



Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Магнитогорский государственный технический университет им. Г.И. Носова»

Е.Г. Зиновьева

КАДРОВАЯ БЕЗОПАСНОСТЬ ОРГАНИЗАЦИИ

*Утверждено Редакционно-издательским советом университета
в качестве учебного пособия*

Магнитогорск
2021

УДК 331.101.1(075.8)
ББК 65.242я73

Рецензенты:

кандидат философских наук
директор ООО «Орион»
А.Ю. Жилин

кандидат экономических наук, доцент,
начальник финансово-экономического отдела,
ФГБОУ ВО «Магнитогорский государственный технический
университет им. Г.И. Носова»
И.А. Агеева

Зиновьева Е.Г.

Кадровая безопасность организации [Электронный ресурс] : учебное пособие / Екатерина Георгиевна Зиновьева ; ФГБОУ ВО «Магнитогорский государственный технический университет им. Г.И. Носова». – Электрон. текстовые дан. (0,94 Мб). – Магнитогорск : ФГБОУ ВО «МГТУ им. Г.И. Носова», 2021. – 1 электрон. опт. диск (CD-R). – Систем. требования : IBM PC, любой, более 1 GHz ; 512 Мб RAM ; 10 Мб HDD ; MS Windows XP и выше ; Adobe Reader 8.0 и выше ; CD/DVD-ROM дисковод ; мышь. – Загл. с титул. экрана.

ISBN 978-5-9967-2187-0

В учебном пособии рассмотрены проблемы кадровой безопасности как феномена организации, система управления кадровой безопасностью в организации, проанализированы вопросы развития лояльности и контроля персонала в контексте технологии кадровой безопасности организации.

Рекомендуется для обучающихся всех форм обучения по направлению 38.03.03 «Управление персоналом», а также может быть полезна руководителям органов государственной власти, специалистам кадровых служб, занимающихся вопросами подбора, отбора и аттестации работников.

УДК 331.101.1(075.8)
ББК 65.242я73

ISBN 978-5-9967-2187-0 © Зиновьева Е.Г., 2021
© ФГБОУ ВО «Магнитогорский государственный
технический университет им. Г.И. Носова», 2021

Содержание

ВВЕДЕНИЕ	4
1. КАДРОВАЯ БЕЗОПАСНОСТЬ ОРГАНИЗАЦИИ: ПОНЯТИЕ И СУЩНОСТЬ	6
1.1. Представления о кадровой безопасности организации	6
1.2. Риски и угрозы кадровой безопасности	10
1.3. Типы противоправного поведения персонала в организации	17
Контрольные вопросы и задания	28
2. СИСТЕМА УПРАВЛЕНИЯ КАДРОВОЙ БЕЗОПАСНОСТЬЮ В ОРГАНИЗАЦИИ	31
2.1. Структура управления кадровой безопасностью в организации	31
2.2. Субъекты и объекты системы управления кадровой безопасностью в организации	42
2.3. Условия эффективного функционирования системы управления кадровой безопасностью	50
Контрольные вопросы и задания	60
3. ТЕХНОЛОГИЯ ОБЕСПЕЧЕНИЯ КАДРОВОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ	64
3.1. Обеспечение кадровой безопасности при найме и увольнении персонала	64
3.2. Развитие лояльности персонала для обеспечения кадровой безопасности организации	79
3.3. Контроль персонала как условие обеспечения кадровой безопасности организации	90
Контрольные вопросы и задания	105
ГЛОССАРИЙ	108
БИБЛИОГРАФИЧЕСКИЙ СПИСОК	112

ВВЕДЕНИЕ

Вопросы обеспечения кадровой безопасности являются важными для любой организации. В настоящих реалиях, когда основой функционирования каждого хозяйствующего субъекта является преодоление кризисных ситуаций и получение наибольшего дохода, безопасность является неперенным условием, определяющим эффективность его функционирования.

На современном этапе развития каждое предприятие нуждается не только в стремлении взаимодействовать со всеми заинтересованными лицами на рынке предоставляемых услуг и товаров, но и в сохранении своей уникальности и целостности. Конкурентоспособность, успех в продвижении своего бизнеса, а также способность занимать лидирующие позиции на рынках зависят от правильно составленной кадровой составляющей предприятия. Грамотно подобранная система деятельности служб кадровой безопасности предприятия, способная вовремя распознавать и противостоять разнообразным угрозам, необходима для достижения намеченных планов и бизнес-идей. Ведь кадровая безопасность, а именно ее обеспечение, выступает в роли направления работы любого современного предприятия.

Целями освоения дисциплины является приобретение обучающимися необходимой знаний и навыков для обеспечения в организации безопасности в работе с персоналом; формирование у обучающихся представлений об кадровой безопасности организации; приобретение практических навыков по оценке кадровой безопасности организации и управлению рисками.

Задачами дисциплины являются:

- изучить современные подходы к понятию кадровая безопасность и формам ее регулирования и организации;
- изучить причины нарушения кадровой безопасности, наиболее уязвимые места в организационной работе с персоналом компании, источники кадровых рисков;
- освоить навыки построения эффективных систем защиты кадрового развития организации на всех его этапах начиная от набора и заканчивая увольнением персонала компании;
- рассмотреть современные подходы к понятию коммерческая тайна и методам ее защиты;
- изучить организационно-правовые и административные методы обеспечения кадровой безопасности организации.

В результате освоения дисциплины обучающийся должен:

знать:

- основы применения информационно-коммуникационных технологий
- основы возникновения, профилактики и разрешения трудовых споров и конфликтов в коллективе

уметь:

- решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры
- регулировать трудовые споры и конфликты в коллективе

владеть:

- навыками получения информации из различных источников, включая Интернет; навыками работы с базами данных официальных сайтов

- навыками диагностики и управления конфликтами и стрессами в организации

Учебное пособие содержит:

- теоретический материал для самостоятельного изучения разделов курса;
- контрольные вопросы и задания, позволяющие проверить качество освоения каждой темы;

- глоссарий ключевых понятий по дисциплине;

- библиографический список, рекомендуемый для более глубокого изучения отдельных вопросов.

Рекомендуется для обучающихся всех форм обучения по направлению 38.03.03 «Управление персоналом», а также может быть полезна руководителям органов государственной власти, специалистам кадровых служб, занимающихся вопросами подбора, отбора и аттестации работников.

1. КАДРОВАЯ БЕЗОПАСНОСТЬ ОРГАНИЗАЦИИ: ПОНЯТИЕ И СУЩНОСТЬ

1.1. Представления о кадровой безопасности организации

Кадровая безопасность – это процесс минимизации рисков негативных воздействий на корпоративную безопасность компании за счет устранения угроз, связанных с персоналом, его деструктивным потенциалом и негативными аспектами трудовых отношений в целом. Она включает в себя защиту от разглашения коммерческих тайн, промышленного шпионажа и некомпетентности сотрудников.

Цели кадровой безопасности:

- формирование целостного представления о кадровой безопасности и ее взаимосвязи с другими элементами безопасности организации;
- определение путей реализации мероприятий, которые обеспечивают необходимый уровень кадровой безопасности.

Задачи обеспечения кадровой безопасности:

- своевременное выявление реальных и потенциальных угроз жизненно важным интересам компании со стороны персонала;
- эффективное противодействие и борьба с факторами, препятствующими реализации законных интересов компании и ее сотрудников;
- сохранение интеллектуальной и материальной собственности компании;
- разработка и реализация механизма оперативного реагирования на возникающие негативные условия и тенденции развития компании;
- сбор информации, анализ, оценка и предотвращение нежелательных и неправомерных действий сотрудников в отношении компании;
- предотвращение проникновения в организацию криминальных элементов и субъектов противоправной деятельности;
- формирование требований к сотрудникам относительно кадровой безопасности;
- составление нормативной документации, проведение информационно-разъяснительной работы, мониторинг системы кадровой безопасности.

Факторы, влияющие на кадровую безопасность организации (Хорев А.И., Горковенко Е.В., Платонова И.В., 2014)¹ (рисунок 1 – 2).

Безопасность жизнедеятельности как составная часть кадровой безопасности включает:

- *безопасность здоровья* – создание безопасных условий труда сотрудников, предупреждение травматизма и профессиональных заболеваний персонала;

¹ Хорев, А.И. Управление кадровой безопасностью организации / А.И. Хорев, Е.В. Горковенко, И.В. Платонова // Актуальные проблемы гуманитарных и естественных наук. – 2014. – № 11. – С. 181 – 184.

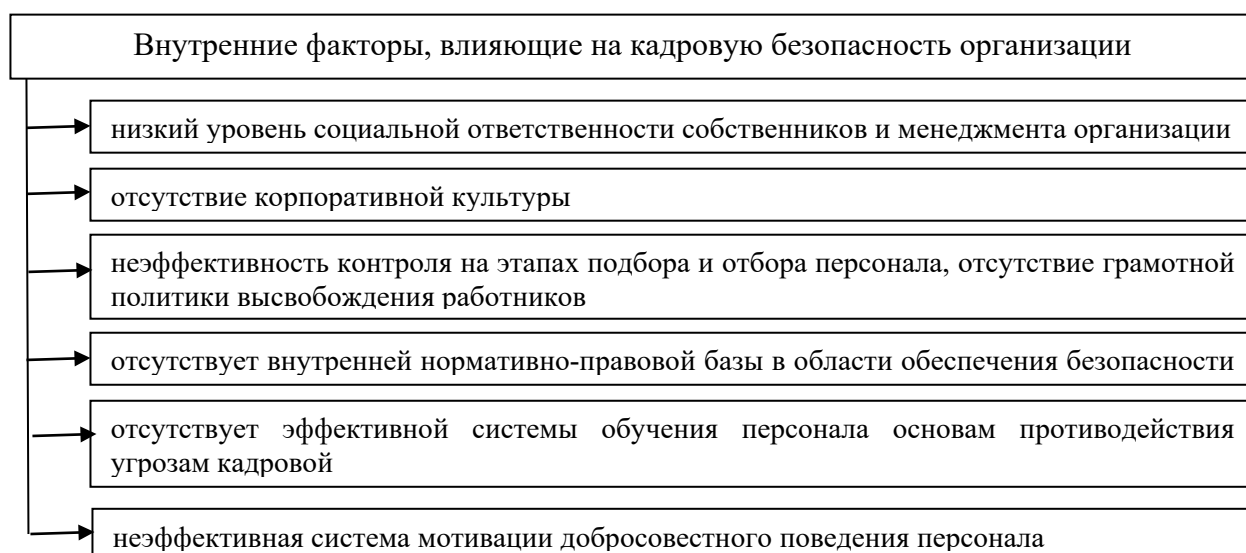


Рис. 1. Внутренние факторы, влияющие на кадровую безопасность организации

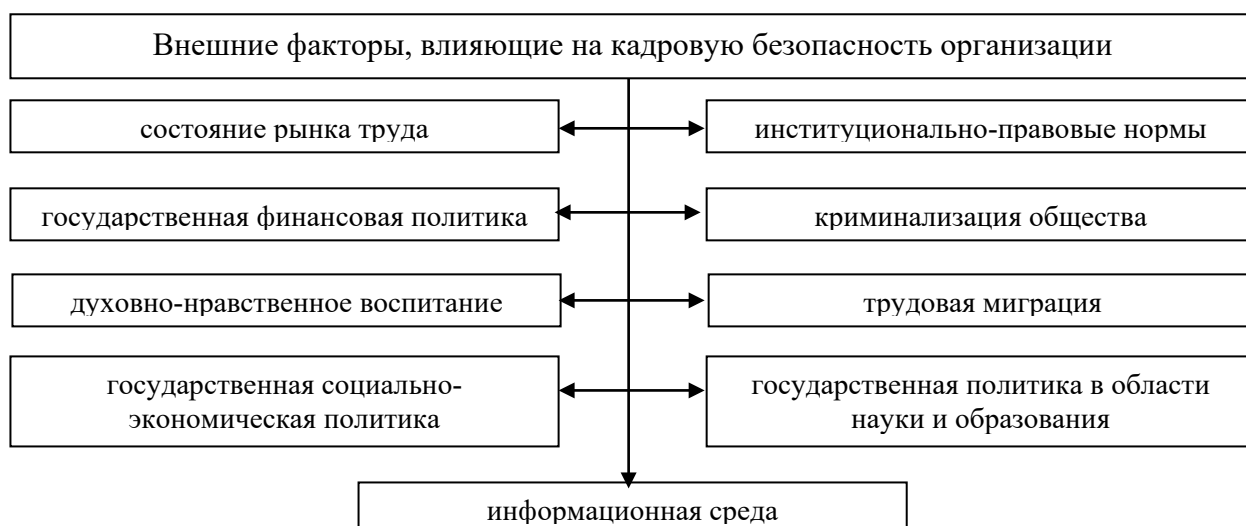


Рис. 2. Внешние факторы, влияющие на кадровую безопасность организации

Структура кадровой безопасности организации представлена на рисунке 3.

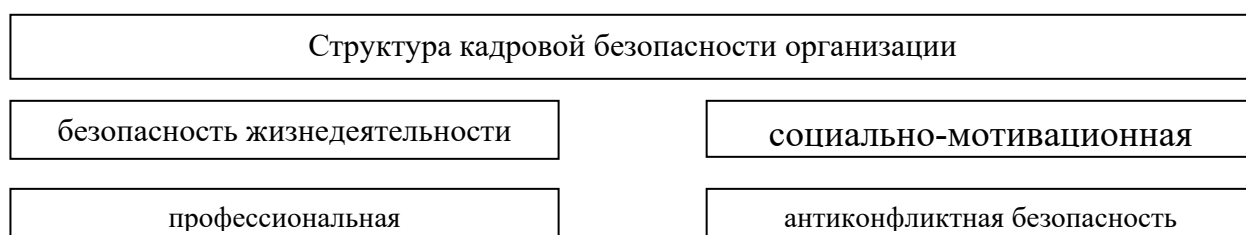


Рис. 3. Структура кадровой безопасности организации

– *физическую безопасность* – выполнение комплекса мероприятий по недопущению внешних опасностей персонала, связанных с их служебной деятельностью, или членам их семей.

Элементы **социально-мотивационной** составляющей кадровой безопасности:

– *карьерная безопасность* – профессионально-квалификационное должностное продвижение работников, поощрение в повышении своей квалификации требованиям функциональных обязанностей, в гарантиях производственного роста, получение шансов для самореализации на рабочем месте;

– *финансовая безопасность* – денежная обеспеченность, которая соответствует объему, квалификации, качеству выполненной работы; уверенность работников в своем рабочем месте, стабильности оплаты труда;

– *технологическая безопасность* – система анализа и прогнозирования, направлена на создание современного оборудования рабочего места, новейших технологий, использование передового опыта;

– *эстетическая безопасность* – проведение общеобразовательных семинаров, конференций, групповых дискуссий; мотивация на удовлетворение персонала своей работой, улучшение собственного имиджа каждого работника;

– *административно-независимая безопасность* – обеспечение объективного оценивания результатов труда и выявление потенциала каждого работника, невозможность назначения неподготовленных и некомпетентных кадров, находящихся в родстве с собственниками (учредителями, акционерами и др.).

В состав **профессиональной безопасности** входят:

– *безопасность труда* – создание безопасных условий труда в банке;

– *интеллектуальная безопасность* – уровень владения современными знаниями, внедрение новаций в развитие персонала, повышение уровня профессиональных знаний, навыков, умений, стимулирование проявления инициативы и способностей, путем создания гибкой системы премирования в соответствии с развитием научно-технического прогресса;

– *пенсионно-страховая безопасность* – социальная защита работников, их страхование, преференции качественного медицинского обслуживания.

Антиконфликтная безопасность имеет следующие составляющие:

– *психолого-коммуникационная безопасность* – согласованность, бесконфликтность общения на социальном личностном уровнях, товарищеская взаимопомощь, требовательность к себе и другим в интересах производства, содействие положительным межличностным коммуникациям, создание благоприятного микроклимата, учета интересов пожеланий работников по вертикали и горизонтали, доброжелательный и уважительный стиль общения «руководитель – подчиненные»;

– *патриотическая безопасность* – создание психологического климата в коллективе на основе положительного отношения к компании, психологического единения работников вокруг общих целей.

С принципами формирования политики безопасности персонала тесно связаны требования, предъявляемые к менеджменту организации (рисунок 4).

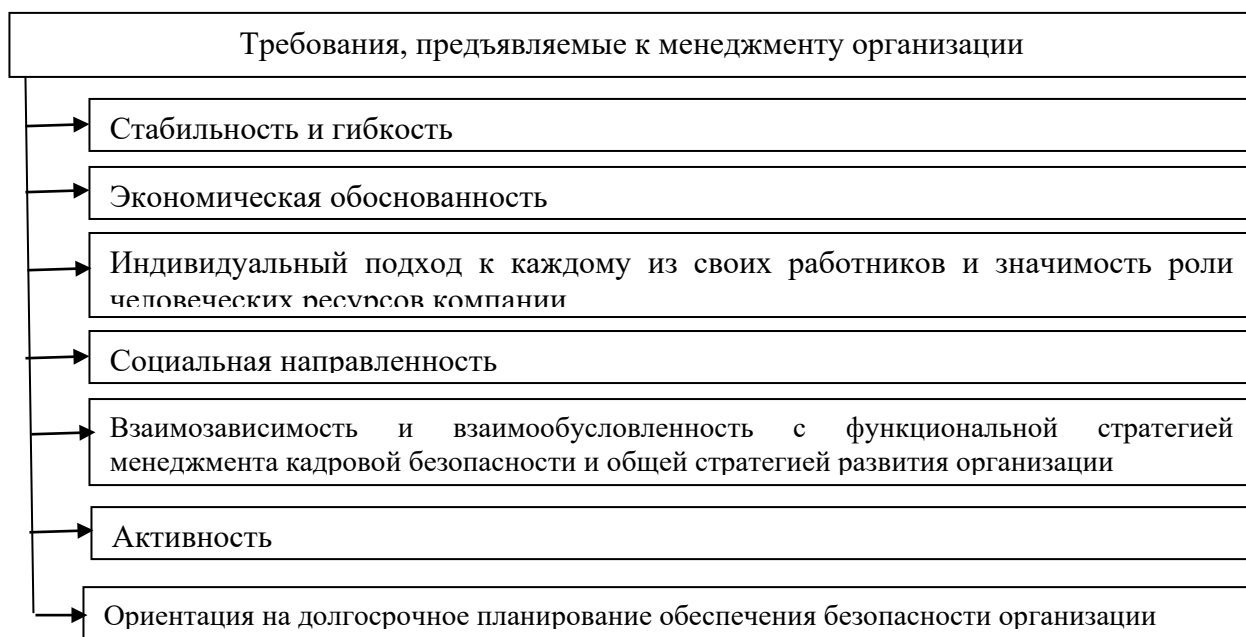


Рис. 4. Требования, предъявляемые к менеджменту организации

Кадровая безопасность организации направлена на минимизацию угроз от собственного персонала как внутренней угрозы. К таким угрозам относятся:

- неквалифицированное руководство, ошибки в разработке внедрении стратегий банка;
- низкая квалификация персонала организации;
- разглашение конфиденциальной информации;
- низкая организация хранения информации, материальных и финансовых ценностей;
- недостаточное изучение клиентов, партнеров, конкурентов и других рыночных субъектов.

В теории кадровой безопасности работники позиционируются одновременно в двух направлениях – как объекты и как субъекты потенциальных угроз. Сотрудник организации может стать объектом такой угрозы со стороны конкурирующей организации, как, например, склонение его к нарушению доверия работодателя в форме разглашения конфиденциальной информации. Для этого могут использоваться разнообразные методы (подкуп, шантаж и др.). В случае если он примет предложения конкурента своего работодателя, то его статус автоматически изменится. Из объекта угрозы кадровой безопасности указанный сотрудник превратится в ее субъекта, а объектом будет выступать уже информационная безопасность соответствующей организации.

Существует заблуждение, связанное с тем, что кадровой безопасностью должна заниматься только служба безопасности. Однако вся деятельность служб персонала может быть разложена на этапы (поиск, отбор, прием, адаптация и т. д. вплоть до увольнения и далее) и на каждом этапе присутствует

масса вопросов безопасности, решаемых именно этими специалистами. Любое действие менеджера по персоналу на любом этапе – это либо усиление, либо ослабление безопасности компании по главной ее составляющей – по кадрам.

По статистике, около 80% ущерба материальным активам компаний наносится их собственным персоналом. Только 20% угроз корпоративной безопасности приходит извне. Также невозможно обойти вниманием и общемировую статистику, применимую к России: 10-15% всех людей являются нечестными по определению, 10-15% абсолютно честны, остальные 70-80% – колеблющиеся, то есть те, кто поступит нечестно, если риск попасться будет минимальным.

Таким образом, **субъекты кадровой безопасности** – сотрудники, непосредственно занятые обеспечением безопасности (рисунок 5).

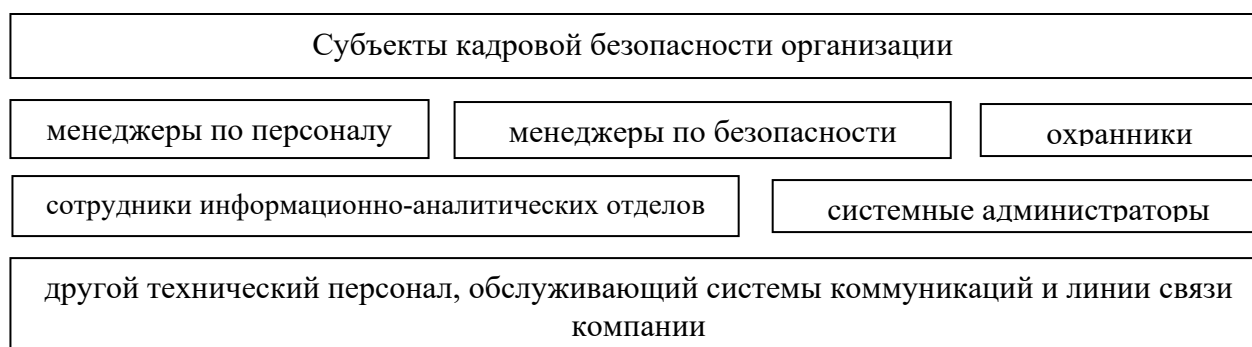


Рис. 5. Субъекты кадровой безопасности

1.2. Риски и угрозы кадровой безопасности

Суть мероприятий по обеспечению кадровой безопасности – защита деятельности от вероятных угроз и рисков, вызванных человеческим фактором.

В *экономической науке* **риск** – это возможность появления негативного инцидента в будущем и размер последствий после него. Под **угрозой** же понимается намерение нанести какой-либо вид вреда. Риск и угроза чаще всего рассматриваются очень близко; данные понятия имеют похожие характеристики.

При решении проблем обеспечения безопасности организации важную роль играет знание кадровых рисков и угроз, которые могут исходить от персонала организации и в его адрес.

Кадровый риск – ситуация, отражающая опасность нежелательного развития событий, которые напрямую или косвенно затрагивают функционирование и развитие организации, персонала, общества в целом и наступление которых связано с объективно существующей неопределенностью, обусловленной рядом причин: неэффективностью системы управления персоналом, поведением, действием (бездействием) персонала, внешней средой организации.

Есть несколько **причин**, по которым компании считают, что риски человеческого капитала являются наибольшей угрозой их бизнесу. Наиболее важная из них – острая нехватка кадров в отдельных отраслях и регионах.

Например, в России проблемы возникают с ИТ-специалистами, потому что информация о том, как работают ИТ-системы компании, замыкается в голове одного человека, и если он уходит, то новому специалисту приходится осваивать все заново. Еще один риск связан с тем, что многие компании начинают заниматься в России деятельностью, по которой отсутствует образовательная подготовка, например, риск-консалтинг. Существуют также проблемы миграции населения, старения персонала.

Руководитель и HR-менеджеры проявляют готовность идти на определенные кадровые риски, поскольку наряду с риском потерь существует возможность дополнительных доходов. Такая возможность основана на признании принципиальных отличий человеческих ресурсов организации от иных материальных, природных или финансовых ресурсов. Эти отличия заключаются в следующем:

- наличие интеллекта у работника, а, следовательно, возможности качественных преобразований иных видов ресурсов и технологий их использования;
- способность к постоянному самосовершенствованию и саморазвитию;
- возможность долговременного характера взаимоотношений организации и человека на основе сближения интересов и формирования лояльности по отношению к компании;
- уникальность каждого человека, креативные способности, позволяющие создать во взаимодействии с другими сотрудниками неповторимую инновационную культуру;
- синергетический эффект компетенций сотрудника, рождающийся при получении им второго (третьего) образования или специальности.

Деятельность по управлению человеческими ресурсами – именно та сфера, которая как никакая другая подвергается наибольшему числу рисков, сложно предсказуемых и оцениваемых. Фундаментальная причина тому – квалификация и опыт сотрудников являются самым ценным активом во многих компаниях. В результате появилось осознание того, откуда исходят ключевые риски – в отличие от других активов эти могут просто хлопнуть дверью и перенести свои знания и умения в другую компанию.

Вместе с тем для любой компании очень важно обеспечить объективное, адекватное представление о совокупности кадровых рисков, влияющих на ее деятельность. Это важно по ряду причин. Во-первых, для принятия оптимального решения необходима информация о рисках, связанных с его разработкой и исполнением. Во-вторых, следует ослаблять влияние неполноты информации и неопределенности путем расширения круга прогнозируемых управляемых рисков. И, наконец, ясное представление о рисках и кадровых угрозах позволяет определить эффективные методы управления этими рисками и, соответственно, безопасностью организации.

Каждый сотрудник проходит три этапа взаимодействия с организацией (рисунок 6).

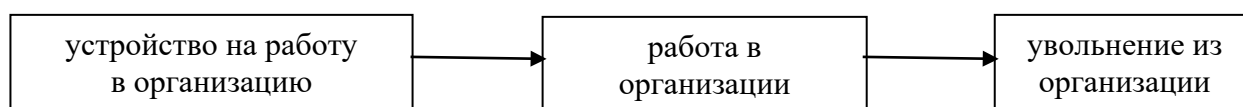


Рис. 6. Этапы взаимодействия сотрудника с организацией

В связи с этим риски кадровой безопасности дифференцируются в 3 группы по указанным этапам. Рассмотрим кадровые риски с разных позиций (таблица 1).

С кадровыми рисками компания сталкивается на разных этапах своей деятельности, и, естественно, причин возникновения конкретной рискованной ситуации может быть очень много.

