах специалистов и сотрудников.

Нельзя игнорировать правовой аспект обеспечения безопасности организации. Важно иметь в структуре организации не только юридический отдел, но и формировать правовую грамотность специалистов и руководителей, способных предвидеть и устранять потенциальные угрозы кадровой безопасности на своем уровне. Примером может быть – неправильно начисленная заработная плата; ошибки в исполнении договоров при приеме на работу (прежде всего терминологические) и при увольнении сотрудников; ошибки в ведении финансовых документов; ошибки в принятии управленческих решений, приводящие к конфликту с персоналом и т.д.

Механизм расследования преступлений представим на рисунке.

Технологии также используются для отслеживания экономических преступлений. В России все больше и больше компаний используют технологии в качестве основного инструмента для выявления экономических преступлений, чем в мире в целом, особенно в таких сферах как выявление мошенничества, противодействие взяточничеству и коррупции, а также комплексная проверка надежности деловых партнеров. Несомненно, киберпреступники берут на вооружение и технологии. В условиях пандемии, когда бизнес перешел в онлайн, а все коммуникации осуществляются через корпоративные сети, количество кибератак на бизнес-инфраструктуру неуклонно многократно увеличивается. По данным Group IB (2020), в 2019 году многие операторы программ-вымогателей отошли от атак на обычных пользователей и переключили свое внимание на компании из различных отраслей и государственные органы. Нападения на эти жертвы приносят большую пользу злоумышленникам.

Обычно существуют следующие начальные векторы атаки:



− вредоносные электронные письма;

− получение доступа к внутренней сети путем компрометации данных аутентификации;

− работа общедоступных приложений, в том числе связанных с VPN.

После первоначального компромисса; многие криптографические операторы сначала пытаются получить более высокие права доступа, а затем пытаются получить доступ к другим учетным записям с помощью различного программного обеспечения. Количество проданных доступов к корпоративным сетям увеличивается из года в год, но основной пик продаж пришелся на 2020 год, рост в 2,6 раза. Ожидается появление специализированных торговых площадок для размещения лотов с доступом к корпоративным сетям, что может привести к еще большему увеличению инцидентов.

Официальные данные также подтверждают эти тенденции. В первом полугодии 2020 года количество преступлений в сфере информационных технологий в России увеличилось на 91,7% по сравнению с аналогичным периодом прошлого года, а доля этих противоправных действий в общей структуре преступности достигла 22,3% (МВД России, 2020).

В заявлении SEC США (2018) отмечается, что компании сталкиваются с постоянно меняющимся ландшафтом угроз кибербезопасности, в котором хакеры используют сложный набор инструментов для проведения кибератак, включая использование украденных данных доступа, вредоносных программ, программвымогателей, отлова и структурированных запросов. атаки языка ввода и распределенные атаки отказа в обслуживании, среди прочего (Комиссия по ценным бумагам и биржам (SEC), 2018). Цели кибератак широко варьируются и могут включать в себя кражу или уничтожение финансовых активов, интеллектуальной собственности или другой конфиденциальной информации, принадлежащей компаниям, их клиентам или их деловым партнерам.

Кибератаки также могут быть направлены на нарушение деятельности публичных компаний или их деловых партнеров. В целях защиты интересов инвесторов SEC потребовала от публичных компаний информировать инвесторов о значительных рисках и инцидентах в области кибербезопасности.

Требование является обязательным не только для компаний, подвергшихся кибератакам, но и для тех, кто подвержен значительным рискам кибербезопасности, но, возможно, еще не стал целью кибератак. Механизм защиты коммерческой тайны на предприятии представлен на рис. 7

Каковы основные каналы утечки информации? Это:

− человек;

− документ;

− изделие-процесс.