Таблица 1

Классификация рисков кадровой безопасности организации

Группа рисков	Состав
Риски кадровой безопасности при работе с персоналом на входе в организацию	– риск неправильного выбора источника поиска кандидатов (опыт, сфера деятельности, пол, социальный статус); – риск отсутствия формализованных компетенций должности или нечеткого формирования требований к кандидату на должность; – риск неправильной оценки кандидата на этапе подбора (недостаточная квалификация, акцентуации, девиации, зависимости, психологическая несовместимость); – риск принятия кандидата с прямыми угрозами кадровой и экономической безопасности организации.
Риски кадровой безопасности при работе с персоналом внутри организации	– риск неудачной адаптации работника в коллективе или невосприятие коллективом; – риск снижения и потери работником мотивации и стимулов к эффективной работе; – риск оттока профессионалов к конкурентам через предложение лучших условий работы (переманивание); – риск снижения темпов развития и потеря кадрового потенциала работниками организации; – риск возникновения неконструктивных внутренних конфликтов между работниками организации; – риск прямых злоупотреблений работника, наносящий экономический ущерб организации (прямые финансовые злоупотребления, воровство, мошенничество, распространение коммерческой тайны, деликатный риск правонарушений); – риск создания отрицательного имиджа организации на рынке.
Риски при работе с персоналом на выходе из организации	– риск финансовых претензий работника (в случае увольнения по инициативе работодателя) к организации; – риск формирования отрицательного имиджа организации как работодателя через распространение отрицательной информации о нем; – риск распространения работником информации, являющейся коммерческой тайной, среди его конкурентов.

Обычно под *причиной возникновения* подразумевается какое-то условие, вызывающее неопределенность исхода ситуации. Для кадровых рисков такими

источниками могут являться факторы различного характера: экономического, политического, экологического, юридического, социального, технического и даже нравственного, поскольку мы имеем дело с человеческим фактором производства.

К сожалению, как бы человечество ни стремилось к рациональности своего поведения и принимаемых решений, фактор иррациональности всегда будет присутствовать в поведении работников. Это объясняется как объективными, так и субъективными причинами. Объективно восприятие и оценка ситуаций у людей различны: одни видят в переменах опасности и риск, а другие рассматривают те же перемены как источник новых возможностей. Различны судьбы людей, круг общения, ценности и мировоззрение, предпочтения и интересы. Но и субъективно каждый человек стремится к уникальности, неповторимости, особенностям. Поэтому он часто сознательно пытается обойти рациональный ортодоксальный путь решения и выбирает парадоксальное направление движения. Справедливо считается: кто не рискует, тот не выигрывает. Более высокий риск связан с вероятностным извлечением и более высокого дохода.

Иными словами, для получения экономической прибыли часто необходимо осознанно пойти на принятие рискованного решения. Рассчитывая на стандартное человеческое поведение, мы очень часто подвергаем себя значительным рискам, которые приносят в работу компании элементы непредсказуемости и нестабильности. Естественно, руководство вправе частично переложить кадровый риск на других субъектов экономики (кадровые агентства, страховые компании), но полностью избежать его они не могут.

Как же измерить риск? Для этого необходимо прибегнуть к вероятностным категориям. Вероятность события – это число от нуля до единицы, и чем ближе это число к единице, тем выше возможность события, которое может наступить или не наступить в условиях неопределенности. Эту вероятность можно оценить субъективно (экспертно), а можно применить более тонкие, хотя и не всегда более точные методы.

Объективный метод определения вероятности основан на вычислении частоты, с которой происходят некоторые события. Частота при этом рассчитывается на основе фактических данных. Так, например, частота возникновения некоторого уровня потерь в процессе реализации инвестиционного проекта может быть рассчитана по формуле (1):

$$f(A) = n(A) / n \quad (1)$$

где f – частота возникновения некоторого уровня потерь;

$n(A)$ – число случаев наступления этого уровня потерь;

n – общее число случаев в статистической выборке, включающее как успешно осуществленные, так и неудавшиеся инвестиционные проекты.

Но одной вероятности мало для описания рисков. При исследовании риска необходимо понимать уязвимости и угрозы для организации.

Уязвимость показывает слабые места в стратегии, структуре, кадровой политике компании и характеризуется сложностью и уровнем различных навыков и средств, необходимых для того, чтобы ею воспользоваться. Уязвимость, которой легко воспользоваться и которая позволяет злоумышленнику получить полный контроль над системой, является уязвимостью высокого уровня риска. Уязвимость, которая потребует от атакующего вложения значительных средств в оборудование и персонал и позволит лишь получить доступ к не особо ценной информации, считается уязвимостью низкого уровня риска.

Таким образом, риск – это сочетание угрозы и уязвимости. Угрозы без уязвимости не являются риском так же, как и уязвимости без угроз.

Риск качественно характеризуется тремя **уровнями**:

Низкий уровень риска – существует маленькая вероятность проявления угрозы. По возможности нужно предпринять действия по устранению уязвимого места, но их стоимость должна быть сопоставлена с малым ущербом от риска.

Средний уровень риска – уязвимость является значительным уровнем риска для безопасности компании и ее сотрудников. Существует реальная возможность осуществления такого события. Действия по устранению уязвимости целесообразны и необходимы.

Высокий уровень риска – уязвимость представляет собой реальную угрозу для безопасности компании, ее стратегии, структур, процессов и персонала. Действия по устранению этой уязвимости должны быть предприняты незамедлительно.

Угроза – это действие или событие, способное нарушить безопасность компании. У нее есть три составляющие: цели, агенты и события.

Цели – это те компоненты безопасности (активы, информация, люди, службы), которые подвергаются атаке. При кадровых угрозах целью, как правило, является тот сотрудник или руководитель, который обладает интересными для атакующего агента полномочиями или ресурсами.

Агентами угроз являются люди, которые стремятся нанести ущерб организации. Для этого они должны иметь доступ к нужному сотруднику (прямой или опосредованный), необходимые знания или компрометирующую информацию о нем, а также мотивацию для совершения требуемых действий (алчность, злые намерения, месть, жажда славы и т.п.) (рисунок 7).



Рис. 7. Агенты угроз

События – это способы, с помощью которых агенты угроз могут причинить вред организации. Например, кража, мошенничество, махинации с документами, уничтожение собственности, физическое вмешательство в системы или операции, несанкционированный доступ к информации и активам, нарушение внутренних или внешних коммуникаций, переманивание сотрудников и клиентов, шантаж для заключения невыгодного контракта и т.д.

Составной частью любого события является благоприятная возможность. Такая возможность существует в любой компании только потому, что сотрудники оставляют двери открытыми, не соблюдают правил безопасности, не проявляют бдительности и в целом не обеспокоены в отношении имеющихся у компании угроз.

Теперь рассмотрим угрозы кадровой безопасности.

Угроза кадровой безопасности – совокупность условий и факторов, которые создают опасность жизненно важным интересам участников социально-трудовых отношений, препятствуют эффективному и гармоничному развитию человеческих ресурсов.

Существуют различные классификации угроз кадровой безопасности организации.

По *признаку целевой направленности* выделяются:

- угрозы безопасности сотрудников организации, которые могут стать объектами переманивания, вербовки, шантажа, угроз и прямых покушений;
- угрозы безопасности организации со стороны ее собственных сотрудников, которые в силу своей безответственности или злого умысла способны нанести ущерб ее имущественным и неимущественным интересам.

По *признаку характера потерь от реализованных угроз* выделяются:

- угрозы информационной безопасности, связанные с деятельностью персонала и реализуемые в форме разглашения конфиденциальной информации, а также искажения или уничтожения любых сведений и баз данных, используемых организацией в своей деятельности;
- угрозы имущественной безопасности, связанные с деятельностью персонала и реализуемые в форме хищения или умышленного повреждения (уничтожения) различных элементов имущества организации – от основных фондов до наличных денежных средств.

По *признаку источника угрозы (субъекта)* выделяются:

- угрозы со стороны конкурентов, стремящихся к усилению собственных позиций на соответствующем рынке путем использования недобросовестных методов, например, деловой разведки, переманивания высококвалифицированных сотрудников, дискредитации соперника в глазах партнеров и государственных структур;
- угрозы со стороны криминальных структур и отдельных злоумышленников, стремящихся к достижению собственных целей, находящихся в противоречии с интересами конкретной организации или ее клиентов, например, захвата контроля над ним, хищения имущества, нанесения иного ущерба;

– угрозы со стороны государства в лице уполномоченных надзорных, регулирующих, фискальных и правоохранительных органов, деятельность которых в некоторых случаях может вызывать угрозы по кадровому направлению работы организаций;

– угрозы со стороны сотрудников организации, осознанно или в силу общей безответственности наносящих ущерб ее безопасности ради достижения личных целей, например, минимизации трудовых усилий, улучшения материального положения, карьерного роста, мщения работодателю за реальные или мнимые обиды и т.п.

По *экономическому характеру угрозы* выделяются:

– угрозы материального характера, наносящие организации прямой и легко исчисляемый финансовый ущерб, например, похищенные денежные средства и товарно-материальные ценности, сорванный контракт, примененные штрафные санкции;

– угрозы нематериального характера, точный размер ущерба от реализации которых обычно невозможно точно определить, например, сокращение обслуживаемого рынка, ухудшение имиджа организации в глазах ее клиентов и деловых партнеров, утеря ценного специалиста.

По *вероятности практической реализации* выделяются:

– угрозы потенциальные, практическая реализация которых на конкретный момент имеет лишь вероятностный характер (т.е. у субъекта управления есть время на их профилактику или подготовку к отражению);

– угрозы реализуемые, негативное воздействие которых на деятельность субъекта управления находится в конкретный момент на различных стадиях развития (т.е. у субъекта имеются шансы на их оперативное отражение в целях недопущения или минимизации конечного ущерба);

– угрозы реализованные, негативное воздействие которых уже закончилось и ущерб фактически нанесен (т.е. субъект управления имеет возможность лишь оценить ущерб, выявить виновников и подготовиться к отражению подобных угроз в дальнейшем).

Среди *факторов, провоцирующих возникновение угроз кадровой безопасности организации* и создающих опасность реализации ее интересов, можно выделить следующие (рисунок 8).

Таким образом, носителями угроз кадровой безопасности могут быть:

– персонал организации (направленность личности, морально-нравственные ориентации, склонность к зависимостям, уровень тревожности и др.);

– криминальные структуры;

– конкуренты,

– государственные и общественные институты, сама организация.

Результатом влияния угроз кадровой безопасности могут стать склонение к нелояльному поведению, переманивание, вербовка, утрата здоровья, потеря репутации и т.п.

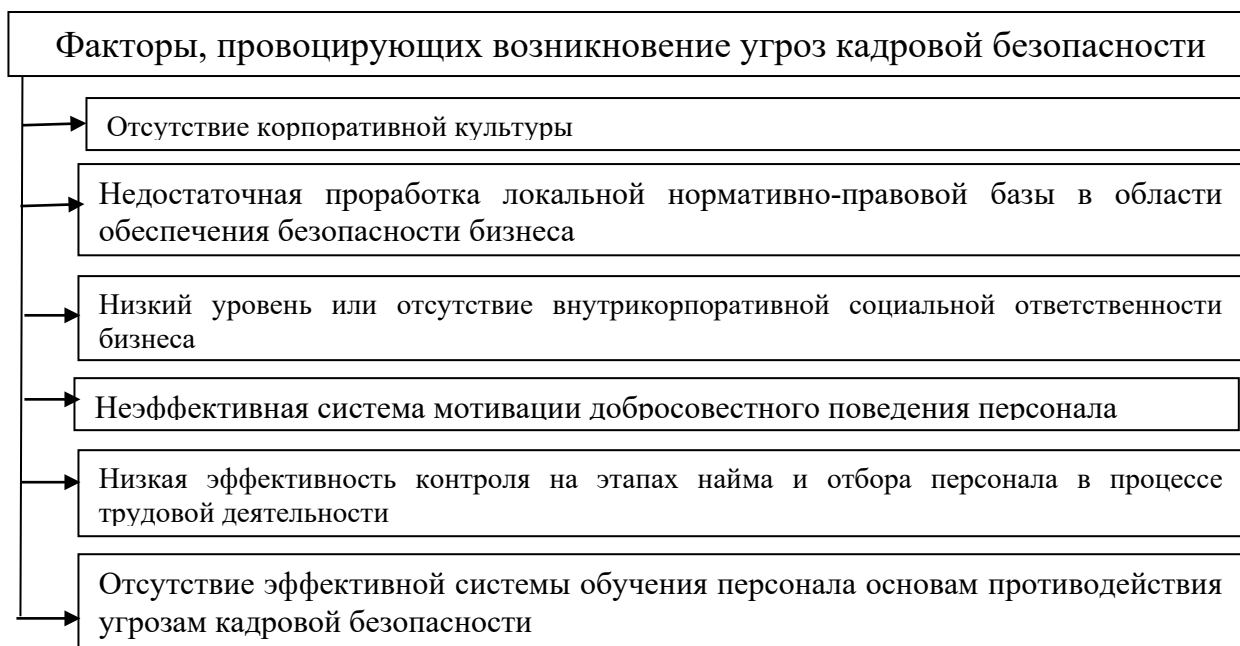


Рис. 8. Факторы, провоцирующих возникновение угроз кадровой безопасности организации

1.3. Типы противоправного поведения персонала в организации

Можно выделить несколько типов поведения сотрудников, входящих в группу риска, которые представляют потенциальную или реальную угрозу безопасности организации (таблица 2).

Типы противоправного поведения сотрудников

Тип поведения	Особенности
Аддиктивное поведение	Уход от реальности путем изменения своего психического состояния с помощью наркотиков, алкоголя или постоянной фиксации внимания на определенных предметах или видах деятельности (карты, бега) для получения интенсивных эмоций. Эти процессы управляют жизнью человека, делают его беспомощным, лишают воли. Для достижения своих целей аддикт может пожертвовать, чем угодно.
Антисоциальное девиантное поведение	Основная черта – совершение действий, противоречащих этике и морали, безответственность, игнорирование законов и прав других людей.
Суицидное поведение	Подвергающее свою (соответственно и рядом находящихся людей) жизнь риску.
Конформистское поведение	Исполнение воли «авторитета», приспособленчество, не критичность, неспособность принимать решения, брать на себя ответственность.
Нарцисстическое поведение	Повышенная чувствительность к оценкам других людей, отсутствие достаточного чувства сопереживания, дистанцирование от коллектива (как следствие неприятие его норм и требований).
Эгоистическое, индивидуально-целевое деструктивное поведение	Реализуется в направлении достижения личных целей за чужой счет, сопровождается, как правило, имитационным поведением, когда истинные эгоистические цели камуфлируются псевдоактивностью, псевдоисполнительностью, демагогией, ошибками восприятия (сделал задания так, как понял, а понял и воспринял неверно).
Фанатическое поведение	Слепая приверженность какой-либо идее, нетерпимости к другим взглядам, что может сопровождаться действиями насильственного характера. Нейтральные или дружеские поступки других людей часто оцениваются как враждебные или заслуживающие презрения.
Аутистическое поведение	Затруднение социальных контактов, оторванность от действительности, погруженность в сферу мечтаний. Отсюда невозможность адекватно оценить ситуацию и принять решение.

Рассмотрим *аддиктивное поведение* более подробно.

Данный тип поведения связан с желанием человека уйти от реальности путем изменения состояния своего сознания. В зависимости от того, посредством чего осуществляется уход из реальности, различают следующие виды зависимостей:

- фармакологические (химические) – наркотизм (наркомания), алкоголизм, табакокурение, токсикомания;
- субстанциональные – компьютерные, игорные зависимости, эмоциональные созависимости, трудовголизм и др.;
- пищевые.

Средства аддикций подразделяются на следующие типы:

- психоактивные вещества (алкоголь, наркотики и т.д.);
- активность, включенность в процесс (хобби, игра, работа и т.д.);
- люди, предметы и явления окружающей действительности, вызывающие различные эмоциональные состояния (секты, финансовые пирамиды и пр.).

Уход от реальности всегда сопровождается сильными эмоциональными переживаниями. Человек фактически зависит, скажем, не от препарата, а от эмоций. Эмоции являются составной частью зависимости. Посадив человека на «эмоциональный крючок», им очень легко управлять.

Почему присутствие таких зависимых людей в организации является риском для кадровой безопасности?

1. Возможность управления работником, входящим в группу риска, извне, что может быть направлено на дестабилизацию организации (получение секретов, уход клиентов и т.д.).

2. Постоянные попытки зависимого распространить влияние своих пагубных пристрастий, привычек на окружающих, поиск или формирование им круга единомышленников, то есть увеличение количества представителей группы риска в организации.

3. Удовлетворение своих зависимостей за счет временных и материальных ресурсов работодателя.

4. Разрушение стабильного работоспособного коллектива (команды).

5. Склонность к преступным действиям и нарушениям либо ради, либо вследствие удовлетворения своих зависимостей.

Рассмотрим основные группы риска.

1. **Члены религиозных новообразований.** Чаще всего это люди, отвечающие следующим признакам:

– одиночество, так как любая секта – это сплоченный коллектив с общими групповыми целями и став ее членом, человек забывает, что такое одиночество;

– переходный возраст – с помощью секты можно уйти от опеки родителей, бросить вызов окружающим;

– неуверенность в себе – в секте не надо думать, что сделать, какой путь выбрать, не надо думать вообще;

– поиск легких путей – люди искренне верят, что, участвуя в религиозной организации, можно решить все свои проблемы;

– стремление вырваться из некомфортной домашней атмосферы.

Существуют общие для членов большинства сект внешние признаки, по которым его можно выявить. Это может быть наличие фотографии духовного наставника, особенный режим питания (определенное время, свои продукты, ритуалы), характерные одежда, манера говорить, какие-либо аксессуары (четки и т.п.) и др.

Становясь частью коллектива компании, член такой религиозной организации почти всегда будет пытаться распространить влияние своей «религии» на окружающих. Признаками начала негативного воздействия на организацию являются:

– прямая информация о попытках вербовки;

– периодическое отсутствие более одного члена коллектива в определенные дни недели (якобы по болезни);

– появление на рабочих местах сектантских брошюр или приглашений на «семинары», рассказы об «очень хороших» заведениях для детей и т.п.

Вовремя распознав указанные признаки, можно изменить ситуацию или удержать ее под контролем. Однако следует помнить, что есть ряд сект, члены которых полностью безопасны для предприятия.

2. Алкоголики. Алкоголизм – одна из форм фармакологической (химической) зависимости, в основе которой лежит употребление спиртосодержащих напитков. Алкоголь, вопреки распространенному мнению, не изменяет, а кристаллизует текущее состояние.

Выявить признаки алкоголизма у кандидата на вакансию при приеме на работу и у любого работающего в организации можно различными способами: и медико-психологическими методиками, и по внешним признакам.

Внешние признаки злоупотребления алкоголем:

- поведение работника на деловых и развлекательных мероприятиях, связанных с употреблением алкоголя, и после них;
- повышенная суетливость при подготовке к выпивке;
- внешний вид (красный кончик носа, опухлость, отеки);
- речевые признаки и многие другие.

Медицинские методики заключаются в применении различного рода обследований и пригодны для определения предрасположенности к этой зависимости.

Отрицательное воздействие алкоголика на организацию связано преимущественно с изменением под воздействием алкоголя личностных качеств работника и влечет за собой:

- потери от неэффективного использования рабочего времени;
- перманентную угрозу производственной и информационной безопасности, в том числе несчастных случаев при работе, связанной с источниками повышенной опасности;
- попытки вовлечь в круг собутыльников своих коллег;
- совершение преступных деяний в связи с алкоголизмом;
- использование материальных и финансовых ресурсов предприятия для удовлетворения потребности в алкоголе и т.д.

3. Наркоманы. Выявить принадлежность кандидата на вакансию или работника к этой группе риска можно, установив факт или последствия употребления наркотиков, что делается несколькими путями:

- по косвенным признакам употребления наркотиков и наркотической зависимости;
- с помощью экспресс-тестов на наркотики;
- в процессе наркологической экспертизы.

Специалисту по работе с персоналом следует знать косвенные признаки употребления наркотиков и наркотической зависимости:

- как правило, это молодые люди;
- длинные рукава одежды, независимо от погоды и обстановки;
- часто неряшливый вид, сухие волосы, отекающие кисти рук;
- невнятная, «растянутая» речь;
- неуклюжие и замедленные движения при отсутствии запаха алкоголя;
- признаки потери контроля над собой;

- явное стремление избегать встреч с представителями руководства и службы безопасности;
- раздражительность, резкость и непочтительность в ответах на вопросы;
- периодические уходы с рабочего места, после которых появляются перечисленные отклонения в поведении.

Признаками появления наркоманов в коллективе являются:

- участвовавшие пропажи вещей и денег;
- нахождение следов приготовления или употребления наркотиков (одноразовые шприцы, закопченные ложки, иглы и пр.);
- пропажи чайных ложек из столовой предприятия;
- производственные травмы;
- прямая информация о том, что кто-то предлагает «попробовать».

Экспресс-тесты для определения наркотиков с высокой степенью достоверности позволяют определить наличие наркотиков, например, в моче. Экспресс-тесты свободно продаются в аптеках.

Наркологическая экспертиза производится, если необходимо доказать, что кто-то злоупотребляет наркотиками или находится в состоянии наркотического опьянения в настоящий момент и от этого зависит решение спорных трудовых или юридических вопросов. Судебно-наркологическая экспертиза проводится только специалистами государственных наркологических лечебных учреждений и только по запросу органов МВД или юстиции.

Влияние наркоманов на организацию в основном носит индивидуальный характер и проявляется в следующем:

- увеличение количества мелких хищений;
- риск совершения преступления в состоянии наркотического опьянения;
- частые нарушения режима рабочего времени, потери от его неэффективного использования;
- возрастание уровня конфликтности в подразделении;
- срыв решения важных задач, порученных такому работнику;
- распространение наркотиков и увеличение числа зависимых.

Одним из видов химической зависимости является *токсикомания*. Она развивается в связи с употреблением лекарственных средств и веществ, не отнесенных к наркотическим, но также изменяющих состояние психической деятельности человека и его поведение. Диапазон веществ с вызывающим зависимость действием очень широк – от медикаментов (анальгетики, транквилизаторы, снотворные, стимуляторы и др.) до технических растворителей и средств бытовой химии. Почти все, что ранее сказано про алкоголиков и наркоманов, справедливо по отношению к токсикоманам.

4. Игроки. Игровую аддикцию по-другому называют гэмблингом (от англ. gambling – игра). К этому виду аддикций относятся такие зависимости, как зависимость от казино, карт, скачек, игровых автоматов, различных азартных игр. Сюда относятся также и зависимости от компьютерных игр. Американская Ассоциация психиатров провела комплексное исследование этой зависимости и идентифицировала ее как заболевание с диагнозом «патологическая страсть к

азартным играм», которому подвержен неограниченный круг людей и которое имеет те же последствия, что и алкогольная и наркотическая зависимость.

Принадлежность работника к этой группе риска выявляется по следующим признакам:

- внезапное появление или исчезновение денег у игрока;
- постоянные разговоры об азартных играх;
- жалобы членов семьи на низкую зарплату и т.д.

Отрицательное воздействие игрока на организацию носит индивидуальный характер, и степень его связана с характером и силой зависимости: потери организации от неэффективного использования рабочего времени сотрудника; совершение изощренных трудно раскрываемых мошеннических действий; хищения информации, денежных и материальных ценностей в крупных размерах.

Общие меры предотвращения отрицательных влияний групп риска на безопасность организации заключаются:

- во-первых, в надежном входном контроле пристрастий и зависимостей: (полное анкетирование, проверка заявленных сведений, эффективное собеседование с целью выявления внешних признаков девиантного поведения и др.);

- во-вторых, в тщательном контроле во время срока испытания или адаптации работника;

- в-третьих, в постоянной готовности администрации к «безопасному» увольнению работника из группы риска (четкое оформление событий дисциплинарной практики в виде актов, объяснительных и пр., проведение грамотного внутреннего PR перед его планируемым увольнением).

Появление сотрудников с опасным для компании поведением является, прежде всего, результатом привлечения на вакантные места персонала извне, а также следствием неоднородности культуры компании, проявляющейся в наличии субкультур и контркультур внутри данной культуры.

В организации, как правило, в той или иной степени присутствуют все из вышеперечисленных деструктивных форм поведения. Однако наибольшую опасность, в том числе и финансовую, представляет *девиантное поведение*, существующее в виде различных типов мошенничества. Мошенничество представляет собой незаконное, путем обмана, подтасовки, манипуляций, присвоения чужой собственности, активов компании поведение.

В организационном поведении выделяют шесть *типов мошенничества* в зависимости от его субъекта (рисунок 9):

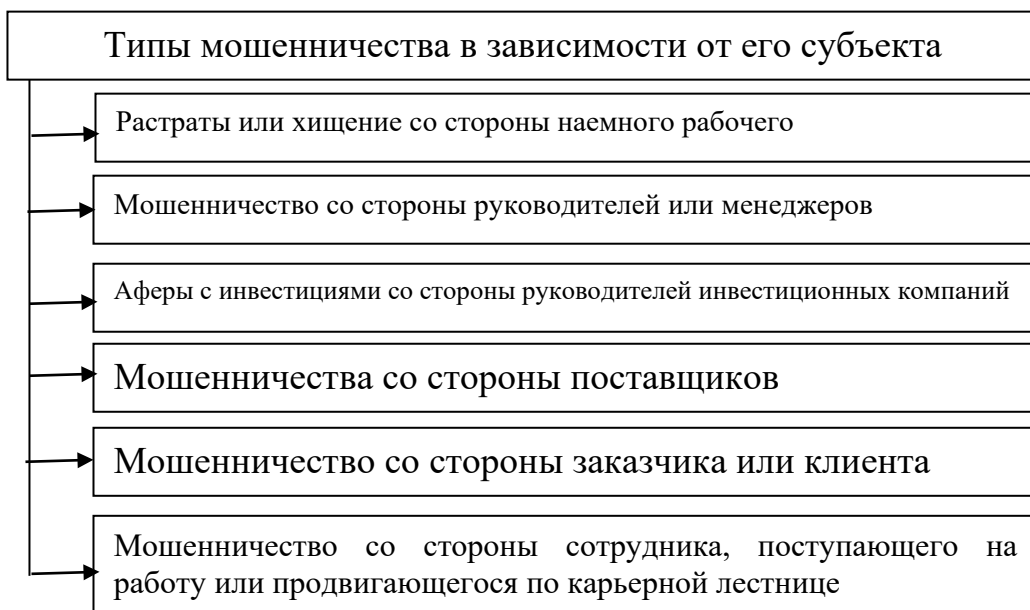


Рис. 9. Типы мошенничества в зависимости от его субъекта

1. *Растраты или хищение со стороны наемного рабочего.* В эту группу мошенничества входят: воровство наличности, чеков, инвентаря, использование наличности не по назначению, фальсификация кассовых книг и сумм на банковских счетах, оплата личных счетов чеками фирмы, фальсификация транспортных накладных, сговор с клиентами или поставщиками, «откаты», «кикбэки» (благодарности за услуги), искусственное вздувание цен, использование подставных поставщиков, переплата «сверху», выдача дутых векселей (кайтинг), манипуляции с кредитными карточками, мошенничества со страховкой, медицинскими счетами, фальсифицирование налоговых деклараций, записей в бухгалтерских книгах, искажение расходов в отчетах о командировках, несанкционированная продажа имущества фирмы, компьютерные преступления, мошенничество с выплатой заработной платы (обналичивание невостребованных чеков, фальсификация часов переработки, оплата труда работников-невидимок).

2. *Мошенничество со стороны руководителей или менеджеров.* Наиболее частый обман совершается путем манипуляций с финансовой отчетностью, в которой искажаются данные о доходности и дебиторских задолженностях фирм. При этом руководство всегда стремится к тому, чтобы держатели акций верили, что финансовое положение компании гораздо лучше, чем оно есть на самом деле. Второй вид мошенничества – создание параллельного бизнеса и перекачивание туда активов и средств компании.

3. *Аферы с инвестициями со стороны руководителей инвестиционных компаний.* Этот тип мошенничества связан с предложением инвесторам сделать инвестиции, которые впоследствии оказываются липовыми, не имеющими никакой стоимости. В эту категорию попадает телемаркетинг, финансовые

пирамиды, вложения в «проекты века», которые благополучно разваливаются, унося инвестиции на счета мошенников.

4. *Мошенничества со стороны поставщиков* проявляются часто в завышении количества поставленных изделий, поставке бракованных товаров, недопоставке уже оплаченной партии, поставке товара более низкого качества.

5. *Мошенничество со стороны заказчика или клиента* включает неплатежи за уже поставленный товар, получение платы за непроделанную работу, поставку совершенно ненужных вещей взамен указанных в договоре.

6. *Мошенничество со стороны сотрудника, поступающего на работу или продвигающегося по карьерной лестнице*, предполагает фальсификации документов об образовании, профессиональной квалификации, возрасте, наградах и иных данных, позволяющих не столько присвоить прибыль, сколько занять место, получить ранг, несоответствующий истинным личностным качествам и биографическим данным работника.

Другая классификация рассматривает *виды мошенничества в зависимости от характера совершаемых действий* (рисунок 10):



Рис. 10. Виды мошенничества в зависимости от характера совершаемых действий

А. *Мелкие разовые хищения («бес попутал»)*. Люди склонны иногда совершать мелкие кражи, необъясняемые рациональными причинами (например, хищение товаров в магазинах самообслуживания). Такие хищения не создают системы и не приносят заметной экономической выгоды. Они совершаются скорее из озорства в тех случаях, когда человек уверен в своей безнаказанности. К ним бывают склонны люди независимо от материального достатка. Они мотивируются в основном стремлением «пощекотать нервы», иногда – мелкой «мстостью». В большинстве случаев они происходят без предварительной подготовки и продумывания: человек просто хватается то, что, по его мнению, плохо лежит.

Для экономики предприятия такие хищения вряд ли могут нанести заметный ущерб. Их опасность в другом: развращение персонала и вероятность перехода привыкшего к таким хищениям человека на следующий уровень. Главное средство защиты от них – не создавать соблазнов.

Б. *Систематические хищения среднего размера: «надбавка к зарплате»*. Эта группа хищений отличается от первой тем, что совершается из экономических мотивов, носит систематический характер, продумана и обычно обеспечивается мерами безопасности. Именно по этой причине расхищаются обычно незначительные (на фоне общего денежного потока) суммы: менее вероятно, что на них обратят внимание. Тем не менее, таким способом работник может обеспечить себе постоянный доход, сопоставимый с уровнем заработной платы.

Такие хищения, в отличие от предыдущей группы, несут значительный ущерб для предприятия. Их опасность для морали персонала в том, что, хотя никто особо не афиширует своих «подвигов», в коллективе вырабатывается негласное отношение к ним как к обыденности: «Ты здесь – хозяин, а не гость: тащи с работы каждый гвоздь!». Особенно опасно, когда это отношение молчаливо разделяет и менеджмент предприятия: создаётся атмосфера попустительства, при которой главное – не попасться при всех с поличным. Известны организации, куда поступают на работу не из-за зарплаты (обычно низкой), а из-за возможностей такого дополнительного заработка. Менеджмент таких организаций не повышает сотрудникам зарплату, поскольку считает, что те «всё равно своё возьмут».

Подобная атмосфера быстро коррумпирует новых сотрудников. Известны случаи, когда новичков, сопротивляющихся этому, под тем или иным предлогом «выживали» из организации.

Важная психологическая особенность таких хищений – отсутствие у воровующих чувства вины. Оно подавляется оправданиями: «все так делают», «мне всё равно не доплачивают, я беру своё», «когда от многого берут немножко, то это не кража, а просто делёжка» и т.п.

Если в организации или отдельных подразделениях сложилась такая атмосфера, то победить её полностью можно лишь уволив старый персонал и наняв новый. Попытки менеджмента бороться с подобными хищениями путём налаживания системы учёта и контроля внедряются с большим трудом, зачастую вызывая возмущение у персонала, вплоть до увольнений.

В. *«Внутреннее предпринимательство»*. Это наиболее опасный тип злоупотреблений, возникающий там, где сотрудникам предоставляется возможность распоряжаться крупными суммами и самостоятельно принимать крупные финансовые решения. Формально работая на организацию, такие люди создают на её основе внутренний «частный бизнес». Здесь речь идёт уже не о «дополнительной зарплате», а о присвоении крупных сумм.

Этот тип злоупотреблений распространён в следующих организациях:

- а) властные структуры, где чиновники берут взятки за благоприятное для «клиента» решение вопросов;
- б) промышленные предприятия, где наёмные руководители и сотрудники отделов снабжения и сбыта берут «комиссию» с поставщиков и клиентов (если продукция дефицитна);
- в) коммерческие структуры, где отдельные наёмные работники (торгующий персонал) реально оперируют сделками на крупные суммы, лично

общаются с клиентами, имеют доступ к наличным и получают возможность так или иначе присваивать часть этих сумм.

Главный способ вычисления «внутреннего предпринимателя» – отслеживание его расходов. Как правило, они совершают покупки не по средствам: дорогие иномарки, квартиры, дорогостоящие круизы. В отношении «средних» и «мелких» мошенников это не срабатывает, так как при своих доходах они, как правило, не позволяют себе особенно шиковать.

Явный признак «внутреннего предпринимательства» – «закрытость» отношений трейдера с клиентом. Трейдеры пытаются под предлогом того, что «клиент не будет работать ни с кем, кроме меня», максимально ограничить информацию о сделке, вплоть до попыток скрыть имя получателя комиссии.

Суть любого мошенничества составляют три основных элемента (рисунок 11). Эти три основных условия впервые указал криминолог Дональд Кресси, разработавший концепцию так называемого «треугольника мошенничества». Нарушители, как правило, имеют определенную мотивацию или подвержены давлению внешних обстоятельств, которые подталкивают их к совершению неправомерных действий. Также должна существовать возможность для совершения мошенничества. Кроме того, мошенникам нередко удается найти аргументированное обоснование или оправдание своим действиям.



Рис. 11. «Треугольник мошенничества»

95% всех случаев мошенничества вызваны давлением финансовыми обстоятельствами или человеческими пороками. Финансовые обстоятельства могут включать в себя жизнь не по средствам, большие долги, жадность, значительные медицинские счета, финансовые потери и неожиданную потребность в деньгах. Наркомания, алкоголизм, страсть к азартным играм и дорогим сексуальным удовольствиям также становятся факторами давления, так как требуют больших финансовых затрат. Иногда мотивацией для мошенничества являются кажущаяся недооценка своих успехов, чувство неудовлетворенности от работы, страх ее потерять, несправедливость с премиальными и вознаграждением, т.е. факторы, связанные непосредственно с работой персонала. Для некоторых людей достичь успеха более важно, чем быть честным.

Возможность для мошенничества создают недостаточные меры контроля, невозможность или неспособность оценить качество выполненной работы, отсутствие производственной дисциплины, предоставление искаженной

информации, безразличие со стороны руководства и коллег, отсутствие аудиторских проверок.

Третьим компонентом «треугольника мошенничества» является способность сотрудников, будь то рядовые служащие или члены совета директоров, обосновать причину преступных действий и найти им оправдание. Почти каждый случай мошенничества сопровождается оправданием самого себя в правомерности своих действий по причине, например, того, что «я заслуживаю большего, а моя фирма мне задолжала, эти деньги я направлю на благие дела и через какое-то время верну, и от этого никому хуже не будет».

Выделяют две группы причин для совершения противоправных действий:

- личные причины – личный стимул и способность логически обосновать действия для себя (алчность, страх за себя или своих близких, безразличие, внутренний авантюризм и др.);

- корпоративные причины – недостаточный контроль (тщеславие, легкомыслие, низкий уровень лояльности, нескрываемый расчет и др.).

Выявить мошенника можно двумя способами: случайно или при помощи имеющихся в компании механизмов контроля и систем управления рисками.

Вообще достаточно несложно для наблюдательного человека выявить основные признаки мошенничества со стороны наемных работников и менеджеров:

- необычное поведение, выходящее за привычные рамки образа жизни;
- повышенный интерес к рискованным сделкам;
- склонность к азартным играм;
- слишком сильно демонстрируемая приверженность организации;
- наличие жалоб и наводок;
- подчеркнутая дружба с начальством и подозрительность к коллегам, охотно отрабатываемые сверхурочные;
- невразумительные ответы на обычные вопросы;
- признаки раздражения при ответе на простые вопросы;
- переписывания по своей инициативе документов для придания им более «аккуратного» вида.

Исследования свидетельствуют, что, когда человек совершает преступление (особенно впервые), он неизбежно испытывает сильные эмоции, прежде всего чувство вины, страха, стресса. Эти состояния ведут к определенным поведенческим изменениям – бессоннице, повышенной раздражительности, подозрительности, неспособности расслабиться, общаться с коллегами, смотреть глаза в глаза, постоянному страху разоблачения. Ранее приятный в общении человек становится агрессивным, замкнутым, невыносимым. В большинстве фирм наверняка имеется достаточно много сотрудников, которые о чем-то знают, подозревают, но не сообщают об этом.

Контрольные вопросы и задания

1. Кадровая безопасность», ее цели и задачи, объекты и субъекты.
2. Кадровые риски, определение, их классификация, уровни, методы измерения.
3. Характеристика угроз кадровой безопасности?
4. Понятие групп риска. Виды зависимостей. Угрозы кадровой безопасности, создающиеся группами риска.
5. Как выявить сотрудника, принадлежащего к группе риска? Меры, предпринимаемые в отношении сотрудников из групп риска.
6. Типы мошенничества и его признаки.

Задания для самостоятельной работы

1. В Правительстве субъекта Российской Федерации создается новое структурное подразделение (какое – на ваше усмотрение). Обоснуйте необходимость его создания и разработайте план мероприятий по обеспечению его кадровой безопасности.
2. Проведите сравнительный анализ кадровых рисков и угроз на разных стадиях развития организации. Например, в Департаменте образования и науки, Департаменте здравоохранения и Департаменте экономического развития какого-либо субъекта Российской Федерации.
3. Проведите сравнительный анализ организационной структуры органа местного самоуправления, с точки зрения рисков и угроз кадровой безопасности, в рамках одного или нескольких субъектов Российской Федерации.
4. На примере какого-либо органа местного самоуправления оцените кадровые риски и угрозы, и на этой основе определите возможные ситуации возникновения конфликта интересов и пути (способы) его профилактики.

Тестовые задания

1. Административно-независимая безопасность является элементом
А) безопасности жизнедеятельности
Б) профессиональной безопасности
В) социально-мотивационной безопасности
Г) антиконфликтной безопасности
2. Пенсионно-страховая безопасность является элементом
А) безопасности жизнедеятельности
Б) профессиональной безопасности
В) социально-мотивационной безопасности
Г) антиконфликтной безопасности
3. Патриотическая безопасность является элементом
А) безопасности жизнедеятельности

- Б) профессиональной безопасности
- В) социально-мотивационной безопасности
- Г) антиконфликтной безопасности

4. Создание психологического климата в коллективе на основе положительного отношения к компании, психологического единения работников вокруг общих целей – это

- А) финансовая безопасность
- Б) безопасность труда
- В) физическая безопасность
- Г) интеллектуальная безопасность
- Д) патриотическая безопасность
- Е) эстетическая безопасность

5. Выполнение комплекса мероприятий по недопущению внешних опасностей персонала, связанных с их служебной деятельностью, или членам их семей – это

- А) финансовая безопасность
- Б) безопасность труда
- В) физическая безопасность
- Г) интеллектуальная безопасность
- Д) патриотическая безопасность
- Е) эстетическая безопасность

6. Субъектом кадровой безопасности организации не является

- А) менеджеры по персоналу
- Б) менеджеры по безопасности
- В) менеджеры по инновациям
- Г) охранники
- Д) сотрудники информационно-аналитических отделов

7. Риск – это...

- А) намерение нанести какой-либо вид вреда
- Б) возможность появления негативного инцидента в будущем и размер последствий после него
- В) совокупность условий и факторов, которые создают опасность жизненно важным интересам участников социально-трудовых отношений, препятствуют эффективному и гармоничному развитию человеческих ресурсов
- Г) ситуация, отражающая опасность нежелательного развития событий
- Д) какое-то условие, вызывающее неопределенность исхода ситуации

8. Риск финансовых претензий работника к организации входит в состав группы....

- А) риски кадровой безопасности при работе с персоналом на входе в организацию
- Б) риски кадровой безопасности при работе с персоналом внутри организации
- В) риски при работе с персоналом на выходе из организации

9. Риск создания отрицательного имиджа организации на рынке входит в состав группы....

А) риски кадровой безопасности при работе с персоналом на входе в организацию

Б) риски кадровой безопасности при работе с персоналом внутри организации

В) риски при работе с персоналом на выходе из организации

10. Составной частью любого события является

А) благоприятная возможность

Б) угроза

В) цель

Г) агенты

11. Угроза кадровой безопасности – это...

А) намерение нанести какой-либо вид вреда

Б) возможность появления негативного инцидента в будущем и размер последствий после него

В) совокупность условий и факторов, которые создают опасность жизненно важным интересам участников социально-трудовых отношений, препятствуют эффективному и гармоничному развитию человеческих ресурсов

Г) ситуация, отражающая опасность нежелательного развития событий

Д) какое-то условие, вызывающее неопределенность исхода ситуации

12. По вероятности практической реализации выделяются

А) угрозы материального и нематериального характера

Б) угрозы потенциальные, реализуемые, реализованные

В) угрозы информационной и имущественной безопасности

13. Игровая аддикция – это

А) гэмблинг

Б) кикбэки

В) кайтинг

Г) девиантное поведение

2. СИСТЕМА УПРАВЛЕНИЯ КАДРОВОЙ БЕЗОПАСНОСТЬЮ В ОРГАНИЗАЦИИ

2.1. Структура управления кадровой безопасностью в организации

Обеспечение собственной безопасности, в том числе кадровой, является одним из стандартных направлений деятельности любой современной организации. При ее разработке должно учитываться следующее.

1. Система кадровой безопасности не должна быть стандартной либо универсальной. Она должна создаваться, основываясь на специфике каждой отдельной организации (как внешней, так и внутренней). Такой спецификой могут выступать: внутренние нормы и распорядки, морально-психологический климат в коллективе, специализация, конкуренция рынка и др.

2. Кадровая безопасность организации должна быть согласована с остальными элементами корпоративной безопасности: правовой безопасностью, технико-технологической, информационной и финансовой безопасностью. Только при их полном взаимодействии и согласованности можно обеспечить полную защиту организации от неблагоприятного воздействия.

3. Поскольку кадровая безопасность ориентирована на кадровый состав, то в ее систему необходимо включить соответствующие структуры, элементы, аппараты, механизмы и средства, обеспечивающие должный контроль за деятельностью персонала внутри организации.

Принципы, оказывающие влияние на систему кадровой безопасности (рисунок 12).



Рис. 12. Принципы, оказывающие влияние на систему кадровой безопасности

Система управления кадровой безопасностью организации позиционируется ею в качестве одного из необходимых элементов комплексной системы корпоративного менеджмента (рисунок 13).

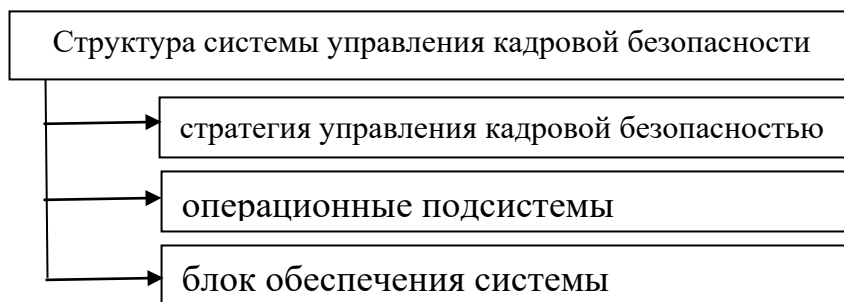


Рис. 13. Структура системы управления кадровой безопасности

Стратегия управления кадровой безопасностью является ключевым элементом системы управления кадровой безопасностью и определяется как совокупность долгосрочных целей и управленческих подходов, реализация которых обеспечивает защиту организации от любых потенциальных угроз, связанных с функционированием кадрового направления ее деятельности.

Стратегии присущи следующие черты:

- она служит инструментом реализации стратегии более высокого уровня (стратегии безопасности организации), ее декларируемых целей, поэтому обоснованным можно считать в качестве целевого ориентира данной стратегии достижение целей организации за счет усиления ее конкурентных преимуществ в результате выявления, оценки, минимизации и нейтрализации кадровых рисков и угроз;

- по своей сути она является функциональной, реализуемой на корпоративном уровне;

- имеет долгосрочный характер, что объясняется необходимостью разработки и реализации планируемых действий по обеспечению кадровой безопасности на перспективу;

- предполагает учет многочисленных факторов внешней и внутренней среды, каждый из которых оказывает влияние на содержание ее структурных элементов, особенности противодействия угрозам кадровой безопасности;

- в основу ее разработки должен быть заложен вероятностный характер реализации угроз со стороны персонала и в его адрес.

На выбор варианта общей стратегии управления кадровой безопасностью организации влияют следующие факторы:

- отрасль или сфера деятельности организации;
- степень агрессивности конкурентной стратегии организации;
- степень легитимности бизнеса организации;
- финансовые возможности организации по обеспечению безопасности;
- квалификация персонала службы безопасности;
- наличие поддержки со стороны органов государственной власти.

Выделяют следующие типы стратегий управления кадровой безопасностью (рисунок 14).

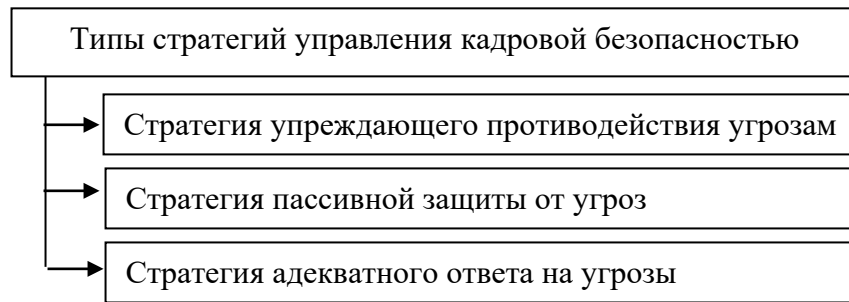


Рис. 14. Типы стратегий управления кадровой безопасностью

Стратегия упреждающего противодействия угрозам. В основе данного варианта лежит стратегическая ориентация руководства организации на максимально жесткое противодействие возможным угрозам кадровой безопасности путем реализации двух принципов.

Первым принципом является выраженный приоритет профилактических методов противодействия возможным угрозам. Исходя из него, уполномоченные инстанции и должностные лица стремятся в первую очередь обеспечить такие условия функционирования кадрового направления деятельности организации, при которых соответствующие угрозы не смогут возникнуть вообще или будут пресечены еще на стадии их подготовки.

Пример. Самым эффективным методом противодействия угрозам переманивания конкурентами наиболее ценных сотрудников выступает реализация в кадровой стратегии работодателя требований законов перемены труда и непрерывного улучшения его условий. В свою очередь, наиболее эффективным методом профилактики угрозы вербовки персонала различными внешними для организации субъектами угроз выступает использование специальных технологий отбора кандидатов на трудоустройство. Такие технологии позволяют выявить и, соответственно, отказать в найме претендентам, личностные качества которых делают их уязвимыми для вербовки (повышенный меркантилизм, сверхамбициозность, эгоцентризм и т.п.).

Вторым принципом является возможность применения для профилактики и отражения возможных угроз не в полной мере легитимных методов. Выбирая между легитимностью и эффективностью того или иного метода, руководители организации отдают предпочтение именно эффективности, несмотря на связанные с этим риски. В этих условиях важной задачей является четкое определение границы между полулегитимными и нелегитимными методами. Пересечение такой границы автоматически выводит организацию из числа законопослушных хозяйствующих субъектов и грозит возможностью применения к нему предусмотренных законом санкций.

Пример. Действующее законодательство категорически не допускает использования работодателями, равно как и частными детективными агентствами, таких методов проверки лояльности сотрудника, как слежка,

проникновение в его жилище с целью установления подслушивающих устройств или проведения негласного обыска. Однако закон не запрещает собирать информацию о гражданине другими методами, например в процессе бесед с сослуживцами, знакомыми, соседями и т.п. Подобные методы нельзя отнести к этическим, поскольку они предполагают вмешательство в частную жизнь, вместе с тем они не являются нелегитимными.

Из всех вариантов стратегии обеспечения кадровой безопасности рассматриваемый вариант является наиболее эффективным, поскольку позволяет работодателю своевременно предупреждать возможные угрозы или пресекать их практически сразу после возникновения. В результате риски имущественных или неимущественных потерь организации, связанные с функционированием кадрового направления ее деятельности, сводятся к минимуму.

Дополнительным преимуществом варианта служит возможность обеспечения поддержки других направлений персонального менеджмента. В процессе исполнения своих функций в рамках рассматриваемой стратегии служба безопасности прямо или косвенно содействует топ-менеджменту, службе персонала, руководителям других структурных подразделений организации в решении поставленных перед ними задач. Это позитивно отражается на конечной эффективности не только управления персоналом, но и всей системы внутрикорпоративного менеджмента.

Пример. В процессе сбора информации о потенциальном партнере в целях выявления отсутствия у него криминальных связей (что является необходимым элементом технологии профилактики покушений на собственников и руководителей организации) служба безопасности может получить данные, дополняющие сведения, собранные другими штабными службами. Вывод службы безопасности о полной законопослушности, но низкой финансовой надежности проверяемой фирмы позволит предотвратить возможный кредитный риск.

Главным недостатком рассматриваемого варианта выступает высокая вероятность конфликтов организации с действующим законодательством, профессиональным союзом и собственными сотрудниками. Конфликты возникают у работодателей, которые, как уже ранее отмечалось, пересекли границу между полулегитимными и откровенно нелегитимными методами. При выявлении сотрудниками фактов прослушивания их телефонных разговоров, скрытого видеонаблюдения (без письменного предупреждения со стороны администрации), принудительного склонения к проверкам на полиграфе (детекторе лжи) становится возможным возбуждение индивидуальных и коллективных (от имени профсоюза) исков к организации. Даже в случае их отклонения судебными инстанциями имиджу данного работодателя на рынке труда может быть нанесен ощутимый ущерб, например, благодаря освещению конфликта средствами массовой информации. Не менее серьезный ущерб организация может понести в случае инициативного увольнения ценного специалиста, обиженного на использование в отношении его специальных мероприятий по контролю потенциальной лояльности.

Вторым, чисто «техническим», недостатком являются необходимость дорогостоящей ресурсной поддержки процесса реализации данной стратегии – финансовой, кадровой, материально-технической, а также высокая трудоемкость осуществляемых в соответствии с ней управленческих процедур.

С учетом последнего недостатка практическая реализация рассматриваемого варианта доступна только для:

- корпораций, занимающих лидирующие позиции на обслуживаемом высоко конкурентном рынке;
- высокорентабельных организаций, работающих в условиях жесткого прессинга со стороны конкурентов или криминальных структур и вынужденных в качестве одного из условий собственного выживания обеспечивать безопасность наиболее эффективными методами.

Стратегия пассивной защиты от угроз. В основе данного варианта лежит стратегическая ориентация руководства организации на фактический отказ от обеспечения кадровой безопасности своими силами путем реализации следующих двух принципов.

Первым принципом является приоритетная ориентация на защиту со стороны государства в лице правоохранительных и судебных органов. Позиционируя себя в качестве добросовестного налогоплательщика, организация предполагает, что и государство, в свою очередь, будет добросовестно исполнять свои традиционные функции, в частности обеспечивать надежную защиту безопасности не только своих граждан, но и законных интересов юридических лиц, в том числе в области безопасности.

Теоретически подобный подход абсолютно корректен и полностью соответствует конституции государства, равно как и другим правоустанавливающим законодательным актам. Однако на практике он может быть сегодня реализован только в ограниченном числе стран, отличающихся высоким уровнем законопослушности населения и приверженностью юридических лиц принципам ведения упорядоченного и социально ответственного предпринимательства.

Вторым принципом является минимизация затрат по рассматриваемому направлению деятельности. Он логически взаимосвязан с первым принципом и предполагает отказ от двойной оплаты собственной безопасности (через налоги государству и через собственный бюджет). В этом случае организация будет финансировать только те затраты, которые обеспечивают минимальный уровень ее безопасности (например, оплачивать две смены сотрудников вневедомственной охраны МВД России).

Основным преимуществом варианта является экономия финансовых ресурсов и трудозатрат на обеспечение кадровой безопасности. Подобная экономия обеспечивается не только за счет отсутствия полноценной службы безопасности, но и благодаря отказу от таких трудоемких управленческих процедур, связанных с текущим управлением персоналом, как:

- тщательный отбор кандидатов на трудоустройство в целях отсева потенциально нелояльных сотрудников;

- специальное обучение новых сотрудников правилам обеспечения безопасности работодателя;
- специальная подготовка всех категорий менеджеров;
- мониторинг психологического климата в трудовом коллективе в целях своевременного выявления недовольных сотрудников и т.п.