По данным каналам утечки информации выделяют и направления расследования по факту разглашения коммерческой тайны. Зная источники, можно рассмотреть и механизм защиты коммерческой тайны на предприятии. В рамках действующего механизма защиты информации следует уделить внимание пакету документов:

− Постановление РСФСР от 05.12.91 г. № 35 «О перечне сведений, которые не могут составлять коммерческую тайну»;

− Положение по защите коммерческой тайны организации;



Рис. 7 Механизм защиты коммерческой тайны на предприятии

− Положение о конфиденциальном производстве в организации;

− Положение о службе безопасности организации;

− Положение о защите информации в отношении с контрагентами;

− Инструкция по защите конфиденциальной информации в информационной системе организации;

− Обязательство о неразглашении коммерческой тайны организации;

− Перечень сведений, составляющих коммерческую тайну.

По мере необходимости могут быть составлены и другие документы.

*Меры предотвращения рисков*

Трудоустройство граждан.

С лицами, кто претендует на должность, заключают один из видов контрактов:

− коммерческий (документ, представляющий собой договор поставки товаров или предоставления услуг);

− трудовой (вид трудового договора, заключающегося в письменной форме со всеми постоянными или временными работниками).

В контракте в письменной форме должны быть оговорены договорные условия с сотрудником:

− согласие лица на сбор информации о его биографических и других данных, характеризующих личность;

− особо оговорить, что такого рода сбор информации проводится как до вступления контракта в силу (например, во время прохождения испытательного срока), так и во время его реализации, т.е. до расторжения контракта.

Содержание информации в проверяемого:

− преступления и административные проступки, совершенные им в прошлом;

− судебные процессы по гражданским делам, в которых он выступал в качестве истца или ответчика;

− качество исполнения ранее заключаемых договоров с другими партнерами;

− участие в организациях, дискриминирующих по признакам пола, расы, цвета кожи, убеждениям, религиозной и национальной принадлежности;

− жизнь не по средствам;

− наличие значительных финансовых накоплений сомнительного происхождения;

− систематические посещения проверяемого лицами, не имеющими отношения к его служебным обязанностям;

− факты отказа от использования очередного отпуска;

− результаты различных тестов;

− семейные проблемы;

− долги и займы и т.д.;

− болезни, которые он перенес ранее;

− материальное положение;

− случаи увольнения с работы по отрицательным мотивам, не нашедшие отражение в трудовой книжке;

− аморальные проступки (пьянство, наркотики и т.д.);

− суждения бывших сослуживцев и руководителей о его профессиональных и моральных качествах;

− необоснованный и нелогичный отказ от продвижения по службе, перевода на новое место работы;

− жалобы клиентов и других лиц, контактирующих с проверяемым;

− прогулы и частые отвлечения от выполнения служебных обязанностей;

− задержки по надуманным предлогам на работе после окончания рабочего дня.

*Как распознать неблагонадежного партнёра*

Некредитоспособным признается тот партнер, у которого для получения кредита нет предпосылок, подтверждающих способность возвратить его.

Характеристики некредитоспособного партнера:

1 Неаккуратность при расчетах по ранее полученным

2 Ухудшение текущего финансового положения.

3 Неспособность при необходимости мобилизовать денежные средства из различных источников.

4 Обналичивание денежных средств в объемах, превышающих размеры фонда зарплаты.

5 Удержание им (без согласия партнера) денежных средств, полученных в качестве кредита или предварительной оплаты.

6 Совершение операций с банковскими документами необеспеченными кредитными ресурсами.

7 Нецелевое использование кредитных средств или их получение по фиктивным документам.

8 Попытка оттянуть выплату денежных средств партнеру при добросовестном выполнении им условий контракта и т.д.

Служба безопасности обязана выявлять некредитоспособных партнеров как до заключения, так и в процессе реализации досвоевременно информировать об этом руководство предприятия.

Ненадёжность делового партнёра определяется:

1 Большим количеством сорванных по его вине сделок с другими фирмами.

2 Несвоевременным и некачественным выполнением условий заключенных договоров.

3 Значительным количеством в фирме ранее судимых лиц.

4 Фактами ведения против предприятия-учредителя экономического шпионажа.

5 Отсутствием доверия потребителей.

6 Испорченной репутацией среди деловых кругов.

7 Нерегулярной и ненадежной поставкой сырья и товаров.

8 Умышленным затягиванием деловых переговоров.

9 Предъявлением к нему значительного количества судебных исков.

10 Наличием большого долга.