Другим преимуществом является полное отсутствие каких-либо угроз конфликтов и связанных с ними проблем в отношениях с государством, собственным персоналом, профсоюзом. Реализация рассматриваемого варианта предполагает автоматический отказ от применения не только нелегитимных, но и полулегитимных методов обеспечения безопасности. Таким образом, конкретная организация не только демонстрирует свою полную законопослушность, но и не дает повода к недовольству со стороны сотрудников и их профессиональных объединений.

Основным недостатком варианта является полная зависимость безопасности организации от внешних, не зависящих от нее факторов:

- общей законопослушности населения конкретной страны;
- исторически сложившихся в ней традиций ведения профессионального предпринимательства;
- эффективности действующего законодательства;
- качества работы правоохранительных органов и судебных инстанций.

Выше уже отмечалось, что благоприятные условия для реализации рассматриваемого варианта сегодня существуют лишь в очень немногих странах, в число которых Россия не входит. Поэтому попытка отечественного работодателя полностью положиться на государство в части обеспечения безопасности, скорее всего, станет фатальной для его бизнеса.

Вторым недостатком варианта выступает ориентация на методы противодействия уже реализованным угрозам, в данном случае – в режиме обращения за помощью к государству в целях наказания виновников и возмещения нанесенного ущерба. Из всех групп методов обеспечения безопасности карающие методы являются наименее эффективными в сравнении с методами профилактическими и пресекающими. Следует учитывать, что в отношении некоторых видов угроз кадровой безопасности практически не существует легитимных карающих методов.

Пример. У организации нет никаких законных возможностей для наказания конкурента, открыто переманивающего лучших ее специалистов. Ни в одной стране не существует законных инструментов, позволяющих в полном объеме возместить ущерб имиджу работодателя, пострадавшему в результате разглашения нелояльным сотрудником конфиденциальной клиентской информации. Более того, в законодательстве ряда стран (например, США) существует прямой запрет на применение каких-либо санкций к сотруднику, передавшему государственным надзорным органам информацию о финансовых нарушениях, допущенных работодателем.

С учетом указанных недостатков практическая реализация рассматриваемого варианта в нашей стране доступна только:

- организациям, фактически принадлежащим государству, статус которых автоматически предполагает эффективную централизованную защиту их безопасности;

- организациям любого организационно-правового статуса, в безопасности которых реально заинтересованы конкретные органы государственной власти или субъекты крупного бизнеса;

- низкорентабельным субъектам малого и среднего бизнеса, работающим на низкоконтурных сегментах рынка.

Стратегия адекватного ответа на угрозы. В основе данной стратегии лежит стратегическая ориентация руководства организации на компромисс между первым и вторым вариантом, смягчающий их радикальные недостатки, но и не позволяющий в полной мере использовать соответствующие преимущества. Ориентация на такую стратегию предполагает возможность использования службой безопасности всего комплекса легитимных методов профилактики и отражения потенциальных угроз. В порядке исключения допускается использование и не полностью легитимных методов, но лишь в отношении тех конкурентов или иных источников угроз, которые первыми применили подобные методы.

Стратегия адекватного ответа на угрозы рекомендуется для большинства современных работодателей.

Следующий элемент системы управления кадровой безопасностью – это **операционные подсистемы**, каждая из которых направлена на решение формализованного перечня однотипных задач по обеспечению данного вида безопасности организации. Отражая установленные стратегией управления цели и приоритеты, операционные подсистемы имеют своими объектами:

- противодействие угрозам безопасности сотрудников организации;

- противодействие угрозам безопасности организации со стороны ее сотрудников.

В соответствии с методологией менеджмента, при формировании операционных подсистем необходимо соблюдать следующие общие требования:

- подсистемы не могут содержать элементов (методов, процедур и т.п.), практическое функционирование которых может объективно затруднить эксплуатацию смежных подсистем;

- общая структура каждой из подсистем должна соответствовать следующей типовой схеме: «определение целей процесса – планирование и организация процесса – оперативное управление процессом – оценка результатов процесса путем сопоставления их с ранее запланированными целями»;

- формализованное закрепление функций, связанных с эксплуатацией подсистем, за соответствующими руководителями и специалистами, как штабных, так и коммерческих подразделений организации, включая и механизм персонифицированной ответственности за их выполнение.

Блок обеспечения является необходимой частью любой системы управления. Формируя исходные условия для эффективного управления, он включает в себя несколько направлений (рисунок 15).

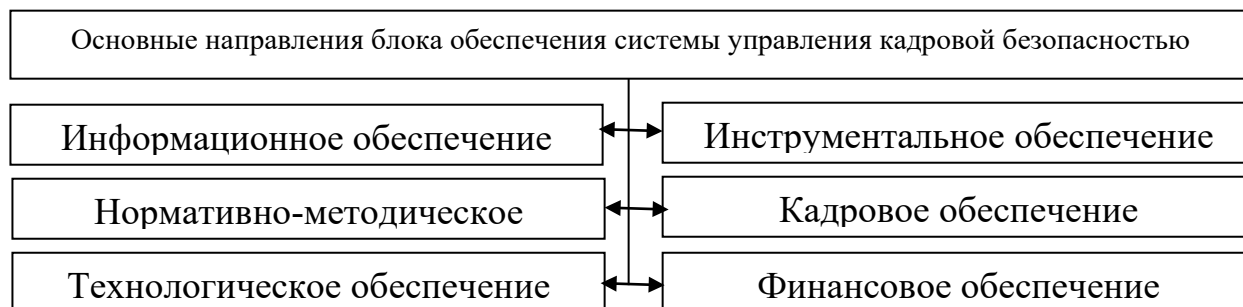


Рис. 15. Направления блока обеспечения системы управления кадровой безопасностью

Информационное обеспечение системы управления кадровой безопасностью включает в себя три компонента:

- используемые в рамках системы методы и конкретные процедуры получения субъектами управления необходимой первичной информации;
- формализованные каналы прохождения информации в рамках системы, которые определяют маршрут движения ранее собранной информации по инстанциям (принципиальная схема: «от кого - кому - в какой форме - в какие сроки»);
- базы данных, связанных с любыми проблемами внутренней и внешней кадровой безопасности, которые накапливаются и обновляются в течение всего периода функционирования конкретной организации и используются при формировании управленческих решений любого уровня.

Нормативно-методическое обеспечение включает в себя комплект внешних и внутренних регламентов, используемых в процессе управления рассматриваемым направлением деятельности, а также документов рекомендательного, т.е. не директивного характера.

К внешним регламентам относятся законодательные и подзаконные акты, которыми обязаны руководствоваться все организации в процессе обеспечения собственной кадровой безопасности.

Основные законодательные акты, действующие в рассматриваемой области:

- Конституция РФ;
- Трудовой кодекс РФ;
- Закон РФ «О безопасности»;
- Закон РФ «О частной детективной и охранной деятельности в РФ»;
- Федеральный закон «Об информации, информационных технологиях и защите информации»;
- Закон РФ «О государственной тайне»;
- Федеральный закон «О коммерческой тайне».

К числу подзаконных актов относятся различные положения, инструкции, иные регламенты, введенные в действие уполномоченными органами исполнительной власти государства (Правительством РФ, Министерством труда и социальных отношений, Министерством внутренних дел и др.), например, Постановление Правительства РФ «О перечне сведений, которые не могут составлять коммерческую тайну».

К внутренним регламентам и рекомендациям относятся любые постоянно действующие документы, разработанные в рамках конкретной организации и введенные в соответствии с действующим в ней порядком – инструкции, приказы, распоряжения и т.п. Единственным ограничением при разработке внутренних регламентов является их хотя бы формальное соответствие (непротиворечивость) действующему законодательству.

Основные документы, необходимые для эффективного управления кадровой безопасностью организации:

- положения о службе персонала организации;
- положения о службе безопасности организации;
- должностные инструкции топ-менеджеров, возглавляющих соответствующие направления деятельности организации, специалистов кадровой службы и службы безопасности, а также руководителей всех структурных подразделений;
- инструкции, определяющие порядок работы с конфиденциальной информацией (базами данных, документами на бумажных носителях), правила проведения конфиденциальных переговоров и т.п.;
- инструкции, определяющие порядок работы с имущественными комплексами организации в части обеспечения их сохранности;
- рекомендации сотрудникам организации в рассматриваемой области (например, «Памятка молодому специалисту организации»).

Технологическое обеспечение определяется как совокупность формализованных технологий обеспечения безопасности организации от различных видов кадровых угроз. Их наличие является основной предпосылкой эффективности управления, поскольку позволяет четко определить:

- непосредственных участников (инстанции и рабочие места, принимающие участие в описываемой операции по защите от конкретной угрозы);
- управленческие процедуры (мероприятия, осуществляемые в рамках операции);
- типовые сроки по операции в целом и каждой управленческой процедуре в отдельности;
- ответственность участников за нарушение описываемой технологии.

Инструментальное обеспечение определяется как совокупность прикладных методов управления, используемых в рамках системы. Классификация этих методов по различным признакам представлена в таблице 3.

Кадровое обеспечение – полностью укомплектованный штат службы безопасности, включающий в себя три квалификационные категории работников:

- руководители различного уровня – от вице-президента, отвечающего за данное направление до бригадира смены охранников;
- высококвалифицированные сотрудники службы безопасности, специализирующиеся на определенных направлениях ее обеспечения (аналитики, разработчики специальных программных средств и т.п.), но не выполняющие при этом прямых управленческих функций;
- исполнители (охранники, ремонтники спецоборудования и др.).

Финансовое обеспечение определяется как совокупность финансовых ресурсов, выделяемых на поддержание и развитие рассматриваемого направления (приобретение спецоборудования, зарплата персонала, оплата информации и т.п.).

Таблица 3

Классификация методов противодействия угрозам кадровой безопасности организации

Признак классификации	Методы противодействия
По времени реализации	– профилактические или превентивные методы, которые используются для предотвращения потенциальных угроз или на стадии их фактического зарождения; – пресекающие или отражающие методы используются для противодействия уже реализуемым угрозам с целью полного предотвращения или минимизации связанного с ними ущерба; – карающие или репрессивные методы, которые используются для наказания виновников уже реализованных угроз и имеют своей целью не столько возмещение уже нанесенного организации ущерба сколько предупреждение реализации аналогичных угроз в дальнейшем.
По характеру действия	– методы административного характера, предполагающие принятие руководством организации тех или иных административных решений, направленных либо на профилактику потенциальных угроз, либо на наказание их виновников; – методы экономического характера, либо создающие необходимую мотивацию у сотрудников организации как потенциальных объектов угроз, либо реализуемые в виде санкций к сотрудникам как субъектам угроз; – методы психологического характера, используемые преимущественно для профилактики возможных угроз и имеющие как коллективную, так и индивидуальную направленность.
По степени легитимности	– методы легитимного характера, реализация которых не противоречит не только действующему законодательству, но и нормам коммерческой этики в области трудовых и конкурентных отношений; – методы нелегитимного характера, реализация которых всегда противоречит нормам предпринимательской и коммерческой этики, реже предполагает определенные нарушения действующего законодательства, не связанные с привлечением виновных к уголовной ответственности; – криминальные методы, факт реализации которых всегда предполагает привлечение виновных к уголовной ответственности.

Необходимым элементом обеспечения кадровой безопасности организации является *оценка ее эффективности*. Она позволяет решить несколько прикладных задач, в частности, осуществлять статистический анализ вероятности негативной реализации тех или иных угроз, а также объективно оценивать результативность деятельности службы безопасности. В отличие от большинства других направлений менеджмента здесь не всегда можно точно подсчитать обеспеченный экономический эффект. В частности, затруднительно определить возможные потери от своевременно пресеченных угроз. По некоторым видам угроз, например, в адрес сотрудников организации прямой эффект невозможно рассчитать в принципе. Поэтому приходится опираться на результаты не только прямой, но и косвенной оценки. Критериями оценки эффективности системы управления кадровой безопасностью организации являются:

- общее количество выявленных угроз с дифференциацией на угрозы, пресеченные в полном объеме, пресеченные лишь частично, негативно реализованные в полном объеме (в динамике в сравнении с предыдущими периодами);
- прямой финансовый ущерб, нанесенный организации в результате частично и полностью реализованных угроз;
- потенциальный ущерб, который могли бы нанести организации полностью или частично пресеченные угрозы;
- результаты реализации плановых профилактических мероприятий;
- отсутствие обоснованных претензий к службам обеспечения кадровой безопасности со стороны правоохранительных органов, собственных подразделений и отдельных сотрудников.

Процесс управления кадровой безопасностью представляет собой последовательность определенных действий, реализация которых позволит сформировать определенное управленческое воздействие. Он должен строиться на основе системного подхода, учитывающего все аспекты обеспечения безопасности (рисунок 16).

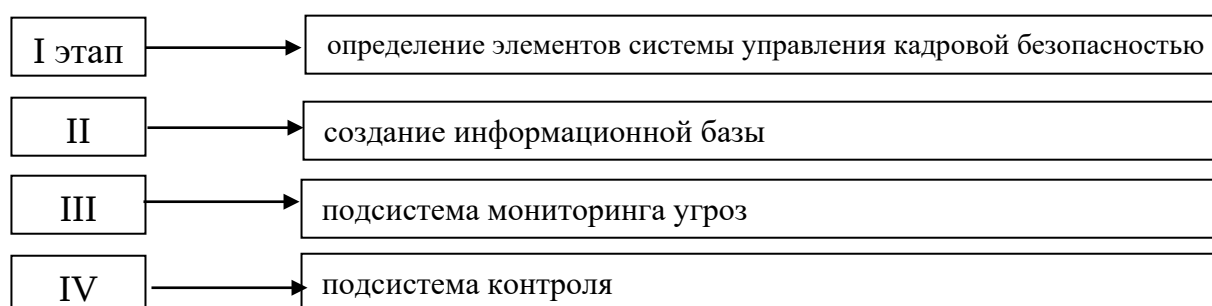


Рис. 16. Схема процесса управления кадровой безопасностью организации

Первый этап – определение элементов системы управления кадровой безопасностью – имеет важное концептуальное значение в организации самого процесса управления. Правильно должны быть определены не только элементы системы, но и существующие между ними взаимосвязи. К элементам системы

управления кадровой безопасностью можно отнести субъекты, объекты, подходы к управлению, приемы и инструментарий управления.

Суть второго этапа – формирование информационно-методического обеспечения оценки состояния кадровой безопасности – заключается в создании информационной базы, позволяющей проводить оценку состояния кадровой безопасности, а также методической базы, включающей методики оценки, учитывающие специфику деятельности организации.

На третьем этапе проводится диагностика уровня кадровой безопасности, включающая расчет оценочных показателей и параметров. Подсистема мониторинга угроз включает в себя два этапа:

- 1) выявление внешних и внутренних угроз кадровой безопасности;
- 2) разработку и внедрение мероприятий по предупреждению (или нейтрализации) угроз.

Подсистема контроля (четвертый этап) должна обеспечивать оценку эффективности внедренных мероприятий по предупреждению или нейтрализации угроз кадровой безопасности, а также уровня управления кадровой безопасностью. Данная подсистема дает основания для корректировки выполнения любого из этапов управления кадровой безопасностью организации.

Таким образом, управление кадровой безопасностью организации позволяет своевременно реагировать на вызовы окружающей среды и обеспечивать эффективность не только персонал-менеджмента, но и управленческих процессов в целом.

2.2. Субъекты и объекты системы управления кадровой безопасностью в организации

Субъект кадровой безопасности – это активный участник процессов в деятельности обеспечения кадровой безопасности, воздействующий на объект кадровой безопасности независимо от характера этого воздействия: наносящего ущерб, разрушение или противодействующего этому.

Сотрудник организации является центральным, ключевым звеном всей совокупности субъектов кадровой безопасности, так как он, с одной стороны, выполняет функции по обеспечению кадровой безопасности организации, а с другой стороны, он может стать источником любой угрозы хозяйствующему субъекту, кроме техногенных угроз, природных катаклизмов, и противодействовать системе корпоративной безопасности.

Все причины, вследствие которых сотрудник становится источником угроз корпоративной безопасности хозяйствующего субъекта, можно разделить на девять групп в соответствии с их характером (рисунок 17).

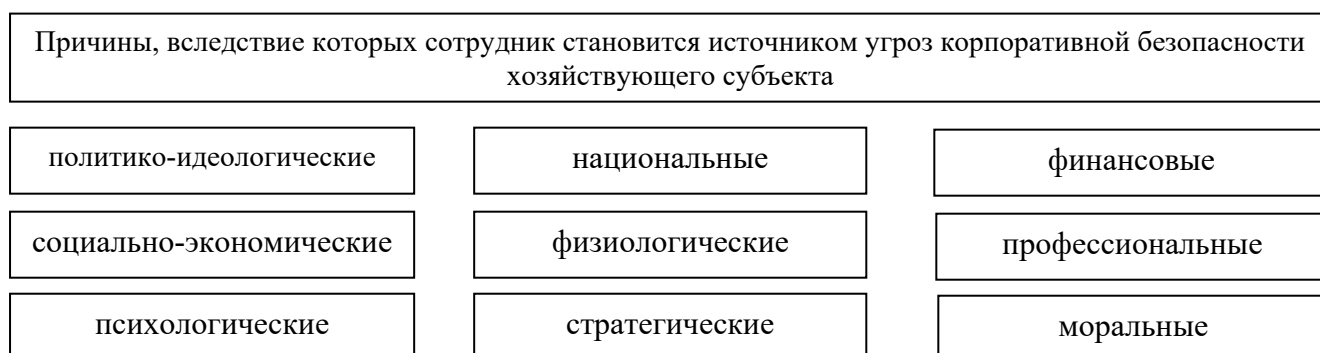


Рис. 17. Причины, вследствие которых сотрудник становится источником угроз корпоративной безопасности хозяйствующего субъекта

Все множество субъектов кадровой безопасности, аналогично субъектам безопасности, можно разделить на две группы (рисунок 18).



Рис. 18. Группы субъектов кадровой безопасности

К *внешним субъектам, способствующим обеспечению кадровой безопасности*, относятся:

- органы законодательной, исполнительной и судебной власти федерального уровня, исполнительной и судебной власти субъектов Федерации, органов местного управления;
- правоохранительные органы;
- функциональные и отраслевые министерства и ведомства;
- налоговые и таможенные службы;
- специально создаваемые органы и организации, координирующие и контролирующие социальные и трудовые вопросы (федеральные службы занятости, трудовые инспекции, региональные комитеты по труду и социальным вопросам, службы охраны труда и т.п.);
- страховые компании;
- биржи, банки и иные хозяйствующие субъекты;
- общества защиты прав потребителей;
- граждане и их объединения.

К *внешним субъектам, противодействующим обеспечению кадровой безопасности*, относятся конкуренты, теневые экономические структуры и

элементы криминальных структур, бывшие сотрудники, неудовлетворенные оценкой своего труда.

К *внутренним субъектам, способствующим обеспечению кадровой безопасности*, относятся сотрудники и структурные подразделения (в том числе и специальные), непосредственно осуществляющие деятельность по защите кадровой безопасности организации на основании предоставленных им исполнительным органом организации полномочий принимать решения о целях, задачах, средствах и методах обеспечения кадровой безопасности и осуществления их:

- служба безопасности и ее сотрудники;
- сотрудники специализированных организаций, оказывающих услуги по договору;
- финансовая служба в целом и ее сотрудники;
- экономическая служба в целом и ее сотрудники;
- юридическая служба в целом и ее сотрудники;
- кадровая служба в целом и ее сотрудники;
- бухгалтерская служба в целом и ее сотрудники;
- техническая служба в целом и ее сотрудники;
- служба автоматизации производственных процессов в целом и ее сотрудники;
- служба внутреннего аудита в целом и ее сотрудники и т.д.

К *внутренним субъектам, противодействующим обеспечению кадровой безопасности* организации, относятся сотрудники, не удовлетворенные оценкой их труда.

Условный перечень функциональных обязанностей по обеспечению кадровой безопасности в организации представлен в таблице 4.

Таблица 4

Направления деятельности по обеспечению кадровой безопасности организации

Категория сотрудников	Направления деятельности
Руководство организации	– разработка общей стратегии кадровой безопасности организации; – обеспечение финансовых и иных ресурсов для реализации стратегии; – мобилизация и стимулирование персонала к участию в реализации кадровой стратегии организации; – контроль над общей эффективностью системы.
Служба безопасности	– разработка и практическая реализация стратегии управления кадровой безопасностью; – методическое руководство деятельностью других подразделений компании; – специальное обучение персонала организации; – общий мониторинг соответствующего направления деятельности других подразделений организации; – организация служебных расследований; – выполнение соответствующих заявок со стороны других подразделений, включая службу персонала;

Категория сотрудников	Направления деятельности
	– общая ответственность за эффективность системы управления.
Службы технического контроля	– анализ безопасности компьютерных программ, систем; – защита конфиденциальной информации, блокада информационных атак.
Служба управления персоналом	– разработка текущих и плановых значений показателей кадровой безопасности для целей стратегического и оперативного планирования; – постоянный мониторинг установленных показателей в сфере своей ответственности и предоставление отчетности; – информирование руководства и службы безопасности при получении сигнала о негативном отклонении значения показателя либо об изменении направления тенденций плановых величин.
Службы экономического контроля, бухгалтерия	– экономический контроль за расходом ресурсов организации; – содействие в осуществлении мотивационных программ.
Руководители структурных подразделений	– текущая работа по специальному обучению подчиненных; – текущий контроль над соблюдением подчиненными правил обеспечения безопасности; – оперативное взаимодействие со службой безопасности
Иные специалисты	– сообщение руководству о подозрительных событиях, поведении сотрудников – следование правилам внутреннего распорядка предприятия

Из таблицы 4 видно, что обеспечение кадровой безопасности сопряжено с деятельностью практически всех сотрудников предприятия, взаимодействующих между собой.

В некоторых российских организациях существует неоправданное мнение, что проблемами, связанными с безопасностью, должна заниматься в основном только служба безопасности. Однако практика показывает, что служба управления персоналом не менее важный субъект, а в некоторых организациях – более значительный:

– во-первых, подбором, оценкой, развитием и т.п. сотрудников службы безопасности занимается именно служба управления персоналом, с помощью чего она оказывает влияние на обеспечение безопасности, в том числе кадровой;

– во-вторых, прямая обязанность специалистов службы управления персоналом – способствовать достижению целей фирмы с помощью персонала, что подразумевает минимизацию негативных влияний со стороны персонала;

– в-третьих, колоссальное количество методов и возможностей обеспечения кадровой безопасности находится в руках именно сотрудников службы персонала.

Кроме того, служба управления персоналом:

– принимает участие в формировании корпоративной культуры;
– участвует в стратегическом планировании безопасности предприятия;
– разрабатывает кадровую политику с учетом проблем кадровой безопасности;

- участвует в разработке нормативных документов, касающихся внутренней деятельности компании;

- ведет документацию дисциплинарной практики.

Специалисты кадровых служб имеют возможность почти на 60% снизить убытки компании, связанные с персоналом и трудовыми отношениями в целом.

Таким образом, служба персонала – более важный субъект в кадровой безопасности, чем служба безопасности.

Рассмотрим более подробно функциональные обязанности ее сотрудников. К ним относятся:

- участие в формировании корпоративной культуры, способствующей реализации кадровой безопасности, и ее мониторинг, включая лояльность персонала;

- участие в стратегическом планировании безопасности предприятия и реализация собственных инициатив обеспечения кадровой безопасности;

- разработка кадровой политики с учетом проблем кадровой безопасности;

- участие в разработке нормативных документов, касающихся внутренней деятельности компании;

- приём на работу, увольнение сотрудников;

- взаимодействие с другими подразделениями компании (службой безопасности, финансовыми и юридическими подразделениям, обеспечивающими подразделениям, службами и специалистами);

- прямой и оперативный выход на руководство компании и службы безопасности;

- контакты с территориальными инспекциями по труду, военными комиссариатами, органами внутренних дел и т.д.;

- мониторинг каналов неофициальной информации, изменений в законодательстве, рынка труда;

- предупреждение и разрешение трудовых конфликтов;

- контроль за осуществлением процедур кадровой безопасности и помощь в их осуществлении.

Функции кадровой безопасности в системе управления персоналом представлены в таблица 5.

Таблица 5

Задачи обеспечения кадровой безопасности организации в аспекте функций управления персоналом

Функциональные блоки управления персоналом	Задачи в области обеспечения кадровой безопасности
Планирование и маркетинг персонала	Определение должностей, со стороны которых могут исходить угрозы корпоративной безопасности, необходимой численности персонала. Мониторинг угроз жизненно важным интересам организации, направленный на обеспечение кадровой безопасности.
Управление наймом и учетом кадров	Оценка благонадежности кандидатов на вакантную должность (выявление у них аддикций, автобиографических данных, вызывающих обоснованные сомнения и пр.). Формирование требований к сотрудникам относительно безопасности.
Управление трудовыми отношениями	Минимизация конфликтов, трудовых споров. Формирование у персонала лояльности. Сохранение благоприятного социально-психологического климата в коллективе. Выявление, предупреждение и пресечение нежелательных действий со стороны работников, могущих повлечь нанесение вреда интересам компании. Обеспечение контроля над соблюдением правил обеспечения безопасности работника и работодателя.
Обеспечение нормальных условий труда	Сохранение и поддержание физического и психологического здоровья персонала как залога обеспечения его физической безопасности. Создание для сотрудников условий труда, минимизирующих вероятность их переманивания.
Управление развитием персонала	Организация обучения персонала правилам обеспечения личной безопасности и безопасности организации, методам распознавания мошеннических действий со стороны клиентов предприятия и других контрагентов; методам защиты информации и интеллектуальной собственности.
Управление мотивацией	Создание у сотрудников устойчивой мотивации к соблюдению правил обеспечения информационной, имущественной и личной безопасности. Стимулирование закрепления кадров. Выявление мотивов и причин увольнения ценных сотрудников и места их последующего трудоустройства.
Управление социальным развитием	Разработка дополнительных социальных гарантий сокращаемому персоналу и содействие в трудоустройстве. Формирование компенсационного пакета с учетом требований безопасности со стороны организации и работника, а также дополнительных опций тем работникам, которые обеспечивают социальное и экономическое развитие организации, и т.д.
Развитие организационной структуры	Регламентация функций безопасности, четкое разделение обязанностей среди подразделений и должностных лиц по обеспечению безопасности и т.д.
Правовое обеспечение	Контроль за соблюдением работниками трудового и гражданского законодательства при выполнении трудовых обязанностей. Предотвращение возможных обращений в суд и проверяющие инстанции, минимизация материальной ответственности работника и работодателя по возникающим трудовым спорам. Разработка локальных нормативных актов, касающихся обеспечения кадровой безопасности и т.д.
Информационное обеспечение	Проведение информационно-разъяснительной работы с сотрудниками о правилах проведения деловых переговоров, общения с клиентами, тактике поведения при попытках вербовки и шантажа, обеспечения информационной безопасности работодателя в рабочее и нерабочее время.

В области обеспечения безопасности предприятия служба управления персоналом осуществляет теснейшее взаимодействие со службой безопасности.

Их функции в контексте кадровой безопасности по сути своей сходны, но имеются и различия.

Главное отличие заключается в направленности деятельности. Если служба безопасности осуществляет всестороннее обеспечение безопасности компании (силовую, информационную, техническую), то служба управления персоналом занимается только кадровыми вопросами, хотя и в широком смысле. Как бы там ни было, её (службы управления персоналом) деятельность более специализирована с точки зрения безопасности.

Например, при отборе и приеме на работу служба персонала осуществляет проверку профессионализма претендента, соответствия его корпоративной культуре организации. Сотрудники службы безопасности проверяют его на отсутствие судимости, связей с криминальными структурами, подлинность документов и других сведений. В период адаптации вновь принятого сотрудника служба персонала обеспечивает усвоение культурных норм организации, минимизирует недовольство, не допускает его увольнения. Служба безопасности контролирует поведение нового сотрудника с точки зрения недопущения вредных действий сейчас и в будущем.

Кроме того, служба безопасности ответственна за корпоративную разведку, контрразведку, отслеживание нарушения правил внутри компании, используя каналы коммуникации и методы «e-spy» (электронные шпионские методы – просмотр электронной почты и транзакций в локальной сети работников, организация прослушивания и/или определения входящих и исходящих вызовов мобильных телефонов, создания досье о личной жизни сотрудников и т.д.).

Выделяют следующие стратегические подходы к организации службы безопасности.

Первый подход предполагает полный отказ от услуг сторонних специализированных структур и формирование полноценной (по функциям) собственной службы безопасности. Преимущества этого подхода заключаются в большей степени доверия к штатным сотрудникам и их высокой степени мотивированности к эффективной работе. Однако этот подход требует больших затрат на содержание подобной службы. Кроме того, существуют объективные сложности с комплектацией ее высококвалифицированными сотрудниками всех необходимых специальностей.

Он рекомендуется для организаций, реализующих стратегию упреждающего противодействия угрозам.

Второй подход предполагает минимизацию штатных сотрудников службы безопасности, с возложением основных ее функций на сторонние специализированные структуры, привлекаемые на договорной основе. С одной стороны, этот подход менее затратный и позволяет руководству организации снять с себя ответственность за нелегитимные действия привлеченного частного агентства, с другой, сторонние для организации сотрудники вызывают меньше доверия, а система управления безопасностью организации менее оперативна.

Он подходит для организаций, реализующих стратегию пассивной защиты от угроз.

Третий подход предполагает возможность ограниченного использования услуг специализированных частных структур для выполнения локальных задач, обычно сомнительных с позиции их легитимности. Данный вариант является компромиссом между первым и вторым вариантами, смягчая радикальные недостатки, но и не позволяя в полной мере использовать их преимущества. Рекомендуется для большинства современных работодателей.

Для обеспечения кадровой безопасности нужна согласованная работа службы управления персоналом и службы безопасности организации. Структура совместно выполняемых этими службами функций представлена в таблице 6.

Таблица 6

Структура совместно выполняемых службой персонала и службой безопасности функций

Функции службы управления персоналом	Функции службы безопасности организации
Отбор персонала	Проверка по базам данных
Оформление на работу	Уровень допуска к информации
Адаптация работника	Инструктаж по правилам безопасности и внутреннего распорядка
Социальная поддержка работника	Юридическая помощь работнику
Управление трудовой дисциплиной	Пропускной и внутриобъектовый режим
Управление конфликтами	Юридическая помощь работникам

Работа службы безопасности организации будет эффективна, если будут соблюдены следующие условия:

- профессионализм, т.е. создавать систему безопасности должны профессионалы, ориентированные на долговременное сотрудничество;
- доверие, т.е. руководитель службы безопасности должен быть доверенным лицом топ-менеджера;
- взаимопонимание, т.е. необходимо смириться с тем, что меры безопасности на первых порах создают трудности и неудобства как для персонала, так и для руководителей организации.

Контроль над деятельностью службы безопасности осуществляется по трем направлениям:

- со стороны правоохранительных органов – отсутствие нарушений законодательства при исполнении службой безопасности своих функций;
- со стороны руководства организации – эффективность исполнения установленных ей функций и отсутствие фактов превышения установленных полномочий;
- в режиме внутреннего контроля в рамках самой службы – по аналогу с деятельностью службы собственной безопасности в государственных правоохранительных органах.

Основные структурные подразделения службы безопасности представлены на рисунке 19.

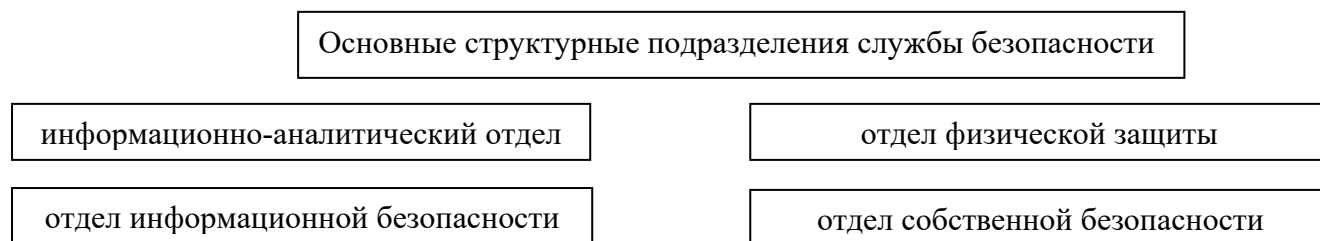


Рис. 19. Основные структурные подразделения службы безопасности

2.3. Условия эффективного функционирования системы управления кадровой безопасностью

Чтобы система управления кадровой безопасностью организации функционировала эффективно, необходимо выполнение определенных условий (рисунок 20).

1. Главным условием эффективного функционирования системы управления кадровой безопасностью организации является *системный подход*. Под ним понимается недопустимость акцентирования усилий службы безопасности на отражении какого-либо одного или нескольких видов потенциальных угроз в ущерб остальным.



Рис. 20. Условия эффективного функционирования системы управления кадровой безопасностью организации

Приведем примерный перечень некоторых потенциальных угроз персоналу:

- прямое переманивание конкурентами ведущих руководителей и специалистов;
- вербовка сотрудников конкурирующими и криминальными структурами, а в отдельных случаях – правоохранительными органами;
- шантаж или прямые угрозы в адрес конкретных сотрудников с целью склонения их к нарушению доверия со стороны работодателя (т.е. к совершению различных должностных нарушений);
- покушения на сотрудников (прежде всего высших руководителей) и членов их семей.

Поскольку подобные угрозы могут быть реализованы в любой организации и по отношению к любому сотруднику, к которому по той или иной причине появился интерес со стороны злоумышленников, поэтому, создавая систему корпоративной безопасности, необходимо иметь в виду их все. Особое внимание следует уделять защите персональной информации, личных специфических данных о работнике как основных факторах их (угроз) осуществления злоумышленниками.

Однако данное требование не должно противоречить принципу рационального ранжирования потенциальных угроз.

Ранги угроз определяют планирование деятельности по их предупреждению и нейтрализации. В соответствии с целевым подходом ранг определяется тем, в какой степени соответствующая угроза снижает интегральную оценку безопасности. Для его определения необходимо сравнить значения интегральных оценок безопасности, получаемые для всей совокупности угроз, и значения безопасности при отсутствии каждой из них. Разность значений будет являться рангом угрозы, поскольку характеризует ее «негативный вклад». Значения рангов должны быть отнормированы на каком-либо удобном для восприятия интервале.

Также как и оценки безопасности, ранги могут быть определены на текущий момент (единичный интервал анализа, например, год) и в масштабе стратегической перспективы.

Ранжирование угроз позволяет выявить, какие из них более серьезны по размерам возможного ущерба, а какие – менее серьезны, какие более вероятны, какие – менее.

Это соотношение обычно представляется в виде треугольника, самый низкий уровень которого представлен наиболее частыми ущербами, небольшими по размерам. Средний уровень – убытки менее частые, но более серьезные по размерам. Верхний слой – катастрофические, достаточно редкие ущербы.

Если в отношении первых двух типов ущербов организация может полагаться на собственные возможности покрытия, то это невозможно при катастрофических ущербах. Их серьезность ставит под угрозу сохранение организации, и финансовые ресурсы для ликвидации последствий ущерба

могут быть найдены только на основе внешнего страхования. Поэтому для организации полезна даже самая простая количественная оценка угроз.

Вероятность и серьезность ущербов оценивается по специальной шкале коэффициентов, которые могут определяться экспертами на основе прошлого опыта.

2. Вторым условием определяется *приоритет мероприятий по предотвращению потенциальных угроз* (т.е. методов профилактического характера). Оно не требует дополнительных обоснований уже в силу обеспечиваемой возможности не допустить ущерба в принципе, тогда как прочие методы в лучшем случае позволяют его сократить или наказать виновников.

Известно, что в динамике система обеспечения корпоративной безопасности проходит три этапа:

- меры по профилактике и выявлению;
- меры по предотвращению и противодействию;
- меры по локализации, минимизации негативных последствий и восстановлению первоначального положения дел.

Целью системы профилактики является предупреждение, затруднение, ограничение и блокирование любых возможностей навредить компании, совершить в отношении нее противоправные действия. Общепрофилактические меры являются превентивными, носят предупредительный характер, осуществляются преимущественно гласно.

Меры по предотвращению и противодействию противоправной деятельности направлены на раннее выявление, локализацию и недопущение соответствующих действий. Они могут реализоваться как в гласной, так и в негласной форме.

Третий этап обеспечения корпоративной безопасности предполагает регламентацию и распределение обязанностей между всеми субъектами, обеспечивающими безопасность, по минимизации негативных последствий противоправных действий и возмещения компании утраченных активов.

Возможности по совершению противоправных действий не сложно просчитать заранее по точкам уязвимости – точкам риска. Скажем, для торговой компании это: хранение товаров на складе, перемещение со склада в торговый зал, нахождение в торговом зале и продажа клиенту.

Комплекс профилактических мер должен включать в себя:

- разработку, введение и поддержание в компании различных режимов безопасности: физической безопасности и охраны объектов, информационной безопасности, социально-психологической безопасности в коллективе, коммуникационной безопасности и противодействию возможной разведывательной деятельности конкурентов и т.п.;

- четкую регламентацию и организацию всех процессов, привлекательных для совершения противоправных действий, в том числе с помощью корпоративного кодекса, инструкций по обеспечению конфиденциальности и сохранению коммерческой тайны, четких должностных инструкций каждого

сотрудника, а также осуществления строгого контроля за их выполнением (документального, визуального, с помощью видеокамер и т.п.);

- справедливую материальную и моральную оценку результатов труда сотрудников, их компетентности и лояльности, позволяющую создать здоровый морально-психологический и этический климат в коллективе;

- профилактическую роль играют любые методы мониторинга и контроля поведения сотрудников, уровня жизни, контактов (прежде всего, с клиентами, поставщиками), использования рабочего времени, ресурсов компании, предоставляемой бухгалтерской и финансовой отчетности и т.п.

Противодействие включает в себя:

- процедуру постоянного мониторинга и контроля за соблюдением установленных режимов безопасности, отслеживание происходящих в коллективе процессов, их причин, хода развития, включая анализ будущих возможных вариантов развития данных процессов и явлений;

- разработанную систему независимого автоматического объективного фиксирования нарушений, отклонений от нормы, несоблюдения регламента и мгновенного информирования руководства об этих отклонениях;

- принятие соответствующих мер административно-правового характера, проведения служебного расследования, в том числе с возможным привлечением правоохранительных органов;

- формирование штаба по управлению в чрезвычайных ситуациях, введение режима работы в чрезвычайных условиях, проведение необходимых экстренных действий, разработку путей выхода из кризиса.

Восстановление первоначального положения возможно двумя основными путями: добровольным или принудительным возмещением сотрудником урона, нанесенного компании. Мотивами добровольного возмещения могут быть чувство стыда, страх огласки, боязнь уголовного преследования, опасение потери репутации и доброго имени. К сожалению, в современной практике не часто удается возместить урон с использованием такой мотивации. Особенно если у компании отсутствуют прямые доказательства вины сотрудника. В этих случаях приходится прибегать к проведению служебного расследования и принятию на его основе правовых решений, обязывающих мошенника возместить нанесенный урон.

Остановимся более подробно на угрозе переманивания ценных сотрудников организации. Единственным эффективным методом профилактики этой угрозы является устранение типовых причин недовольства сотрудников, чем обычно и пользуются конкуренты. К наиболее распространенным причинам относятся:

- неудовлетворенность экономическими и социальными условиями найма;
- отсутствие перспектив профессионального и карьерного роста;
- неудовлетворенность общим состоянием психологического климата;
- неудовлетворенность отношениями с непосредственным руководителем (чаще всего – из-за отсутствия у него необходимых личностных качеств, реже – в силу объективной психологической несовместимости);
- неудовлетворенность отношениями с коллегами по работе.

Ранжирование перечисленных причин по вероятности их практической реализации зависит, прежде всего, от возрастной или квалификационной категории, к которой принадлежит конкретный сотрудник (например, для граждан предпенсионного возраста приоритетное значение имеют высокая зарплата и социальный пакет, для молодых специалистов – перспективы карьерного роста).

Кроме того, данные причины могут подтолкнуть сотрудника не только к инициативному увольнению, но и к прямому нарушению доверия работодателя – от согласия на вербовку до инициативного доноса или акта прямого саботажа из соображений личной мести. Таким образом, при отсутствии справедливых условий найма и социально ориентированной кадровой стратегии защитить организацию от систематически реализуемых угроз со стороны собственного персонала не сможет ни одна, даже самая мощная и профессиональная, служба безопасности.

Второй предпосылкой эффективной профилактики угроз кадровой безопасности организации выступает внедрение специальных технологий отбора кандидатов на трудоустройство, в которых задействованы служба персонала и служба безопасности. Наряду с традиционной проверкой соответствия профессиональных компетенций кандидата требованиям по замещаемому рабочему месту задачей отбора должен стать заблаговременный отсев лиц, чьи личностные качества, привычки или автобиографические данные делают их потенциально опасными для работодателя.

Профилактика угроз кадровой безопасности обеспечивается также специальным обучением сотрудников, включающим первичное обучение новых сотрудников и повышение квалификации уже имеющегося персонала.

Подобное обучение осуществляется силами специалистов службы безопасности в форме прямого инструктажа и рассылки информационных бюллетеней, а также непосредственно на рабочих местах силами руководителей соответствующих подразделений организации.

Первичное обучение направлено на решение следующих задач:

- ознакомить молодых специалистов с общими понятиями и направлениями обеспечения безопасности предпринимательской деятельности;
- отраслевой спецификой обеспечения корпоративной безопасности;
- дополнительными требованиями в этой области, действующими в конкретной организации;
- правилами служебного и внеслужебного поведения, исключающего возможность их последующего шантажа (для топ-менеджеров – снижающего вероятность реализации угрозы прямых покушений);
- правилами поведения в случае попыток их вербовки, шантажа или угроз.

В результате такого обучения должны быть достигнуты три связанные друг с другом цели:

- обучаемые должны осознать необходимость строгого соблюдения правил обеспечения безопасности, установленных работодателем;
- они должны принять к сведению требование немедленно ставить в известность службу безопасности о любых попытках вербовки, шантажа и

угроз, допущенных в их адрес (при этом до них доводится информация о действующем в организации порядке мотивации подобного поведения и о санкциях к нарушителям);

- обучаемых необходимо убедить в целесообразности инициативного сотрудничества со службой безопасности как залога их собственного служебного, а следовательно, и личного благополучия.

Затем в процессе обучения на рабочих местах новых сотрудников знакомят с правилами:

- работы с конфиденциальной информацией;
- обеспечения безопасности имущественных комплексов работодателя;
- обеспечения информационной и имущественной безопасности в процессе работы с соответствующими клиентами.

Традиционным мероприятием, направленным на профилактику угроз кадровой безопасности, является оперативный контроль над сотрудниками, занимающими рабочие места, наиболее опасные с позиции угроз информационной и имущественной безопасности организации. Объектами контроля со стороны службы безопасности выступают имущественное положение сотрудника, его образ жизни, новые привычки, стиль поведения, психологическое состояние и другие характеристики. Их необъяснимое объективными причинами (например, перевод на высокооплачиваемую должность, получение наследства и т.п.) изменение может сигнализировать о реализованных со стороны этого сотрудника угрозах.

Оперативный контроль может осуществляться как легитимными, так и полуполитимными методами.

К первой группе методов относятся визуальный контроль над соблюдением сотрудниками правил обеспечения информационной и имущественной безопасности работодателя со стороны службы безопасности и непосредственных руководителей, применение в тех же целях технических средств (камеры видеонаблюдения и т.п.), регулярные беседы с психологом службы персонала.

Ко второй группе методов относятся контроль, осуществляемый силами внештатных информаторов службы безопасности, использование скрытых от сотрудников средств видео- и аудиоконтроля, а также просмотр их электронной почты.

3. Третьим условием эффективного функционирования системы управления кадровой безопасностью организации выступает ориентированность системы на *обеспечение приоритетной защиты конфиденциальной информации* и лишь затем иных объектов потенциальных угроз.

Роль информации и информационных технологий в функционировании современной цивилизации, государства, отдельных организаций последовательно увеличивается. Для все большего числа хозяйствующих субъектов утрата или разглашение информации становится более значимой потерей, чем хищение денежных средств и материальных ценностей. Появление и развитие глобальных компьютерных сетей определило появление

еще одного источника постоянных угроз информационной безопасности – несанкционированное проникновение в базы данных. Хакерство из экзотической формы интеллектуальной деятельности ограниченного контингента специалистов по разработке программных средств уже в конце 70-х годов превратилась в новую профессиональную специализацию для работников не только государственных спецслужб, но и частного, в том числе и криминального, бизнеса. Наблюдаемый в последние десятилетия резкий рост как общей номенклатуры угроз информационной безопасности, так и масштаба потерь от них, определяет необходимость реализации данного требования.

Сегодня можно выделить несколько основных категорий конфиденциальной информации (рисунок 21).

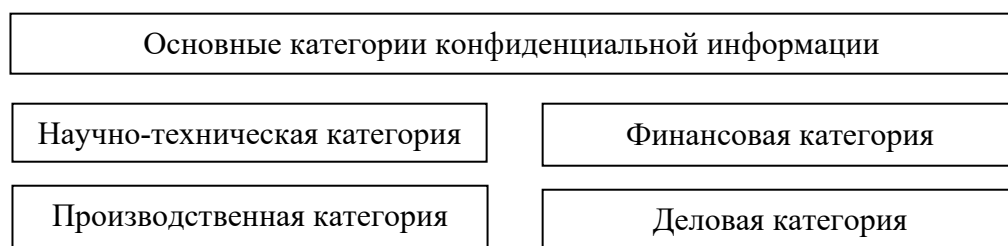


Рис. 21. Основные категории конфиденциальной информации

Научно-техническая категория включает новые идеи, открытия, патенты, оригинальные ноу-хау, современные методики организации в производственной сфере, рационализаторские предложения по внедрению неизвестных ранее и более совершенных технологий, появлению новых типов продукции, уникальные методы анализа конкурентоспособности, коды и пароли, открывающие доступ к конфиденциальной информации, а также уникальное программное обеспечение.

К производственной конфиденциальной информации можно отнести новые технологии в производственной сфере, секретную конструкторскую информацию, схемы и чертежи, данные о материалах, планируемое время выхода товара на рынок, планы выпуска новой продукции, рецептуру изготовления товаров, планы дальнейших вложений в новое производство и так далее.

К конфиденциальной информации финансового характера относится реальный размер прибыли компании, себестоимость производства (или продукции), банковские или торговые сделки, механизм формирования ценовой политики, уровень платежеспособности и так далее.

Что касается группы деловой конфиденциальной информации, то здесь речь идет о следующих данных: условиях заключения договоров с другими участниками рынка, внутренней организационной системе, планировании рекламной компании на ближайшее время, информации о конкурирующих компаниях и поставщиках, данные о работниках компании и переговорном процессе с деловыми партнерами, информации о коммерческой переписке и так далее.

Более подробно об особенностях информационной безопасности организации и методах ее защиты рассмотрено в параграфе 1.1 тема 1.

4. Четвертым условием является *непосредственное участие в обеспечении кадровой безопасности организации всех должностных лиц* в рамках установленной им компетенции и ответственности.

Структура возможных угроз по кадровому направлению деятельности исключает возможность эффективного противодействия им силами исключительно сотрудников службы безопасности. Поэтому важнейшим условием обеспечения безопасности организации выступает воспитание в трудовом коллективе соответствующей идеологии и обучение его членов методам профилактики и пресечения наиболее вероятных угроз.

В таблица 4 (тема 2, параграф 2.2) представлены категории сотрудников, обеспечивающих кадровую безопасность организации.

5. Пятым условием, способствующим эффективному функционированию системы управления кадровой безопасности, выступает *обеспечение взаимодействия системы управления кадровой безопасностью с другими направлениями менеджмента*.

Указанное требование реализуется как на стратегическом, так и на оперативном уровне системы управления. Нарушение его может привести к крайне негативным последствиям. В случае, когда при разработке смежных систем управления (например, финансового менеджмента или маркетинга) будут нарушены требования со стороны рассматриваемой системы, резко увеличивается вероятность негативной реализации соответствующих угроз. В свою очередь, нормальное функционирование смежных систем управления будет постоянно нарушаться, если управление безопасностью будет организовано по принципу самодостаточности – «безопасность ради самой безопасности». Таким образом, комплексная система управления должна формироваться с учетом обеспечения относительного паритета или баланса интересов каждого из направлений деятельности организации.

6. Шестым требованием является *соразмерность затрат на обеспечение кадровой безопасности организации реальному уровню угроз*. Оно связано с реализацией принципа «разумной достаточности». С позиции конечной эффективности системы в равной степени недопустимо экономить на рассматриваемом направлении деятельности, ослабляя собственную безопасность, и преувеличивать возможные угрозы, осуществляя излишние, т.е. некупаемые расходы. Учитывая, что руководство службы безопасности по очевидным причинам склонно именно к завышению уровня потенциальных угроз, для соблюдения данного требования желательно привлечение независимых экспертов в лице сотрудников государственных правоохранительных органов или частных охранных структур.

7. Следующее условие – *формализованное закрепление не только функциональных обязанностей, но и полномочий (предела компетенции) службы безопасности*. В отличие от других направлений деятельности организации, работа большинства сотрудников этого подразделения всегда связана с угрозой превышения служебных полномочий. В результате велика

вероятность возбуждения против организации уголовных дел и гражданских исков по обвинению в нарушении действующего законодательства или гражданских прав.

Как отмечалось выше, одной из основных функций службы безопасности является сбор и обобщение информации как о кандидатах, так и о работающих на предприятии сотрудниках. Ключевым моментом является получение от кандидата до начала проверки его личности согласия на обработку персональных данных, поскольку в Федеральном законе «О персональных данных» четко сказано, что персональные данные могут обрабатываться, храниться и передаваться третьим лицам только с согласия их носителя. Нарушение данной нормы грозит организации штрафными санкциями.

Вторым важным моментом в деятельности службы безопасности является хранение персональных данных. В связи с этим в каждой организации обязательно наличие внутреннего локального нормативного акта, регулирующего порядок использования и хранения персональных данных. В целях предания законности действиям представителей безопасности при проведении проверок, в указанном положении необходимо определить перечень должностных лиц предприятия, имеющих право доступа и работы с персональными данными, включив в них и специалистов сектора безопасности.

Однако сотрудники службы безопасности должны уделять внимание не только первичной проверке кандидатов (на судимость, наличие долговых обязательств и т.п.), но и непосредственной их деятельности после приёма на работу: на постоянной основе отслеживать и контролировать взаимоотношения в коллективе, кадровые перестановки, изменение штатной структуры, для чего необходимо плотное взаимодействие с кадровыми службами, лицами, отвечающими за движение штата работников.

Данное взаимодействие должно существовать не только на словах, но и быть зафиксировано в локальных нормативных актах, при этом, учитывая, что подразделения безопасности привлекаются для разрешения возникающих внутрикорпоративных споров, их полномочия должны быть максимальны, а взаимодействие со всеми смежными подразделениями прозрачным и максимально оперативным.

Служба безопасности должна координировать подбор персонала в области противодействия формирования этнических групп, потому что они могут стать катализатором возникновения рисков злоупотребления полномочиями, что в конечном итоге может привести не только к внутрикорпоративным конфликтам между работниками, но и к принуждению к увольнению более компетентных сотрудников и заменой их менее профессиональными лицами, принадлежащими к данной этнической группе.

Кроме того, отношения между работниками, не ограничивающимися деловым сотрудничеством, существенно увеличивают риск совершения ими противоправных деяний, ведь, имея устойчивые связи им легче вступить во внутрикорпоративный сговор. В этой связи сотрудники службы безопасности должны курировать работу кадровых служб, отслеживая назначения вновь принимаемых работников, и принимать активное участие в распределении

персонала. Данный подход позволяет существенно улучшить работоспособность персонала организации и своевременно осуществлять профилактику возникновения рисков.

Нередко возникает потребность в сборе сведений о частной жизни сотрудника, наличии у него и его родственников собственности. Такие данные позволяют понять, соответствует ли доход работника его реальным тратам, соблюдает ли он антикоррупционную политику организации, надёжен ли он. Но следует помнить, что представители сектора безопасности не имеют права проводить оперативно-розыскные мероприятия, и в случае отсутствия согласия со стороны работника на сбор таких сведений данные действия подпадают под действие статьи 137 Уголовного кодекса Российской Федерации (нарушение неприкосновенности частной жизни). Решить эту проблему служба безопасности может, организовав контроль над деятельностью работников путём введения градации должностей, определения степени рисков для каждой из них и разработки частоты и глубины проведения проверок.

8. Использование всего спектра *методов обеспечения кадровой безопасности* организации, которые способствуют повышению благонадежности и предупреждению нелояльности работников организации, – еще одно обязательное условие. К ним относят административные, социально-экономические и социально-психологические.