11 Непрочной позицией на рынке.

12 Использование помощи сотрудников правоохранительных органов, налоговых инспекций и т.д. с целью парализации экономической деятельности своего партнера.

13 Неуважительным отношением к авторскому или патентному праву.

Известно, что в рамках гражданского производства судами

рассматриваются:

− споры о гражданском праве, затрагивающем права и законные интересы юридического лица (предприятия);

− по жалобе на действия административных органов или должностных лиц, совершенные с нарушением их полномочий;

− дела об установлении фактов, имеющих юридическое значение, рассматриваемые и разрешаемые судом.

Необходимость в сборе информации сотрудниками службы безопасности обычно возникает в следующих случаях:

1 Выявления свидетелей и документов.

2 Проверки достоверности информации участников процесса и подлинности доказательств, представленных на суде.

3 Возникновения необходимости проверки наличия основания для отвода в рассматрении дела.

4 Оказания помощи суду в установлении фактического местонахождения участников процесса.

5 Выявления лиц, оскорбляющих или оклеветавших руководителей предприятия-учредителя.

6 Поиска утаиваемого от суда имущества процессуального противника, необходимого для погашения материального ущерба.

7 Необходимости выявления среди свидетелей лиц, которые в силу своих физических или психических недостатков не способны правильно воспринимать факты или давать о них правильные показания и т.д.

***Тема 6***

В арсенале методов целенаправленного силового воздействия на персонал имеется огромное число явных и скрытых методов. К явным методам силового воздействия относят дискриминацию и насилие на рабочих местах; коррупцию, подкуп и взяточничество; методы, наносящие материальный ущерб организации - воровство, хищения, откаты и другие виды мошенничества, а также крайние формы воздействия, такие как террористические акты, заказные убийства руководителей и VIP-специалистов, отчуждения активов, утечка и «слив» информации. Эти методы воздействия на персонал будут представлены в других частях настоящего учебного пособия.

Особенностью же методов скрытого воздействия, которые также носят активный и агрессивный характер, является то, что обнаружить их присутствие и вовремя отреагировать удается не всегда и не сразу.

В связи с этим особенно важно познакомиться с ними, чтобы знать, как можно эффективно противостоять им для предотвращения массовых и ощутимых угроз кадровой безопасности организации.

Поскольку методы тайного воздействия направлены прежде всего на психику человека, поэтому данное учебное пособие начинаем именно с разбора психологического поведения людей, которое совершенно неоднозначно, иррационально в своем понимании. Людьми, которые испытывают непонятную для них неуверенность в себе, неудовлетворенность и различного рода страхи очень удобно манипулировать и управлять.

Следует подчеркнуть еще один важный аспект. Когда речь идет об угрозе кадровой безопасности, нужно понимать, что эта угроза наносит вред в двух направлениях.

С одной стороны, она касается, прежде всего, самой организации, и которая не всегда может защитить себя от неблагонадежности собственных сотрудников или даже тех, кто ранее входил в число её сотрудников и преследовал свои собственные нечистоплотные интересы, предавая интересы организации, «сливая» информацию конкурирующим компаниям. С другой стороны, угроза кадровой безопасности имеет вектор, направленный на персонал данной конкретной организации, который был так или иначе обижен либо уволен с конфликтом. В обоих случаях мы имеем совершенно неприглядные последствия. Однако их можно избежать или не допускать.

Особенности поведения сотрудников на рабочих местах обусловлены социально-психологическими проблемами, связанными с испытываемыми страхами и неуверенностью, имеющимися у сотрудника или навязанными со стороны руководителей по поводу успешности и перспектив их дальнейшей трудовой деятельности в организации. Особенно данные эмоции сотрудники испытывают в переломные моменты трудовой деятельности, связанные с кризисными явлениями в экономике государства, выбора нового стратегического курса развития организации, внедрения новой техники и технологии на местах. Так или иначе, в период любых нововведений сотрудники демонстрируют не всегда рациональное поведение, которое зачастую приводит в некоторое недоумение всех, кто взаимодействует с ними.