Среди административных методов выделяют:

- проведение всестороннего отбора кадров, при котором не допускается прием на работу лиц, имеющих деструктивную направленность личности, социальные связи, порочащие их; биографию, свидетельствующую о наличии у них морально-нравственных дефектов;
- проведение периодической оценки степени защищенности жизненно важных интересов работников, особенно тех из них, кто занимает должности с повышенным уровнем риска кадровой безопасности;
- информирование персонала о том, какое наказание может следовать в случае нарушения конкретных норм дисциплины (выговор, лишение премии, понижение в должности, лишение определенных льгот, увольнение и др.);
- обучение персонала правилам и нормам обеспечения безопасности;
- обеспечение эффективного контроля над деятельностью персонала;
- формирование локальной нормативно-правовой базы обеспечения кадровой безопасности организации, которая предусматривает разработку и утверждение норм и правил поведения, в том числе этических, обязательных для соблюдения: правила внутреннего трудового распорядка, трудовые договоры, договоры о материальной ответственности, договоры о неразглашении конфиденциальной информации, коммерческой тайны, персональных данных, регламенты использования средств коммуникации и доступа в Интернет и пр., этический кодекс;
- безопасное увольнение работников за грубые нарушения правил и норм кадровой безопасности.

К основным социально-экономическим методам можно отнести:

– создание условий, при которых работнику будет невыгодно осуществлять действия, наносящие ущерб организации;

– введение системы материального и иных видов стимулирования, дополнительно «привязывающих» работника к компании, которые он не сможет получить в конкурирующих организациях (вручение премий, ценных подарков или иных наград, туристических путевок и др.);

– предупреждение ситуаций, при которых работник или близкие ему люди могут оказаться в безвыходном или критическом положении при возникновении острых жизненных проблем (в частности, кредитование работников, создание кассы взаимопомощи и др.).

Социально-психологические методы включают в себя:

– формирование корпоративного духа, включая принятие мер по созданию у работников чувства принадлежности к организации, сплоченности коллектива, по созданию такого социально-психологического климата, который способствовал бы восприятию организации как референтной для каждого работника, а также препятствующего действиям и поступкам, направленным на причинение ущерба организации;

– формирование в организации такого стиля работы руководителей любого ранга, который не будет жестко авторитарным, не станет приводить к унижению, задевать чувство собственного достоинства подчиненных, с тем чтобы не провоцировать обратную негативную реакцию.

Стоит отметить, что методы обеспечения кадровой безопасности должны конкретизироваться с учетом индивидуально-личностных характеристик персонала, быть нацелены на восприятие каждого конкретного работника как потенциального субъекта угроз безопасности организации.

Контрольные вопросы и задания

1. Требования и принципы, оказывающие влияние на систему кадровой безопасности.

2. Охарактеризуйте стратегии управления кадровой безопасностью и операционные подсистемы системы управления кадровой безопасностью организации.

3. Дайте характеристику блока обеспечения структуры системы управления кадровой безопасностью организации.

4. Критерии эффективности системы управления кадровой безопасностью и этапы ее реализации.

5. Охарактеризуйте причины, вследствие которых сотрудники становятся источником угроз корпоративной безопасности.

6. Внешние и внутренние субъекты обеспечения кадровой безопасности.

7. Задачи и функции службы управления персоналом в аспекте управления кадровой безопасностью организации.

8. Задачи и функции службы безопасности в аспекте управления кадровой безопасностью организации.

9. Охарактеризуйте условия эффективного функционирования системы управления кадровой безопасностью организации.

10. Раскройте методы обеспечения кадровой безопасности организации.

Задания для самостоятельной работы

1. На примере какого-либо государственного органа проведите оценку и анализ используемых в ней стратегий управления. Определите кадровые возможные риски и угрозы, с ними связанные, и на этой основе разработайте план мероприятий по повышению кадровой безопасности организации.

2. На примере какого-либо государственного органа соотнесите между собой используемые в нем стратегии управления с типом кадровой политики. Определите возможные кадровые риски и угрозы и на этой основе разработайте план мероприятий по обеспечению кадровой безопасности организации.

Тестовые задания

1. Система кадровой безопасности требует такого построения, при котором она могла бы различать на начальных этапах всевозможные отклонения в деятельности организации, участвовать в процессе устранения их отрицательного влияния и, как следствие, причинения вреда организации – это

- А) принцип целостности
- Б) принцип надежности
- В) принцип срочности
- Г) принцип правомерности
- Д) принцип экономичности
- Е) принцип согласованности
- Ж) принцип открытости и приватности
- З) принцип профессионализма

2. Для сохранения защищенности организации в кадровой сфере все субъекты этого процесса должны взаимодействовать друг с другом, точно знать свои обязанности и полномочия – это

- А) принцип целостности
- Б) принцип надежности
- В) принцип срочности
- Г) принцип правомерности
- Д) принцип экономичности
- Е) принцип согласованности
- Ж) принцип открытости и приватности
- З) принцип профессионализма

3. Вопросами обеспечения кадровой безопасности должны заниматься не любители, а компетентные специалисты, умеющие вовремя дать оценку ситуации и принять верное решение – это

- А) принцип целостности
- Б) принцип надежности

- В) принцип срочности
- Г) принцип правомерности
- Д) принцип экономичности
- Е) принцип согласованности
- Ж) принцип открытости и приватности
- З) принцип профессионализма

4. Принцип приоритета профилактических методов противодействия возможным угрозам – это...

- А) стратегия упреждающего противодействия угрозам
- Б) стратегия пассивной защиты от угроз
- В) стратегия адекватного ответа на угрозы

5. Приоритетная ориентация на защиту со стороны государства в лице правоохранительных и судебных органов – это принцип

- А) стратегии упреждающего противодействия угрозам
- Б) стратегии пассивной защиты от угроз
- В) стратегии адекватного ответа на угрозы

6. Совокупность прикладных методов управления, используемых в рамках системы – это...

- А) информационное обеспечение
- Б) нормативно-методическое обеспечение
- В) технологическое обеспечение
- Г) инструментальное обеспечение
- Д) кадровое обеспечение
- Е) финансовое обеспечение

7. Совокупность формализованных технологий обеспечения безопасности организации от различных видов кадровых угроз – это...

- А) информационное обеспечение
- Б) нормативно-методическое обеспечение
- В) технологическое обеспечение
- Г) инструментальное обеспечение
- Д) кадровое обеспечение
- Е) финансовое обеспечение

8. Является ли следующее утверждение верным?

Подсистема контроля дает основания для корректировки выполнения любого из этапов управления кадровой безопасностью организации

9. _____причины, вследствие которых сотрудник становится источником угроз корпоративной безопасности хозяйствующего субъекта, обусловленные экономической направленностью кадровой политики хозяйствующего субъекта, игнорирующей социальные потребности сотрудников организации

- А) политико-идеологические
- Б) социально-экономические

- В) психологические
- Г) моральные
- Д) национальные
- Е) физиологические
- Ж) стратегические
- З) профессиональные
- И) финансовые

10. Информационно-аналитический отдел – это отдел

А) выполняющий функции «мозгового центра», в который стекается и анализируется вся информация об ее деятельности, а также формируются рекомендации для руководства и других подразделений организации

Б) деятельность которого направлена на защиту любой конфиденциальной информации банка

В) деятельность которого направлена на защиту имущества и персонала организации и включающий в себя службу телохранителей и патрульно-постовую службу

Г) обеспечивающий защиту от угроз со стороны некомпетентных или нелояльных работников самой службы безопасности

11. Является ли следующее утверждение верным?

Главным условием эффективного функционирования системы управления кадровой безопасностью организации является приоритет мероприятий по предотвращению потенциальных угроз

3. ТЕХНОЛОГИЯ ОБЕСПЕЧЕНИЯ КАДРОВОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

3.1. Обеспечение кадровой безопасности при найме и увольнении персонала

Кадровая безопасность зависит от трех основных факторов:

1 **Найм.** Под наймом понимается комплекс мер безопасности при приеме на работу и прогнозирование благонадежности сотрудников. В это понятие входит рассмотрение вопросов безопасности компании на таких этапах в работе менеджера по персоналу, как поиск кандидатов, процедуры отбора, документальное и юридическое обеспечение приема на работу, испытательный срок и даже адаптация. Сюда же можно отнести процедуры безопасности при подготовке аттестации, планировании обучения и увольнении работников.

2 **Лояльность.** Это комплекс мер по установлению позитивных отношений работников к работодателям. От того, кем ощущает себя сотрудник предприятия, – частью общего дела или «винтиком» – зависят и проблемы организации.

3 **Контроль.** Он представляет собой комплекс мер из установленных для персонала, в том числе для администрации, регламентов, ограничений, режимов, технологических процессов, оценочных, контрольных и других операций, процедур безопасности. Контроль непосредственно нацелен на ликвидацию возможностей причинения ущерба и отрабатывается, как правило, службой безопасности или другими подразделениями, но в меньшей степени службой персонала.

Таким образом, комплексная работа по обеспечению кадровой безопасности организации может быть разделена на три основных этапа:

- деятельность на этапе проверки кандидата и приема его на работу;
- мероприятия на этапе осуществления работником своей основной профессиональной деятельности;
- обеспечение корпоративной безопасности на этапе увольнения работника.

Специально вопрос безопасности организации часто не выходит на первый план. Это, как правило, не главная задача при найме. Но при этом следует понимать, что ошибки в отборе новых работников чреваты угрозой безопасности компании из-за приема на работу человека, который умышленно или неумышленно способен нанести вред компании в той или иной области.

Безопасность с точки зрения организации предполагает целый ряд аспектов.

1) стремление защитить компанию от проникновения людей, имеющих связи с криминальными структурами;

2) стремление поставить барьер перед людьми, склонными к воровству; при этом чем выше должность, которую может занять такой человек, тем больший экономический ущерб он может нанести компании, которая возьмет его на работу;

3) проверка работника на склонность к злоупотреблению алкоголем и употреблению наркотиков;

4) обеспечение информационной безопасности компании: защита секретов производства (ноу-хау), защита баз данных, результатов маркетинговых исследований, планов, связанных с заключением договоров с другими компаниями, и другой информации, важной для сохранения ее конкурентоспособности;

5) соответствие работника требованиям организационной культуры («наш» человек или «не наш»).

Последний аспект безопасности при отборе новых работников часто недооценивается, хотя понятно, что и один человек, придерживающийся разрушительных или деструктивных установок, может нанести очень большой вред организации, выражающийся в ухудшении морально-психологического климата, склоках, конфликтах, ухудшении трудовой и исполнительской дисциплины и пр.

Наиболее значимыми мероприятиями в обеспечении кадровой безопасности компании при найме являются организация подбора и отбора кандидатов на вакантные должности.

Подбор персонала – это комплекс мер, направленных на выявление целого ряда знаний о кандидате: его профессиональных навыках, умениях, потенциале в зависимости от целей и задач организации, его психологическом портрете и других немаловажных факторах.

Подбор персонала требует от сотрудника кадровой службы высокой профессиональной квалификации, точного знания потребностей компании, знания специфики конкретной должности, а также личных черт характера и умений. Ошибка в выборе может стоить компании слишком дорого.

При правильном подходе строится план по подбору персонала, который состоит из следующих ключевых принципов:

- анализа действующих сотрудников, их численности и компетенций, перспектив развития;

- анализа перспективных потребностей в области поиска и найма новых сотрудников;

- анализа способов решения перспективных задач: поиска, найма, обучения и продвижения персонала.

Поиск персонала обычно происходит в двух направлениях: использование внутренних резервов компании и привлечение соискателя извне. Нельзя отдавать предпочтение лишь одному из вариантов поиска, т.к. он сужает круг возможных претендентов. В каждом из них есть свои плюсы и минусы. При использовании внутренних резервов предложение делается сотруднику, который уже известен компании. Но в этом случае, если речь идет о повышении в должности, возможно возникновение внутренних конфликтов в коллективе. Принимая кандидата со стороны, никогда до конца нельзя быть уверенным в его профессионализме и личных качествах. Но использование ресурсов извне расширяет круг поиска: это могут быть специализированные

сайты по подбору персонала, кадровые агентства, профильные вузы, ярмарки вакансий и т.п.

Существует ряд подходов, позволяющих решать проблемы безопасности при подборе и отборе сотрудников (рисунок 22).

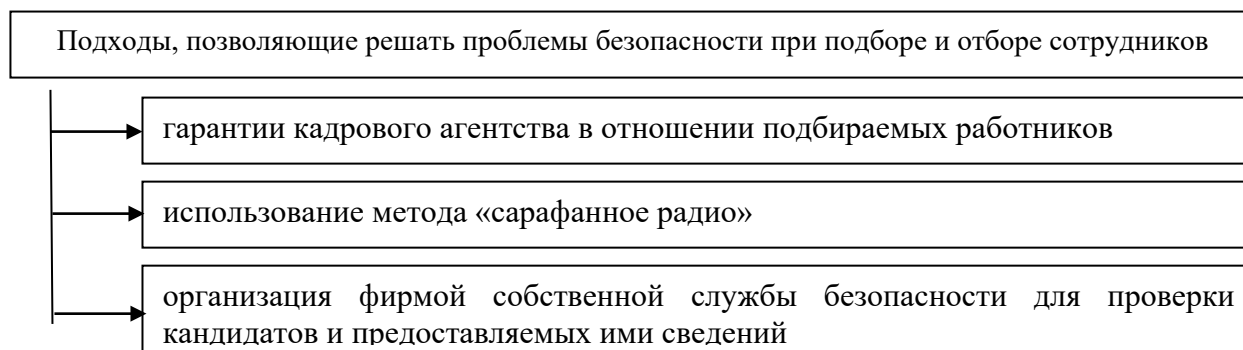


Рис. 22. Подходы, позволяющие решать проблемы безопасности при подборе и отборе сотрудников

Первый вид обеспечения безопасного подбора кадров – гарантии кадрового агентства в отношении подбираемых работников. Эту гарантию агентство может дать не только на основании того, что методы отбора и проверки данных, представленных кандидатами, дают такую уверенность, но и потому, что многие агентства достаточно давно работают с людьми, включенными в их базу данных.

Второй подход – это использование метода «сарафанное радио». Этот способ гарантирует наличие максимально полной информации о новом сотруднике. Кроме того, предполагается, что люди, рекомендовавшие сотрудника, несут за него персональную ответственность, и с них всегда можно спросить за промахи или ошибки новичков.

Третьим подходом является организация фирмой собственной службы безопасности для проверки кандидатов и предоставляемых ими сведений. Например, в банках такая служба обязательна, в ней, как правило, работают бывшие сотрудники силовых структур, обладающие соответствующими связями и возможностями. При проверке кандидатов служба безопасности может действовать параллельно с кадровой службой. Она проверяет работника на отсутствие судимостей, отсутствие связи с криминальными структурами, отсутствие претензий предыдущих работодателей с точки зрения его честности и надежности. Проверка кандидата при приеме на работу может предполагать выяснение того, попадал ли этот человек в ДТП, можно ли ему доверить автомобиль фирмы? В некоторых организациях работнику даже могут предложить принести справку, подтверждающую, что у него нет никаких проблем с правоохранительными органами.

На стадии **отбора** решаются два основных вопроса: отсев заведомо непригодных работников и оценка личных и профессиональных качеств принятых на работу. Чтобы избежать кадровых рисков и угроз безопасности организации, на этом этапе следует особо внимательно изучать, анализировать

и проверять полученную от соискателя информацию о себе, своих профессиональных навыках, знаниях, социальном статусе, психологическом портрете.

Также необходимо выявить принадлежность или склонность соискателя к одной из групп риска. В список «опасных» кандидатов включаются люди, чья работа в организации или их последующее увольнение может вызвать различные проблемы. Ни в одной организации, ни в какой должности (от линейной до ведущей, от исполнительской до управляющей) нежелательно присутствие в коллективе сотрудника, который может потенциально попасть или уже находится в группе риска. К ней относят людей, имеющих следующие проблемы:

- аффилированность, склонность к коррупции;
- наркоманию и токсикоманию;
- игроманию (в том числе сегодня это компьютерные игры);
- принадлежность к неформальным религиозным сообществам;
- тяжелое социально-экономическое положение;
- трудовую зависимость;
- зависимость от людей, предметов, явлений.

Работа с кандидатом на этапе отбора требует от сотрудника кадровой службы высокой квалификации, внимания, должной психологической подготовки. Именно этот этап призван произвести не только профессиональный отсев кандидатов, но и исключить потенциально нежелательных для кадровой безопасности соискателей.

Анализ действующего законодательства и практики его применения позволяют выделить следующие группы источников формирования значимой информации:

- 1) документы и сведения, предоставленные работником;
- 2) данные собеседования, анкетирования, тестирования;
- 3) иные источники (сведения, полученные из органов власти и управления, компрометирующие материалы, опубликованные в средствах массовой информации, слухи и т.п.).

Иногда при рассмотрении вопроса сбора и проверки сведений о кандидате рекомендуют в качестве источника получения информации использовать данные правоохранительных органов. В этой службе персонала помогает взаимодействие со службой безопасности, которое должно быть тесным, постоянным и взаимодополняющим. Такое взаимодействие чаще всего проявляется в организации регулярных и достаточно «глубоких» проверок кандидатов. Приведем примеры распространенных проверочных мероприятий:

- проверка по «полицейским» учетам – судимости, существенные административные взыскания, утерянные паспорта, наличие розыскных дел;
- проверка рекомендаций с мест предыдущей работы через службы безопасности компаний или легендированно (при запросе информации не указываются название организации, должность проверяющего и причины проверки);
- проверка регистрации по месту жительства (пребывания);

- проверка кредитной истории через службы безопасности или кредитные отделы банков;
- проверка на наличие связей в криминальной среде (в том числе связей через родственников и членов семьи);
- проверка наличия недвижимого и движимого имущества (в том числе на соответствие заявленному);
- проверка участия в капитале (учреждение, акционирование и т.д.) организаций – юридических лиц;
- проверка участия (учреждение, попечительство) в некоммерческих организациях – фондах, обществах, ассоциациях, общественных организациях;
- проверка предоставляемых документов (диплом, паспорт) на подлинность и т.д.

В современных отечественных условиях вероятность фальсификации документов очень велика вследствие:

- а) наличия в свободной продаже бланков трудовых книжек, дипломов, других документов, которые ранее являлись объектом строгой отчетности;
- б) возможности заказать любые печати и штампы у частного мастера;
- в) активного предложения поддельных дипломов и аттестатов.

Для решения поставленной выше задачи используются два типа технологий, основанных на криминалистической экспертизе документов и оперативных контрольных мероприятиях.

Для выявления прямых подделок эксперт службы безопасности анализирует соответствие документов установленным формам, устанавливает наличие необходимых реквизитов, проверяет четкость оттисков печатей и штампов, отсутствие разночтений, а также подчисток, исправлений, дописок, правлений. Особое внимание уделяется соответствию подписей должностных лиц, отсутствию извилистости, угловатости, сдвоенности штрихов, вдавленных бесцветных штрихов и т.п.

К оперативным мероприятиям относятся также проверка подлинности документов путем запросов по месту профессионального обучения кандидата и его прежней работы. При отсутствии у службы безопасности банка собственных экспертов указанные технологии могут быть реализованы сторонними для него структурами – криминалистическими лабораториями при территориальных органах МВД и частными детективными агентствами.

Наиболее сложные технологии используются для выявления потенциально опасных для работодателя личностных качеств кандидата. Здесь основная нагрузка ложится на психолога службы персонала или самой службы безопасности. Любой кандидат обычно хорошо представляет, какие личные качества могут скомпрометировать его в глазах потенциального работодателя. Поэтому он будет тщательно скрывать их при написании резюме и в процессе интервью. Это определяет необходимость использования специальных психотехнических технологий, например:

- специальных методик тестирования, разработанных для выявления скрываемых человеком личностных качеств;

- анализа психологом видеозаписей интервью с кандидатом, его фотографий, сделанных в разной обстановке;
- психографической экспертизы образцов почерка.

Эти технологии позволяют выявить как психотип, так и большинство реальных личностных качеств человека. К сожалению, две последние технологии в России, в отличие от многих зарубежных стран, применяются редко.

Результаты проверок, проведенных службой безопасности, в документированной форме представляются сотрудникам службы персонала и учитываются при принятии решения о приеме кандидата на работу.

Задача службы персонала, осуществляющей оценку кандидатов при приеме на работу, состоит в том, чтобы выбрать такого работника, который в состоянии достичь ожидаемого организацией результата. Фактически оценка при приеме – это одна из форм предварительного контроля качества человеческих ресурсов организации.

Целью описываемого мероприятия являются:

- выявление склонности кандидата к мошенничеству;
- выявление связей и фактов биографии, способных навредить компании;
- выявление профессиональной пригодности кандидата;
- получение информации о его особенностях.

Итак, комплексная проверка соискателя вакантной должности должна включать в себя следующее:

1) сбор официальной информации и формальные проверки:

- заполнение специально составленной анкеты;
- предоставление копии паспорта, трудовой книжки, военного билета, документов об образовании, водительского удостоверения и т.п. и проверка их на подлинность;
- получение информации из баз данных;
- получение отзывов с предыдущих мест работы по официальным каналам;
- тестирование кандидата, включающее открытое и скрытое психологическое тестирование, косвенное (через косвенные проявления психических особенностей) и замаскированное тестирование (под видом анкетирования);
- проверка на детекторе лжи;

2) ряд собеседований:

- первое собеседование проводит кадровик и в процессе беседы уточняет полученные из документов данные, также получает общее представление о кандидате;
- второе собеседование также проводит кадровик, устраняя разногласия между предоставленной информацией и информацией, полученной из других источников, кроме этого задаются проблемные вопросы для выяснения профпригодности и отношения к определенным фактам, событиям и подобному; при этом желательно проводить скрытое и явное психологическое тестирование кандидата;

- третье собеседование проводит руководитель, имея на руках результаты предыдущих собеседований и проверок, ставятся конкретные проблемы и выясняются знания и профессионализм;

- скрытые собеседования проводятся вне пределов фирмы под видом подбора сотрудника на сходную должность, но в другую компанию, естественно, их проводят подставные лица;

3) сбор субъективной информации и неформальные проверки:

- неформальное общение (опрос) с бывшими сослуживцами, подчиненными, соседями;

- создание искусственных ситуаций (провокации) и наблюдение за тем, как человек реагирует, как ведет себя;

- наблюдение за поведением в стандартных ситуациях и сопоставление с декларируемыми идеями и принципами;

- сопоставление всей полученной информации и принятие решения о пригодности кандидата.

Для эффективной организации труда служб подбора и кадровой безопасности, их совместного эффективного взаимодействия в рамках одного и того же процесса подбора и отбора кадров необходимо разграничить сферы деятельности и закрепить за каждой из сторон свой специфичный функционал.

Служба безопасности выполняет следующие функции:

- организация служебного расследования;

- планирование мероприятий по диагностике и разоблачению выявленных угроз;

- специальное обучение собственных сотрудников и работников других подразделений по выполнению ими соответствующих действий для сохранения правопорядка;

- выполнение целевых запросов в организации (налоговые, миграционные службы, психоневрологический диспансер, изучение кредитных историй и т.п.);

- проверка подлинности документов (паспорта, трудовой книжки); сбор характеристик с прошлых мест работы для проверки трудовых историй (конфликтности), финансовой стабильности (благонадежности), возможно, данные о родственниках, если есть в этом острая необходимость (смотря на какую должность претендует соискатель).

Служба работы с персоналом организации реализует функции по подбору, обеспечению развития и мотивации, формированию лояльности сотрудников, высокого уровня ответственности за эффективную и инициативную работу на местах; функциональную и профессиональную мобильность, профессиональную грамотность.

Если анализировать методы воздействия на персонал, то в службах безопасности они распределяются по следующим направлениям: методы диагностики угроз кадровой безопасности, как со стороны внешних, так и внутренних факторов воздействия, и методы, противостоящие потенциальной и/или реальной кадровой угрозе для организации.

Классификация методов диагностики кадровой безопасности представлены на рисунке 23.

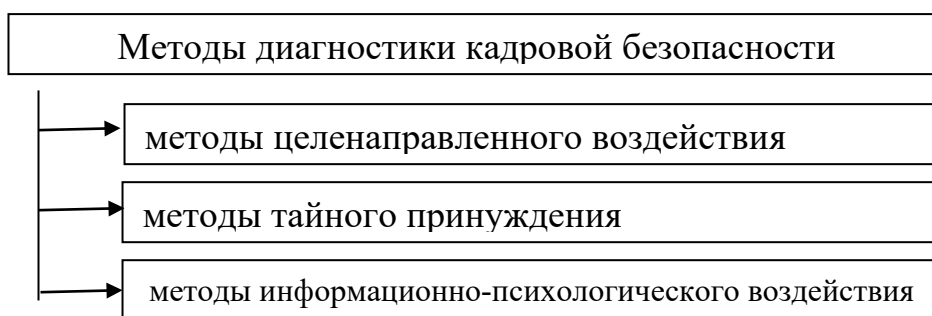


Рис. 23. Методы диагностики кадровой безопасности

К методам целенаправленного воздействия относят пресечение мошенничества, рейдерского захвата, предотвращение коррупционной деятельности в организации и др.

Методы тайного принуждения включают конкурентную разведку, вербовку работников, различного рода манипуляции, в том числе использование нейролингвистического программирования, промышленный шпионаж и др.

Среди методов информационно-психологического воздействия выделяют:

- нарушение прав работников на рабочем месте, дискриминации (по половозрастному признаку, в отношении людей с ограниченными физическими возможностями, больных СПИДОМ, людей, ведущих нездоровый образ жизни);

- психическое насилие: моббинг, буллинг, харасмент, распространение слухов, сплетен, провокаций; утечка / похищение информации; несанкционированные сбор, хранение, обработка, использование персональных данных сотрудников, передача их третьим лицам, и др.

Методы, противостоящие потенциальной и/или реальной кадровой угрозе, классифицируются как профилактические, пресекающие или отражающие и карающие; это могут быть методы легитимного и нелегитимного характера, откровенно криминальные (вербовка, шантаж, взятки).

Перечисленные выше методы воздействия на персонал позволяют диагностировать или противостоять угрозам кадровой безопасности. Они совершенно отличаются от методов работы специалистов кадровых служб. Специалисты этих структур работают параллельно в достижении единой цели, в нашем случае – это заполнение вакантных позиций достойными кандидатами. Однако следует понимать, что смешивать, и, тем более, подменять или дублировать действия этих двух служб совершенно неправомерно. Через применение различных форм и методов работы, разделяя сферы деятельности служб, возможен более полный и качественный сбор необходимой информации по претенденту, позволяющей гарантированно предохранять организацию от возможных кадровых упущений в работе и угроз кадровой безопасности организации.