Для того, чтобы успешно выстраивать отношения в трудовом коллективе, руководителю крайне важно правильно понимать траекторию линии поведения своих подчиненных с тем, чтобы грамотно принимать управленческое решение, распределять функции и профессиональные обязанности.

Несмотря на важность перемен, многие люди отвергают их. Они боятся перемен и противостоят им, потому что перемены ставят под угрозу привычные идеи и мнения. Тем не менее, есть методы, которые позволяют решить проблему сопротивления переменам.

В организации существует два типа людей: Люди, убежденные, что они – жертвы перемен. Они сопротивляются, злятся и нередко впадают в депрессию. Люди, которые полностью поддерживают перемены, разрабатывают и реализуют их. Сопротивление оказывается особенно сильным на начальной стадии реализации перемен, потому что некоторые люди чувствуют себя неуверенно и воспринимают предложенные перемены как угрозу. Возникают конфликты, участники которых часто вспоминают «старое доброе время».

Решение проблемы сопротивления переменам.

Тем не менее, есть методы, которые позволяют решать обозначенные выше проблемы сопротивления переменам, например:

− Создайте комфортную обстановку и атмосферу включенности в процесс перемен. Развивайте у сотрудников уверенность в своих силах и приверженность к переменам, давайте им возможность понять их собственные интересы и реализовать их в работе так, чтобы это способствовало осуществлению общих целей организации.

− Общайтесь с сотрудниками напрямую, сообщайте им информацию о содержании организационной системы сбалансированных показателей и связанных с ней переменах. Давайте работникам своевременную информацию.

Молчание руководства порождает сомнения и распространение слухов, которые подрывают доверие к менеджерам. Не сообщайте сразу слишком много информации, так как работникам нужно время, чтобы ее «переварить».

− Поддерживайте аргументированные предложения.

− Информируйте работников о преимуществах перемен и о том, как они помогут улучшить ситуацию в будущем.

− Встречайтесь с людьми, которые сопротивляются переменам, и давай те детальные ответы на их возражения.

− Подключайте ключевых людей к процессу принятия решений. Если заинтересованные люди участвуют в принятии решений, им легче их принять, благодаря чему реализация решений облегчается.

− Если сопротивление слишком сильное и вы не можете рассчитывать на поддержку большинства сотрудников, приостановите проект.

− Нейтрализуйте страх и недоверие: они мешают сотрудникам учиться новому.

***Лояльность сотрудника*** - это «верность, преданность сотрудника целям и ценностям компании, осуществление деятельности, которая поддерживает и помогает реализовать эти цели» [1]. Лояльность сотрудника влияет на кадровую безопасность предприятия. Влияние лояльности персонала на кадровую безопасность компании

Кадровая безопасность – «это процесс предотвращения негативных воздействий на экономическую и социальную безопасность предприятия за счет рисков и угроз, связанных с персоналом, его интеллектуальным потенциалом и трудовыми отношениями в целом» [2].

Кадровая безопасность, в первую очередь, зависит от благоприятного отношения сотрудников к работодателю и компании. Это отношение зависит от уровня лояльности сотрудника, которая сказывается на производительности той или иной организации. Одним из условий обеспечения кадровой безопасности организации является сохранение лояльности персонала.

Лояльность является условием формирования у сотрудников профессиональной мотивации, которая в дальнейшем сказывается на всей деятельности организации. Такой персонал всегда дорожит рабочим местом в своей компании, стремится качественно выполнять свои задачи и при этом побуждает к этому своих коллег. Только лояльные сотрудники преданы компании и неравнодушны к ее интересам, стремятся проявлять инициативу, не совершают противоправных действий и выполняют все установленные организацией нормы и правила.

Заинтересованность, наблюдательность и преданность сотрудников позволят им находить новые средства получения преимуществ перед конкурирующими компаниями, что в дальнейшем благоприятно сказывается на деятельности организации.

Лояльный персонал играет важную роль в производительности компании, так как:

- лояльные сотрудники способны сохранять коммерческие секреты фирмы, контролировать возможные угрозы и устранять их;

- лояльные сотрудники используют все ресурсы компании для достижения высоких результатов в своей работе, при этом ресурсами являются консультации у специалистов, самостоятельное исследование;

- лояльные сотрудники более ответственны, чувствуют свою обязанность перед организацией сделать все не только в срок, но качественно;

- лояльные сотрудники могут сохранить лидерские позиции предприятия, если это в сочетании с правильной стратегией, конкурентоспособными товарами и услугами.

Нелояльные сотрудники – это те «сотрудники, которые равнодушны к ценностям компании и ее целям, не готовы прилагать усилия для достижения этих целей» [3]. Исследование показало, что на отсутствие лояльности может указывать следующее:

- склонность сотрудников к обману;

- невыполнение функций и обязательств полностью, игнорирование поручений;

- проявление бездействия в критических ситуация;

- негативное высказывание в адрес компании своим коллегам и клиентам, конкурентам;

- склонность к превышению полномочий;

- готовность покинуть компанию при любой возможности;

- несоблюдение норм и правил, установленных организацией;

- проявление спокойного отношения как к успехам организации, так и к неудачам.

Нелояльные сотрудники способны передавать (продавать) конфиденциальную информацию конкурентам, что в дальнейшем может оказать негативное влияние на компанию. Такие сотрудники опасны еще и тем, что могут переубедить коллег, обсуждая с ними реальные или выдуманные недостатки предприятия, обеспечив этим себе большую поддержку и ухудшив психологический климат в коллективе

В настоящее время каждый современный бизнес стремится к созданию кадровой стабильности, что является одним из условий эффективной работы организации и ее благополучного развития. В свою очередь, кадровая стабильность — это одна из основных целей кадровой безопасности бизнеса. При высоком уровне стабильности кадров происходит минимизация экономических рисков, а именно таких как: хищение или мошенничество, связанные с активами организации; поломки, кражи, порчи оборудования; утрата информационных ресурсов и технологий путем шпионажа; искажение информации; формирование нежелательного имиджа; снижение количества и качества человеческих ресурсов [1]. Для обеспечения кадровой безопасности используют систему мотивации и лояльности персонала. От их эффективного формирования и реализации зависит корректное и уважительное отношение персонала к организации, а также личная заинтересованность сотрудников в ее развитии.

Необходимо отметить, что для эффективной мотивации сотрудников следует повысить уровень их лояльности, что определенно преумножит заинтересованность к достижению поставленных руководством целей. Оптимизировать человеческие ресурсы предприятия можно с помощью инструментов мотивации и лояльности. Методы мотивации делятся на два вида: материальные и нематериальные и в российских компаниях, можно сделать вывод, что чаще всего компании используют одновременное несколько видов премий. Из них наиболее распространены ежегодные, ежеквартальные и ежемесячные премии (60,9%), далее премии по итогам выполнения ключевых показателей эффективности (54,5%) и реже всего, ситуативные нерегламентированные премии (42,3%).

Инструменты нематериальной мотивации также обычно используют в комплексе. Праздничные корпоративные мероприятия — самый популярный метод (58,2%), еще используют такие методы как: обучение (56,9%) и публичная похвала успешных сотрудников (51,6%). Удивительно то, что популярность тимбилдингов не так велика: всего 22,9% руководителей используют в командообразовании принципы тимбилдинга. Также в качестве мотивации некоторые компании (11,8%) готовы выделять сотрудникам дополнительные выходные дни, что происходит чаще всего между продолжительными праздниками, когда, итак, трудовая активность на низком уровне.

Среди факторов материальной лояльности в российских компаниях наиболее распространены заработная плата/премии/бонусы (80,9%), социальный пакет (75,9%), возможность профессионального развития и обучение персонала. (52,1%) и возможность роста по карьерной лестнице (56,7%). Судя по опросу чаще всего используют от двух до четырех факторов лояльности. Факторы нематериальной лояльности используют в комплексе с материальными факторами. Наиболее популярные факторы — наличие корпоративной культуры (63,8%), коллективное проведение мероприятий (43,6%), публичная похвала успешных сотрудников (42,4%) и стимулирование отлично работающих сотрудников (32,5%). В связи с последними событиями в мире 403 компании выделился такой фактор, как возможность частично работать удаленно (23,8%)