В настоящее время активно стали применяться и не очень законные методы отбора персонала: *executive search* («переманивание» лиц, принимающих решение), *talent poaching* («кадровое браконьерство»), *talent raiding* («захват талантов»), «партизанский» рекрутинг.

Нетрудно заметить, что методы самые разнообразные и очень специфичные. В силу этого, объективно приходится разграничивать функции HR-структур, которые в большей степени связаны с оценкой деловых и профессиональных качеств кандидатов, от функций служб безопасности.

В процессе оформления приема на работу в иерархии средств предотвращения потерь, кадровой безопасности, на первое место ставится правовое обеспечение деятельности службы управления персоналом. Следует признать, что только юридически грамотные документы и действия способны эффективно и без лишних затрат основать безопасные отношения с персоналом. И это основной принцип «безопасного» найма, то есть такой процедуры, которая способна уберечь компанию от потенциальных негативных последствий правового характера.

Так, при приеме на работу следует особое внимание стоит уделить записям в трудовой книжке. Так, например, запись о расторжении трудового договора по п. 1 ч. 1 ст. 77 ТК РФ (по соглашению сторон) может служить сигналом, что с недобросовестным сотрудником «мирно» расстаются, а с другой стороны, это может быть скрытая форма увольнения «по сокращению штата». Запись о расторжении трудового договора по п. 5 ч. 1 ст. 81 ТК РФ может говорить о низкой дисциплине работника, а с другой стороны, о том, что от данного работника решили избавиться по той или иной причине.

Регламентация закрепления взаимных прав и обязанностей сторон определяется Трудовым Кодексом.

Для снижения рисков, связанных с работой, перед приемом на работу до подписания трудового договора кандидат должен быть ознакомлен с утвержденными локальными нормативными актами организации (Положением о структурном подразделении и должностной инструкцией, Положением о коммерческой тайне, Правилами по охране труда и т.д.), регламентирующими его работу.

Одним из основных документов, с точки зрения кадровой безопасности, является *трудовой договор*. Он должен содержать целый ряд статей, изначально устанавливающих для сотрудника рамки лояльного отношения к работодателю, его собственности и безопасности в целом. С этой целью в тексте трудового договора, как правило, в раздел «Обязанности работника», могут вводиться следующие элементы, имеющие непосредственное отношение к безопасности:

«Работник обязуется:...

- при приеме на работу предъявить работодателю все необходимые документы и заполнить соответствующие учетные формы;
- соблюдать трудовую дисциплину и выполнять установленные нормы труда;

- соблюдать требования по охране труда и обеспечению безопасности труда;
- соблюдать действующие в организации Правила внутреннего трудового распорядка, а также приказы и распоряжения руководства подразделения и администрации организации;
- выполнять правила обеспечения сохранности и неразглашения конфиденциальной информации в соответствии с Положением о конфиденциальной информации организации и иными внутренними нормативными актами;
- в течение одной недели сообщать работодателю об изменениях анкетных и иных учетных данных о себе;
- заключить с работодателем договор о полной коллективной (индивидуальной) материальной ответственности;
- бережно относиться к ценностям и принимать меры к предотвращению ущерба, обеспечивать сохранность товарно-материальных ценностей и денежных средств, переданных ему для хранения или других целей;
- незамедлительно сообщать работодателю (непосредственному руководителю) о возникновении ситуации, представляющей угрозу жизни и здоровью людей, а также сохранности имущества работодателя и других работников...».

Юридические формулировки могут быть иными, однако суть должна точно отражать желаемое поведение работника. И, несмотря на то, что сами трудовые договора для различных сфер деятельности организации (интеллектуальной и материальной), разных категорий сотрудников и уровней управления составляются по разным макетам, установление рамок безопасности в них должно быть очевидным.

Правила внутреннего трудового распорядка. Статья 15 Трудового Кодекса РФ гласит: «Трудовые отношения – отношения, основанные на соглашении между работником и работодателем о личном выполнении работником за плату трудовой функции (работы по определенной специальности, квалификации или должности), подчинении работника правилам внутреннего трудового распорядка при обеспечении работодателем условий труда, предусмотренных трудовым законодательством, коллективным договором, соглашениями, трудовым договором». Из нее следует, что в организации необходимо наличие письменного свода Правил внутреннего трудового распорядка.

Правила внутреннего трудового распорядка – локальный нормативный акт, определяющий не только трудовой распорядок и регламентирующий основные вопросы трудовых отношений в организации, но и являющийся одним из основных документов, устанавливающих процедуры безопасности.

Кроме всего прочего, в текст этого документа включаются различные процедуры и правила, например:

- о пропускном и внутриобъектовом режиме;
- о пожарной безопасности;
- о медицинском обеспечении деятельности и санитарных правилах;

- о материальной ответственности;
- об информационном взаимодействии с администрацией;
- об этике отношений сторон (недопущении конфликта интересов);
- о контроле за совместной работой родственников;
- о процедуре расчета и увольнения и т.д.

Должностная инструкция – документ, детально регламентирующий работу сотрудника на той или иной должности, либо на том или ином рабочем месте. В нем прописаны действия, за неисполнение либо халатное исполнение которых предусмотрены различные виды ответственности.

С должностной инструкцией работник должен быть ознакомлен под роспись.

Обязательство сотрудника о неразглашении конфиденциальной информации. Трудовой кодекс РФ и Гражданский кодекс РФ, а также федеральные законы «Об информации, информационных технологиях и защите информации», «О коммерческой тайне» дают работодателям право требовать от своих работников обеспечения сохранности конфиденциальной информации.

Подписывая данный документ, работник обязуется:

- не раскрывать конфиденциальную информацию какому-либо лицу или организации, за исключением случаев выполнения своих трудовых обязанностей и с прямого указания руководства;
- не использовать, прямо или косвенно, конфиденциальную информацию иначе, чем в интересах организации в целях выполнения своих обязанностей сотрудника и с прямого указания руководства;
- подчиняться правилам организации и указаниям ее должностных лиц, направленным на защиту и сохранение конфиденциальной информации.

В случае прекращения работы в организации и независимо от причин увольнения работник, до осуществления окончательного расчета, должен вернуть все находящиеся в его распоряжении документы, информацию и другие материалы, связанные с деятельностью организации и закрепленные на любых носителях, включая программные продукты.

Кроме того, он обязан оказывать всемерное содействие руководству и службе безопасности в выявлении, предупреждении и пресечении возможных фактов утечки и хищения конфиденциальной информации.

В случае нарушения работником условий данного Обязательства организация имеет право наложить на него дисциплинарное взыскание вплоть до увольнения и возместить понесенные в результате нарушения убытки за счет работника в порядке и размере, оговоренном действующими в организации нормативными актами.

Однако документы указанного характера должны применяться не столько в надежде на санкции, сколько для достижения трех эффектов:

- образовательного (работник узнает о существовании этих правил, ограничений и запретов);
- этического (соблюдение этики отношений «работник-работодатель»);
- профилактического (эффект ожидания санкций).

Итак, эффективные подбор и отбор персонала способствуют усилению безопасности организации.

Угрозы кадровой безопасности организации возникают и при *увольнении* сотрудника.

В ТК РФ четко прописана процедура выхода сотрудника из компании. Однако, если сама процедура была некорректной, компания может понести значительный моральный и материальный ущерб. Моральный ущерб может быть нанесен через антирекламу организации, а материальный – в случае обращения уволенного сотрудника в суд. Юридическая практика показывает, что лучше не доводить трудовые споры до суда, так как финансовые издержки в любом случае лягут на работодателя.

В процессе расторжения трудовых отношений с работником могут возникать деструктивные конфликты. Здесь речь может идти как о преднамеренном увольнении сотрудника по его собственному желанию – с целью причинения ущерба компании, так и об увольнении по инициативе руководства. Однако обе эти ситуации создают предпосылки к возникновению деструктивных конфликтов в организации. Подобную ситуацию гораздо легче предупредить специалистам службы безопасности и службы управления персоналом, чем потом тратить время и ресурсы на поиск позитивных решений, которые для компании не всегда могут быть приемлемыми.

Значительные проблемы могут возникнуть в организации, когда при увольнении сотрудник не передал информацию, а вновь принятый на эту должность работник не имеет опыта работы в этом направлении. В этом случае негативные последствия могут коснуться не только какого-либо подразделения компании, но всей организации в целом (потеря клиентской базы и т.д.).

Следовательно, особый контроль должен осуществляться при увольнении персонала, имеющего отношение к информации компании. Значительный урон организации может быть нанесен, если уволенный или уволившийся сотрудник забирает с собой максимум информации через клиентскую базу и налаженные контакты. При этом, если увольнение работника произошло за разглашение коммерческой тайны, это относится к разновидности мер дисциплинарной ответственности, основанием которой служит дисциплинарное правонарушение, т.е. противоправное, виновное поведение субъекта (работника), предусмотренное нормами ТК РФ.

В любом случае с такими работниками следует расставаться максимально по-дружески, поскольку вполне возможен вариант перехода сотрудника в конкурентную компанию с передачей инсайдерской информации.

Для того чтобы снизить подобные риски, можно использовать следующие меры:

- подписание при приеме на работу соглашения о невозможности работы на прямого конкурента при увольнении на протяжении определенного периода времени;

- подписание договора о неразглашении коммерческой информации с четким определением границ коммерческой тайны и суммами ответственности

за ее разглашение (в случае нарушения договора компенсация может быть взыскана и в судебном порядке);

- перед этапом высвобождения работника из компании осуществить его перевод на работу без доступа к информации, носящей коммерческую тайну;

- изучение причин увольнения и его отношения к компании (последнее в случае отрицательного отношения к организации может привести к распространению негативного имиджа).

В любом случае увольнение сотрудника должно сопровождаться четким объяснением причин увольнения, подкрепленным примерами-фактами либо плохой работы сотрудника, либо наличием проблем в компании.

В настоящее время в крупных корпорациях служба безопасности формируется как отдел, в котором работают профессионалы. В малых компаниях обеспечение безопасности часто становится дополнительной функцией юридического и HR-отделов. Практика показывает, что достаточно часто современные компании различных масштабов приглашают для обеспечения безопасности внешние специализированные агентства. В любом случае необходимо комплектование службы управления персоналом высококвалифицированными специалистами, компетентными в решении всего комплекса вопросов управления персоналом, способными исключить ситуации риска в процессе работы с персоналом.

Профилактическая работа с увольняющимися сотрудниками. Основная задача руководителя службы безопасности при работе с увольняющимися сотрудниками – получение оперативно значимой информации. В данном аспекте речь может идти лишь о сотрудниках, увольняющихся по собственному желанию. Работники, увольняющиеся по инициативе администрации, увольняются, как правило, по отрицательным мотивам. При этом не играет роли юридическая формулировка основания увольнения, т.е. то, что будет записано в трудовой книжке. Речь идет именно о фактических основаниях, а точнее, мотивах увольнения.

Объектом работы руководителя службы безопасности являются именно работники, выразившие желание расторгнуть трудовой договор с торговым предприятием по собственной инициативе. Работа с данной категорией сотрудников дает возможность получения информации из первых рук от людей, которым, как правило, нет смысла что-то скрывать, поэтому они охотно делятся известными им сведениями. Зачастую в результате подобной работы, проведенной руководителем службы безопасности, сотрудники, вполне лояльные к организации и вынужденные уходить из нее из-за других сотрудников, гораздо более «вредных и опасных», оставались. Следует помнить, что потеря грамотного, лояльного, трудолюбивого сотрудника хотя и не принесет прямого ущерба компании, однако косвенно вполне может повлиять на общий массив потерь организации. Более того, многие крупные компании декларируют положение о том, что персонал является «одной из ценностей компании», соответственно, и он подлежит защите со стороны службы безопасности.

Таким образом, процедура увольнения работников должна проводиться таким образом, чтобы человек, прекращающий трудовые отношения с компанией, не оказался источником угрозы для ее безопасности. Расставаться с бывшим сотрудником «без обид» нужно уметь.

Для этого совместно с отделом персонала и руководителями структурных подразделений служба безопасности должна принимать участие в выработке регламента увольнения с учетом законодательства. Разработка такой процедуры и выполнение всех ее требований позволит обеспечить безопасность организации от недобросовестных действий со стороны сотрудников, решивших по тем или иным причинам прекратить трудовые отношения с компанией, а также тех, чья деятельность перестала соответствовать требованиям рабочего места.

Как показывает практика, умение понимать любого сотрудника компании – важная составляющая профессионализма руководителя, особенно высшего уровня. К сожалению, некоторые ответственные лица порой не придают значения чувствам и переживаниям увольняющихся или попадающих под сокращение работников. Невнимание к их потребностям, незнание психологических особенностей членов коллектива зачастую влекут за собой серьезные проблемы, такие как нанесение экономического и материального ущерба, потеря имиджа компании, утечка информации, составляющей коммерческую тайну.

Очень важно задействовать в процессе увольнения возможности службы безопасности. Работники этой службы, зная организационную структуру компании, ключевые подразделения, в которых сосредоточены материальные ценности и сведения, составляющие коммерческую тайну, обязаны предусмотреть, что можно ожидать от того или иного сотрудника в любой ситуации, в том числе и при увольнении.

В случае, если сотрудник подал заявление об увольнении, служба безопасности обязана через руководителя структурного подразделения, доверенных лиц проконтролировать выполнение процедуры передачи дел и документов, а главное – не допустить нанесения материального ущерба, уничтожения рабочих документов и информационных материалов.

Как показывает практика, наиболее травмирующая сотрудника ситуация – увольнение по инициативе руководства или в связи с сокращением штатов.

Специалисты по управлению персоналом рекомендуют: каковы бы ни были причины увольнения, человек должен покидать компанию без чувства обиды, раздражения и жажды мести. В этом случае можно рассчитывать на то, что увольняемый сотрудник не предпримет действий, направленных против компании, останется к ней лояльным. В частности, не будет оспаривать решение руководства компании в суде; публиковать или распространять негативную информацию о деятельности компании; готовить физическую расправу над лицами, которых он считает виновными в своих проблемах; уничтожать документы, необходимые для продолжения работы компании; передавать важную информацию конкурентам и т.п.

В срок, предусмотренный законодательством для оформления увольнения, служба безопасности обязана проанализировать все имеющиеся у нее материалы об этом сотруднике и сделать вывод: может ли он нанести ущерб компании или нет. В случае обнаружения каких-либо негативных моментов необходимо принять меры, чтобы минимизировать ущерб.

Некоторые увольняющиеся сотрудники могут нанести ущерб компании: уничтожить/испортить материальные ценности, скопировать или уничтожить ценную информацию, индивидуальные или коллективные профессиональные наработки, похитить важные документы для дальнейшего личного использования или для передачи конкурентам. Служба безопасности должна предвидеть эту потенциальную опасность.

При увольнении сотрудника, который имел доступ к сведениям, содержащим конфиденциальную информацию или коммерческую тайну, служба безопасности должна оценить, информация какого уровня была ему доступна и в каком объеме, а также каковы возможные последствия от утечки этой информации.

В случае, если работник уже подал письменное заявление об увольнении, или планируется сокращение его должности, сотруднику службы безопасности рекомендуется провести с ним беседу – индивидуально или совместно с непосредственным руководителем. До беседы целесообразно тщательно изучить имеющиеся данные об увольняющемся (увольняемом), а также выяснить мотивы увольнения. При этом важно учитывать:

- характер взаимоотношений сотрудника с коллегами;
- отношение к работе;
- уровень профессиональной подготовки;
- наличие конфликтов личного или служебного характера;
- высказывавшиеся ранее пожелания перейти на другую работу;
- уровень доступа к информации, в том числе содержащей коммерческую тайну;
- предполагаемое в будущем место работы увольняющегося (увольняемого) и др.

Чтобы предупредить возможность нанесения экономического или иного ущерба компании, после увольнения сотрудников целесообразно узнать о новом месте их работы, отслеживать информацию о том, с кем в компании они продолжают поддерживать отношения. Посещение бывшими сотрудниками компании возможно, однако оно не должно оставаться без внимания службы безопасности. Офис не следует превращать в место встреч работающих и бывших сотрудников, поскольку это отвлекает людей от работы, кроме того, такие посещения могут быть предлогом для сбора коммерческой или конфиденциальной информации и др.

Анализ работы службы безопасности с персоналом показывает, что в компании необходимо выработать единую стратегию. При профессиональной работе можно своевременно предупредить возникновение значительной части проблем, связанных с «человеческим фактором».

3.2. Развитие лояльности персонала для обеспечения кадровой безопасности организации

Уровень лояльности сотрудников играет важную роль в создании и обеспечении кадровой безопасности организации, так как только лояльный сотрудник всегда готов смириться с трудностями компании, идти вместе с ней к долгосрочным целям; данный сотрудник способствует увеличению производительности, снижению конфликтности в коллективе, качественному обслуживанию потребителя, что, в свою очередь, приводит к увеличению прибыли компании.

Лояльность сотрудника – это верность, преданность целям и ценностям компании, осуществление деятельности, которая поддерживает и помогает реализовать эти цели.

Лояльность сотрудника непосредственным образом влияет на кадровую безопасность организации, поскольку она, 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.

Таким образом, 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 ответственные, чувствуют свою обязанность перед организацией сделать все не только в срок, но качественно;
- лояльные сотрудники могут сохранить лидерские позиции организации, если это сопровождается правильной стратегией, конкурентоспособными товарами и услугами.

Нелояльные сотрудники – это те сотрудники, которые равнодушны к ценностям компании и ее целям, не готовы прилагать усилия для их достижения.

На отсутствие лояльности может указывать следующее:

- склонность сотрудников к обману;
- невыполнение функций и обязательств полностью, игнорирование поручений;
- проявление бездействия в критических ситуациях;
- 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. Связь лояльности и жизнеспособности компании представлена на рисунок 24:

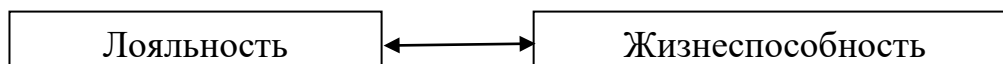


Рис. 24. Связь лояльности и жизнеспособности организации

Лояльность иногда отождествляют с благонадежностью персонала, однако, эти понятия несинонимичны.

Благонадежность сотрудника определяется как соблюдение (стремление соблюдать) человеком правовых и моральных норм, принятых в данной группе. Благонадежность иногда трактуют как законопослушность.

Благонадежность, таким образом, выступает как характеристика, особенность личности.

Лояльность – это принятие, положительное отношение человека к чему-то конкретному. Специалисты отмечают, что основой лояльности является желание быть полезным, преданность, избегание того, что может навредить. Персонал может быть лоялен к руководству компании, клиенты – по отношению к компании, предоставляющей услуги. Если сотрудник лоялен к руководителю, то это предполагает признание высокого уровня его компетентности, уважение, авторитет руководителя в глазах этого человека. Иногда такая лояльность включает чувство симпатии, сочувствия, готовность жертвовать своими интересами.

Лояльность клиентов, потребителей компании связана с признанием высокого качества ее товаров, услуг, доверием к персоналу этой компании.

Следовательно, лояльность является показателем отношения личности к определенному объекту.

Обязательные атрибуты лояльности:

- честность по отношению к объекту лояльности;
- разделение с объектом лояльности основных убеждений, ценностей;
- открытая демонстрация лояльности, доброжелательное отношение;
- переживание за успех лояльности;
- готовность предупредить опасность для объекта лояльности;
- готовность при необходимости идти на определенные жертвы в пользу объекта лояльности;
- чувство гордости за причастность к объекту лояльности (например, за принадлежность к числу сотрудников компании);
- стремление наилучшим образом исполнять обязанности, функции, миссию, возложенные на человека объектом лояльности.

Близкими по значению являются лояльность и преданность, верность. Преданность может рассматриваться как высший уровень лояльности.

В каждом конкретном случае, применительно к отдельным людям и в отношении различных объектов лояльность и благонадежность могут сочетаться по-разному:

- благонадежен и лоялен (например, работник стремится честно выполнять все нормы и предписания и с большим уважением относится к руководству);
- неблагонадежен, но лоялен (человек, имеющий склонность к воровству, мошенничеству, но по определенным причинам признающий авторитет и компетентность руководства компании);
- благонадежен, но не лоялен (в целом очень законопослушный сотрудник может быть крайне нелоялен к компании, осознав несправедливое отношение к себе со стороны руководства);
- неблагонадежен и нелоялен (пожалуй, самое опасное сочетание, когда склонность к нарушению норм усиливается негативным отношением к компании, ее руководству).

Можно выделить ряд форм деструктивного поведения (рисунок 25), представляющего угрозу для безопасности организации и успешной мотивации персонала.

Следствием наличия работников, обладающих такими типами поведения, являются:

- разрушение единения и сплоченности коллектива, нарушение его стабильной работоспособности;
- рождение угрозы непредсказуемого, опасного для окружающих поведения, вызванного страхом, гневом, сниженным самоконтролем;
- нарушение техники безопасности, ведущей к риску возникновения несчастных случаев на рабочем месте, угрожающих производственной безопасности в целом;

– продажа конкурентам важнейшей конфиденциальной информации, воровство и мошенничество, используемое для удовлетворения своих потребностей за счет работодателя.

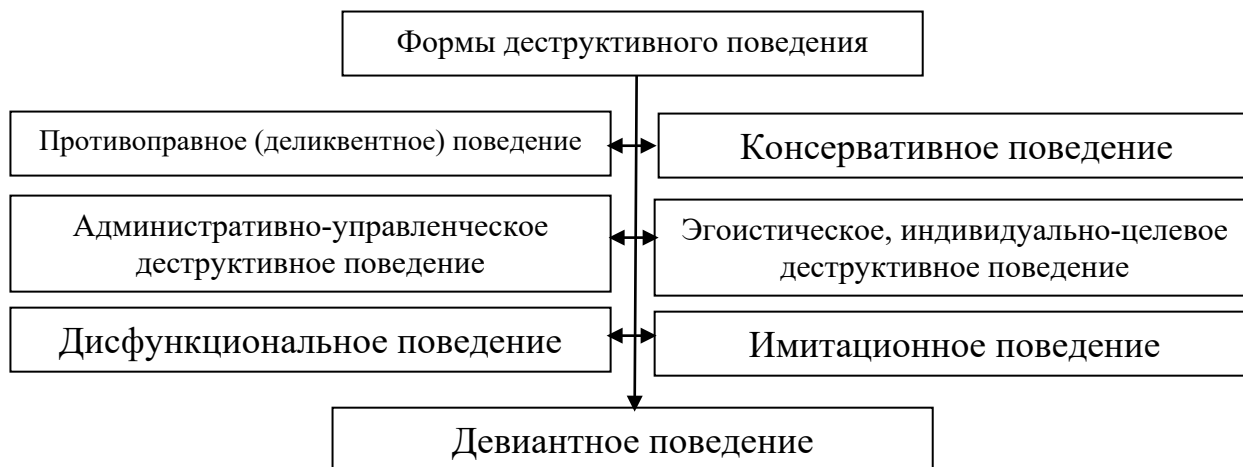


Рис. 25. Формы деструктивного поведения

Лояльность – комплекс мер по установлению позитивного отношения работников к работодателям. От того, кем ощущает себя сотрудник предприятия – механическим элементом или частью общего дела, заменимым «винтиком» или уважаемым участником производства, зависят и проблемы кадровой безопасности.

Кадровая безопасность, являясь элементом экономической и социальной безопасности компании, нацелена на такую работу с персоналом, на установление таких трудовых и этических отношений, которые можно было бы определить как «лояльные».

Лояльность может оказывать существенное влияние на благонадежность сотрудников, между ними существует взаимосвязь. Эту связь наглядно иллюстрирует схема-метафора «Бассейн».

В структуре благонадежности выделяют три элемента:

- 1) общечеловеческие нормы и ценности, которые усвоил человек в данный момент (на схеме это «кирпичи», из которых построен «бассейн»);
- 2) стремление, желание человека соблюдать эти нормы и ценности («цемент», соединяющий «кирпичи»);
- 3) внешние и внутренние причины, побуждающие человека к неблагонадежному поведению, к кражам, мошенничеству и иным проступкам и преступлениям («вода» в «бассейне»).

Получается, что чем выше стенки «бассейна» (т.е. чем больше норм и правил усвоил человек), тем больший объем «воды» (т.е. давления) он будет удерживать. «Вода» может пролиться, что символизирует нарушение человеком принятых норм, если ее уровень станет выше, чем стенки «бассейна». Примером такого сильного давления может быть шантаж. В этом случае даже тот сотрудник, который имел высокую благонадежность, может совершить преступление, наносящее ущерб организации.

Однако даже если уровень давления будет невысоким, «вода» может пролиться (т.е. человек совершит правонарушение) и по другой причине – если «цемент», соединяющий «кирпичи», будет непрочным. В этом случае человек, несмотря на знание норм и правил, идет на нарушение в силу нежелания выполнять их. Отечественная практика свидетельствует, что именно сотрудниками (или с их участием) совершаются 90% краж внутри организаций, так как именно они лучше всего знают «слабые места», которые можно использовать в своих корыстных целях».

Желание (готовность) соблюдать правила у человека может изменяться: от фанатичного соблюдения каждого из них до пренебрежения всеми правилами. Современные исследования, в частности проблемы мошенничества персонала, дают основания утверждать, что одним из основных факторов, влияющих на желание соблюдать нормы, выступает лояльность в отношении предприятия, его руководства. Лояльные сотрудники более благонадежны.

Таким образом, повышая лояльность работников, можно защитить организацию от значительной доли внутренних угроз. Но сложность состоит в том, что причиной значительной части угроз такого характера является психологическая некомпетентность руководителей, менеджеров или их несоответствие профессионально важным требованиям.

В процессе многочисленных психологических исследований установлено, что большинство людей хотят работать хорошо. Но то, как они работают на самом деле, зависит от руководителя. К сожалению, очень часто можно наблюдать организации, в которых персонал работает не благодаря руководству, а вопреки ему. Некомпетентные руководители разрушают даже те остатки мотивации, которые присутствовали у сотрудников на момент найма на работу.

С целью защиты организации от внутренних угроз рекомендуется руководствоваться следующими правилами:

- создать действенную систему материальных стимулов;
- обеспечить каждого сотрудника долговременной работой;
- относиться к сотрудникам как к личностям, способным принимать самостоятельные решения;
- обеспечить участие в прибылях;
- создать возможности для продвижения по службе;
- обеспечить участие всего персонала в выработке решений;
- создать гибкую, не травмирующую систему увольнений.

В коллективе, где царит уважение и доверие, дружеские отношения и поддержка, гибкий график работы, возможность работы «на стороне», корпоративные вечеринки, спортивные и прочие «семейные» мероприятия, желание предать коллектив и выдать конфиденциальную информацию компании практически не возникает.

Создание атмосферы открытости, которая является условием формирования лояльности, одновременно выступает одним из средств профилактики воровства персонала. Безусловно, в некоторых случаях не избежать применения технических средств контроля, но их использование

должно быть гласным, «без элементов параноидальной подозрительности». Ученые отмечают, что если в коллективе сформировать деловые отношения, основанные на открытости, персональной ответственности и конструктивной обратной связи, можно сократить не только урон, связанный с воровством, но и затраты на создание систем технического мониторинга.

Для решения задачи предотвращения воровства персоналом можно создать так называемую «самоконтролирующуюся систему». Ее основным элементом является максимальная прозрачность для всех сотрудников финансовых и материальных потоков внутри подразделений фирмы, что одновременно является и одним из важных условий или принципов формирования лояльности. Современный бизнес и присущие ему методы менеджмента слишком «затемняют» механизмы распределения общей прибыли. Именно по этой причине воровство и коррупция стали бичом современных компаний.

С точки зрения изучения лояльности работников компании, построения прогнозов их поведения, планирования мероприятий, направленных на повышение лояльности, большое практическое значение имеет представление об уровнях лояльности (рисунок 26).



Рис. 26. Уровни лояльности персонала

Шкала имеет нулевую точку, обозначающую так называемую нулевую лояльность. Наличие этой точки демонстрирует, что отсутствие лояльности не является нелояльностью. Нулевая лояльность может быть у постороннего человека, не сформировавшего своего отношения к определенному объекту. Близкой к этой отметке может быть лояльность к компании у человека, поступающего туда на работу, но не информированного об особенностях ее корпоративной культуры.

Выше нулевой отметки на шкале находятся уровни лояльности, а ниже – нелояльности. Рассмотрим эту шкалу, начиная с низших точек, т.е. с

нелояльности. Здесь можно различать два уровня: скрытая (тайная) нелояльность и демонстративная (открытая). Психологи указывают на следующие признаки демонстративной нелояльности:

- ложь, обман;
- сарказм, высмеивание, демонстративное пренебрежение к ценностям, которые важны для объекта лояльности;
- потребительское отношение, преимущество личных интересов;
- нарушение достигнутых договоренностей и т.п.

Опасность, исходящая от нелояльных сотрудников, связана с их влиянием на других людей. Они разрушают ценности и убеждения своих коллег, порождают сомнения в целесообразности определенных действий.

Скрытая нелояльность проявляется так: будучи на виду, люди исправно выполняют предписываемые правила и требования, но причина такого поведения – не положительное отношение, а опасения наказания или ожидание вознаграждения. Зачастую именно те сотрудники, которые имеют скрытую нелояльность, распространяют негативные корпоративные слухи и сплетни.

На организационном уровне следствием нелояльности сотрудников является высокая текучесть персонала. А это, в свою очередь, увеличивает затраты на поиск, наем и обучение новых работников, повышает риск утечки конфиденциальной информации и прочие издержки. Поэтому некоторые компании предпринимают попытки реализации программ удержания сотрудников. Целью таких мероприятий является повышение уровня лояльности персонала.

Выше нулевой точки на шкале представлены уровни лояльности. Чем выше уровень, тем выше степень вовлеченности и преданности сотрудника.

Первый уровень – это лояльность на уровне внешних атрибутов. С такой лояльностью человек готов носить отличительные символы и знаки компании, фирменную одежду, знаки, символизирующие статус в компании (например, продавец, старший продавец, продавец-инструктор). При этом внешние атрибуты не позволяют их обладателю демонстрировать нелояльное поведение. Пока он на виду, человек будет воспроизводить обусловленное этими атрибутами поведение. В компаниях, специализирующихся на реализации определенных товаров, этот уровень лояльности предполагает, что работники компании становятся активными потребителями этих товаров. Верно и обратное утверждение: побудив к потреблению товаров, мы повышаем уровень лояльности людей. Этот принцип активно используется, например, в сетевом маркетинге.

Лояльность на уровне поступков, поведения связана с соблюдением ритуалов, традиций, обычаев, принятых в компании. Такими традициями могут быть особая тональность в обращении с клиентами, формальные и неформальные собрания (вечеринки) и т.п. Сотрудники, лояльные к компании на таком уровне, с энтузиазмом или как минимум без затруднений участвуют в таких мероприятиях. Но здесь возникает сложность, связанная с тем, что в коллективе могут быть негативные традиции. Именно они становятся причиной

лояльного в отношении конкретной группы, но не лояльного в целом для компании поведения.

Лояльность на уровне действия связана и с профессиональной компетентностью. Лояльный сотрудник стремится овладеть необходимыми профессиональными знаниями, умениями, навыками, продуктивными стереотипами деятельности. Такое стремление, как правило, приводит к повышению эффективности деятельности. И наоборот, отсутствие желания учиться, можно рассматривать как один из признаков более низкого уровня лояльности. Для данного уровня лояльности характерна дисциплинированность. При этом сотрудники выполняют требования дисциплины не столько из-за опасности наказания, сколько в силу своего отношения к компании и ее руководству.

Лояльности на уровне убеждений большинство работников компании не достигают. Для компании достаточно, если столь высокого уровня лояльности достигают 10–15% работников. Это в первую очередь касается руководителей среднего и высшего звена. Лояльность персонала на уровне убеждений представляет большую ценность для компании в силу ее положительного влияния на профессиональную мотивацию. Лояльные сотрудники максимально отдают себя работе, нетерпимы к нарушениям правил со стороны других людей. Они активны в устранении проблем, могут быть инициаторами усовершенствования деятельности, способны отстаивать конструктивные предложения.

Сотрудники, имеющие этот уровень лояльности, как правило, более ответственные. Они чувствуют свою обязанность выполнять все точно, правильно, качественно. По наблюдениям специалистов, лояльные сотрудники легче переносят трудные для компании времена и остаются работать, руководствуясь чувством верности, сопричастности. Они более склонны доверять официальной информации, решениям, которые принимает руководство.

Вместе с тем, по мнению специалистов, с такой лояльностью сотрудников могут быть связаны и некоторые сложности. Например, если по тем или иным причинам компания изменяет принятые ранее ценности и убеждения, то она может столкнуться с сопротивлением части коллектива, разделяющего прежние убеждения. Поэтому при проведении организационных изменений важно убедить таких сотрудников в необходимости перемен, привлечь их к планированию и осуществлению нововведений. Еще одна сложность: формирование этого и более высокого уровня лояльности требует определенного стиля лидерства, способности высших руководителей внушать определенные ценности и установки, целенаправленно формировать необходимые убеждения.

Лояльность на уровне идентичности является самым высоким уровнем. Вероятно, именно такую лояльность называют преданностью, верностью. В этом случае человек максимально отождествляет себя с объектом лояльности. Исследователи отмечают, что именно такой уровень лояльности у персонала формировала японская система пожизненного найма.

Лояльность в этом случае не так зависит от уровня вознаграждения. Человек с такой лояльностью меньше подвержен негативному влиянию со стороны окружающих. Он связывает свою жизнь с компанией. Такой работник максимально мотивирован и предельно эффективен.

Лояльное поведение – это либо поведение, в основе которого лежит лояльность, либо поведение, демонстрирующее таковую. Поэтому в некоторых случаях лояльное поведение и действительная лояльность могут не совпадать.

Какой же уровень лояльности сотрудников будет удовлетворять компанию и как его повысить, если он недостаточно высок?

Для большинства организаций вполне достаточными являются первые два уровня лояльности персонала. Для низшего исполнительского уровня сотрудников, деятельность которых предполагает жестко регламентированные и контролируемые процедуры, достаточно даже нулевой лояльности. Но руководители среднего и высшего звена должны иметь более высокий уровень лояльности. То есть, чем выше должность, тем большей лояльности она требует.

Анализируя современные тенденции в кадровой работе, специалисты отмечают общее снижение уровня лояльности работников в отношении их работодателей. Это, с одной стороны, обусловлено низким уровнем компетентности менеджеров, руководителей, их неумением целенаправленно формировать лояльность персонала, с другой стороны, появлением на рынке рабочей силы принципиально новой категории наемных работников, которых стали называть «knowledge workers» – «знающими», или «вооруженными (обладающими) знаниями работниками». Основной особенностью этих сотрудников является их способность создавать новую ценность за счет собственных знаний, а не материальных ресурсов. В отличие от пролетария индустриальной эпохи обладающие знаниями работники не зависят от материальных факторов производства, они уже располагают всем, чтобы быть производительными. Поэтому такие работники склонны к более независимому поведению, гораздо легче меняют места работы, поддерживают отношения с несколькими компаниями одновременно.

Вопрос о том, как повысить лояльность, требует анализа ее составляющих. Можно выделить минимум три составляющие лояльности:

- доверие персонала к руководству компании;
- справедливость отношений, складывающихся у сотрудника с представителями администрации компании;
- удовлетворенность работой.

Развитие лояльности, следовательно, состоит в увеличении ее составляющих. Работа, направленная на повышение лояльности, имеет циклический характер и состоит из последовательных этапов.

Первым этапом является диагностика (изучение) уровня лояльности персонала. Полученная в процессе диагностики информация является основанием для принятия решения о необходимости повышения лояльности и разработки программы ее развития. После реализации программы важно получить обратную связь, т.е. снова провести диагностику уровня лояльности и

убедиться в действенности реализованной программы. Естественно, что реализация такого цикла растянута во времени, рассчитана на долгосрочную перспективу.

Работа, связанная с развитием лояльности персонала, обычно возлагается либо на сотрудников и руководителей кадровых подразделений компаний, либо на внешних консультантов. Но, как показывает опыт, развитие лояльности обычно требует существенного изменения стиля управления (стиля лидерства), внедрения серьезных организационных преобразований и в целом совершенствования корпоративной культуры. Поэтому успешная реализация программ повышения лояльности персонала невозможна без непосредственного участия высшего руководства компании (таблица 7).

Таблица 7

Влияние профилактических мероприятий на лояльность персонала

Цели мероприятий	Влияние на возможности мошенничества	Влияние на причины мошенничества
1. Создание атмосферы честности, открытости и взаимопомощи	– равнодушие к происходящему со стороны руководства – равнодушие со стороны коллег – некомпетентность сотрудника или коллег	– явное неравноправие внутри коллектива – враждебная атмосфера по отношению к коллегам – недружелюбная атмосфера соперничества – плохой стиль общения – другие личностные причины
2. Ликвидация элементов кадровой политики, способствующих мошенничеству	– отсутствие четких должностных обязанностей – отсутствие факторов, морально дисциплинирующих сотрудников – отсутствие четкой системы приема на работу и критериев оценки кандидатов – недостаточная обученность и подготовка кадров – большая текучесть кадров и прогулы – неспособность начальства оценить качество выполненной работы – отсутствие обратной связи руководства с персоналом – низкое качество подготовки менеджеров	– излишне жесткие правила внутреннего распорядка – ошибочное сознание того, что руководству неинтересны моральные принципы персонала – неучет различий между людьми, – плохие возможности для продвижения по службе – неадекватная заработная плата – мнимая недооценка своих успехов – чувство неудовлетворенности от работы – боязнь потерять работу – ошибочное ощущение того, что платят меньше заслуживаемого – сведение счетов с начальством – наличие руководителей, поведение которых неадекватно должности – стремление руководителей к шикарному образу жизни – авторитарический стиль руководства, импульсивность, бесчувственность, давление – стиль управления, направленный на устранение последствий, а не причин проблем
3. Помощь	– факт, что фирма в	– сознание такого факта, особенно если

Цели мероприятий	Влияние на возможности мошенничества	Влияние на причины мошенничества
сотрудникам как проявление заботы о персонале	экстренных или тяжелых ситуациях не защитит и не позаботится о своем сотруднике	таковой реально имеет место
4. Специальная подготовка менеджеров и сотрудников противостоянию мошенничеству	– незнание порядка необходимых действий при обнаружении или подозрении в совершении мошенничества	– легкость осуществления мошенничества в рабочем коллективе или на рабочем месте
5. Проверка персонала	– низкое качество знания своих сотрудников, влияющее на оценку предсказуемости их действий – невнимание в проблемы сотрудников.	– жизнь сотрудника не по средствам – необычное, подозрительное поведение сотрудника – неясное или уголовное прошлое сотрудника
6. Правовое и юридическое обеспечение деятельности.	– нарушение принципа неотвратимости наказания – отсутствие отработанной организационно-правовой базы материальной ответственности и ответственности за разглашение коммерческой тайны и др.	– незнание видов и степени ответственности за противоправные деяния и другие нарушения

Для успешной реализации данных мероприятий следует соблюдать следующие условия.

1) В такой работе должно быть заинтересовано высшее руководство компании. Именно они принимают решение о реализации программы.

2) Руководитель компании должен быть готов к последующим изменениям, материальным и нематериальным затратам, необходимым для претворения плана в жизнь.

3) Ответственный за реализацию плана должен иметь такой статус в компании, который позволит ему координировать усилия различных служб и подразделений.

4) Компания заинтересована в долгосрочных отношениях с теми сотрудниками, в отношении которых осуществляется программа развития лояльности.

Как можно видеть из таблицы, мероприятия по предотвращению мошенничества должны охватывать практически все стороны деятельности организации, хотя бы потому, что проблемы создают люди и работают они везде.

Что же касается влияния на лояльность, а в таблице ясно видно преобладание проблем менеджмента, основная задача службы безопасности – добиться понимания руководителями всех уровней, что лояльность – это

определяющий фактор устойчивости организации в целом, а не только в связи с мошенничеством.

Программа развития лояльности может включать определение или корректировку долгосрочных и краткосрочных целей компании, ценностных ориентиров. Изначально нужно спрогнозировать противоречия и препятствия в достижении цели. В некоторых случаях может возникнуть необходимость избавиться от некоторых нелояльных сотрудников, препятствующих реализации мероприятий. Так же, как и при внедрении любых других организационных изменений, важно создать активную «группу поддержки». Такая работа зачастую предполагает дополнительные финансовые затраты.

Специалисты убеждены в том, что создание лояльности у работников – лучшее вложение средств, способное быстро и значительно повысить эффективность организации и ее безопасность.

3.3. Контроль персонала как условие обеспечения кадровой безопасности организации

Контроль – комплекс мер, установленных для персонала и содержащихся в регламентах, объединяющих ограничения, режимы, технологические процессы, оценочные, контрольные и другие операции и процедуры безопасности. Контроль нацелен непосредственно на обеспечение безопасности организации, ликвидацию возможностей причинения ущерба и является, как правило, функцией службы безопасности или других подразделений.

Обеспечение кадровой безопасности в процессе функционирования трудового коллектива осуществляется по четырем основным направлениям (рисунок 27) и в рамках трех форм контроля (предварительного, текущего и итогового).

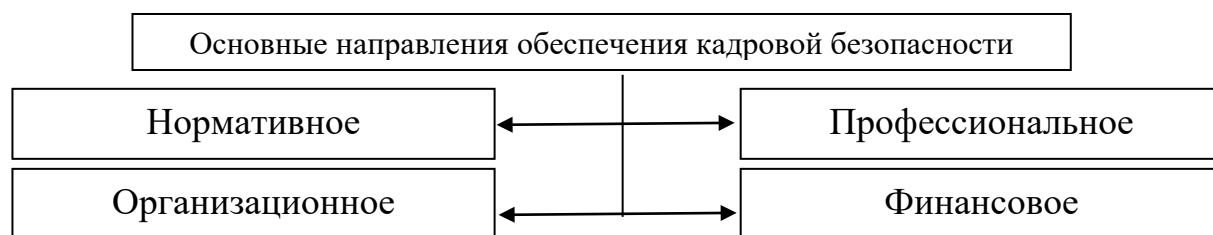


Рис. 27. Основные направления обеспечения кадровой безопасности

Нормативное направление обеспечения кадровой безопасности предполагает разработку (на предварительном этапе контроля) и необходимую корректировку (на последующем этапе) следующих регламентов:

- правил внутреннего трудового распорядка;
- трудовых договоров;
- договоров материальной ответственности;
- должностных инструкций, определяющих обязанности и действия сотрудников;
- соглашений о неразглашении конфиденциальной информации, коммерческой тайны, персональных данных;

- регламентов использования средств коммуникаций и доступа в Интернет;

- перечня контрольных процедур за исполнением должностных инструкций;

- порядка наложения дисциплинарной и финансовой ответственности за ненадлежащее выполнение должностных обязанностей и нарушение прочих нормативных актов.

В рамках *организационного направления* мероприятия предварительного контроля включают утверждение и внедрение в практику деятельности соответствующих сотрудников и подразделений следующих локальных нормативных актов:

- перечня контрольных процедур за выполнением должностных инструкций;

- описания дисциплинарной и финансовой ответственности за ненадлежащее выполнение должностных обязанностей;

- программы противодействия угрозам сотрудникам организации и мошенничеству;

- порядка внесения в нее корректировок.

На этапе предварительного контроля проводится подготовка решения о назначении лица на должность ответственного за осуществление контроля персонала организации с широким кругом полномочий. Эффективным средством кадровой безопасности в области предотвращения мошенничества является также создание линии доверия. В компьютерные сети в обязательном порядке должны быть внедрены средства защиты от мошенничества, адекватные объему и характеру проводимых финансовых и товарных операций.

Текущий контроль в рамках данного направления обеспечения кадровой безопасности должен обеспечить ознакомление сотрудников с действующим порядком закрепления обязательств, должностных функций и ответственности за их неисполнение.

Профессиональное направление предполагает проведение мероприятий текущего контроля в соответствии с утвержденным перечнем контрольных процедур за выполнением должностных инструкций, позволяющих, с одной стороны, оценить соответствие лица занимаемой должности, а с другой – пресечь нарушения в будущем посредством наложения установленных дисциплинарной и (или) финансовой ответственности за ненадлежащее выполнение должностных обязанностей.

При этом текущий контроль должен проводиться по четырем основным направлениям:

- 1) соблюдения трудовой дисциплины, т.е. выполнения правил внутреннего трудового распорядка;

- 2) соблюдения исполнительской дисциплины, т.е. требований должностной инструкции, приказов, распоряжений, положений, регулирующих деятельность персонала, а также устных указаний руководителей;

3) рационального и эффективного использования материальных ресурсов, с помощью которых выполняется работа и исполняются служебные обязанности;

4) профессионального поведения, соблюдения делового этикета, поиска и сбора информации только в пределах своей компетенции, обсуждения рабочих вопросов только с лицами, в обязанности которых они включены соответствующими регламентами.

При итоговом контроле проводится анализ установленных нарушений и выявляются их причины с целью внесения корректив в соответствующие регламенты.

Финансовое направление кадровой безопасности осуществляется в форме текущего контроля (мониторинга) расходов сотрудников организации и полноты, обоснованности и правильности расчетов с ними по заработной плате. Достоверность финансовой информации о расчетах с сотрудниками по заработной плате является обязательным условием соблюдения интересов государственных органов и внебюджетных фондов не только в части реализации государственных социальных программ, но и полноты взносов в бюджеты субъектов и внебюджетные фонды. Поэтому особое внимание в организации кадровой безопасности должно уделяться вопросам правового и финансового контроля за расчетами с сотрудниками организации, бюджетом и внебюджетными фондами.

Данный контроль в рамках организации, как правило, осуществляется специальным подразделением внутреннего аудита, ревизорами или внешними аудиторами, а также непосредственно Федеральной налоговой службой РФ.

В настоящее время многие руководители все более глубоко осознают роль и место своих сотрудников в создании и поддержании общей системы корпоративной безопасности. В связи с этим большое внимание уделяется внедрению процедур тщательного подбора и расстановки персонала. Постепенно приобретают значимость рекомендательные письма, научные методы проверки на профпригодность и различного рода тестирования, осуществляемые кадровыми подразделениями, сотрудниками служб безопасности и группами психологической поддержки.

Изучение персонала, проверка его профессиональной пригодности, работоспособности, оценка иных качеств на предмет соответствия требованиям и уровню безопасности предприятия продолжается и в период трудовой деятельности работника. В большей степени это касается так называемого «проблемного персонала».

Одним из способов, позволяющих работодателю оградить свою организацию от некомпетентных или недобросовестных работников, является возможность установить испытательный срок при приеме на работу новичка. Трудовым законодательством на этот счет предусмотрено следующее. При заключении трудового договора соглашением сторон может быть обусловлено испытание работника в целях проверки его соответствия поручаемой работе. Условие об испытательном периоде должно быть указано в трудовом договоре.

Если этот пункт в трудовом договоре отсутствует, что работник принимается в штат без испытания.

В период испытания на работника распространяются положения ТК РФ, законов, иных нормативных правовых актов, локальных нормативных актов, содержащих нормы трудового права, коллективного договора, соглашения. Испытательный срок не может превышать трех месяцев, а для руководителей организаций, главных бухгалтеров, их заместителей, руководителей филиалов, представительств и иных обособленных структурных подразделений организаций – шесть месяцев, если иное не установлено федеральным законом.

Среди целей испытательного срока можно выделить проверку благонадежности вновь принятого работника, оценку его деловых качеств, требуемых для занимаемой должности качеств личности. Оценка деловых качеств и того, насколько сотрудник справляется с порученной ему работой, имеет определенные сложности. В первую очередь они связаны со спецификой выполняемой работы, а также со сферой труда. Так, в производственной сфере, где результатом труда является конкретный осязаемый результат, можно четко определить, насколько качественно выполняется работа. Если же есть недостатки, то не представляет большого труда выявить, с чем они связаны: с технологическими особенностями производства или с отсутствием достаточной квалификации у работника. В сфере услуг можно принять во внимание количество претензий клиентов к качеству оказания той или иной услуги.

Сложнее обстоит дело, когда работа связана с интеллектуальным трудом. В данном случае здесь должны анализироваться качество выполнения поручений руководителя, соблюдение сроков исполнения заданий, выполнение сотрудником общего объема работы, соответствие работника профессионально-квалификационным требованиям.

На этом этапе работа службы персонала направлена не только на продолжение тестирования нового работника, но и на формирование у него таких важных качеств, как лояльность, ответственность, преданность коллективу и руководству, соответствие корпоративной культуре и т.п.

Хорошо зарекомендовала себя практика наставничества, когда новичок снабжается персональным супервайзером из числа опытных сотрудников. Такой специалист – своего рода двойной агент. С одной стороны, он обеспечивает своему подшефному комфортное вхождение в должность, обучение в рабочем режиме. С другой – он способен проконтролировать сферу интересов новичка, выявить области излишней заинтересованности (в том числе в отношении конфиденциальной информации) или индифферентности.

Вместе с тем не является аксиомой то обстоятельство, что именно молодые, вновь принятые сотрудники содержат в себе потенциальную угрозу безопасности организации. Принципиально источником причиненного ущерба могут выступать даже ранее проверенные и перепроверенные работники.

Обеспечение безопасности организации и контроль с этих позиций за деятельностью персонала необходимы по той простой причине, что именно с этой стороны компании угрожают следующие риски:

- 1) продажа сотрудниками секретов фирмы;

- 2) выдача конфиденциальной информации в результате беспечности или по неосторожности;
- 3) вербовка сотрудников конкурентами;
- 4) хищение сотрудниками имущества, денежных средств организации.

По первым трем пунктам в качестве превентивных мер применяются проверка благонадежности персонала и обеспечение соответствующего режима. По последнему пункту – меры по защите имущества, информации, иных ценностных приоритетов организации.

В целях проверки благонадежности персонала теорией и практикой обеспечения безопасности организации выработан целый комплекс методов, среди которых приоритетом пользуются психологический, социометрический и контрразведывательный.

Содержание социометрического метода сводится к тому, что потенциальная возможность нелояльного отношения к организации со стороны отдельных работников выявляется на основе оценок его коллег. Сотрудник, вызывающий подозрение, проходит через процедуру анкетирования в составе формальной или неформальной группы. В анкете должны быть несколько вопросов, содержащих закамуфлированную оценку личного доверия.

Использование названных методов предполагает предварительную подготовку. Формирование тестов, назначение дня тестирования, само тестирование (анкетирование) должны проводиться таким образом, чтобы не нарушать права и интересы сотрудников и не вызывать лишнего подозрения. Целесообразно приурочивать подобного рода мероприятия к событиям, связанным с аттестацией, следующей «ступенью» карьерного роста сотрудника, либо обосновывать их необходимостью выявления слабых сторон деятельности организации и ее руководства. Подозреваемых в неблагонадежности лиц, а также потенциально опасных работников необходимо проверять в составе групп, наиболее приближенных к ним по работе (единство выполняемых трудовых функций, кадрового подразделения и т.п.).

Контрразведывательный метод отличается большей степенью аналитики, чем предшествующие. Здесь больший интерес представляют сведения не о психологических особенностях личности, а о событиях, явлениях и ситуациях, с которыми так или иначе эта личность связана.

Служба безопасности, менеджер по работе с персоналом должны регулярно отслеживать и обобщать поступающую информацию о правонарушениях, к которым причастны сотрудники организации. Имеются в виду, прежде всего, такие правонарушения, которые подрывают корпоративную безопасность организации (например, мелкие хищения) и в силу определенных обстоятельств не могут быть обнаружены охраной. Противоправные действия работника тщательно документируются (справки, объяснения, акты и так далее) и передаются в тот орган, в компетенцию которого входит их рассмотрение. Особое внимание при этом следует обратить на то, чтобы при задержании правонарушителя присутствовали очевидцы, чья объективность не подвергается сомнению (например, не рекомендуется приглашать в качестве очевидца сотрудника службы безопасности).

Систематический анализ информации позволяет своевременно и качественно выявлять причины, порождающие правонарушения, и условия, способствующие их совершению со стороны персонала организации. Обобщенные сведения необходимо регулярно представлять руководству. При этом важно не только своевременно информировать об этом, необходимо также одновременно вносить предложения по их устранению. Следует также помнить, что перечень причин и условий должен быть разработан на уровне конкретной организации.

Поскольку преступники при реализации своих замыслов стараются привлечь к негласному сотрудничеству других работников, то данной категории персонала со стороны службы безопасности уделяться самое пристальное внимание. С этой целью составляется список потенциальных помощников преступников, и с ними проводится работа с применением законных методов. Результатом такой работы должно быть либо документирование преступных действий сотрудника предприятия, либо склонение его к отказу от совершения преступления.

Консультирование сотрудников организации происходит преимущественно по всем видам безопасности. Формы консультирования – групповые (лекции, семинары и так далее) и индивидуальные. Среди персонала следует выделить те группы, которые необходимо систематически инструктировать. Если есть необходимость, то можно создать специализированные учебные курсы со сдачей зачетов.

Особую важность с точки зрения кадровой безопасности представляет мониторинг каналов неофициальной информации. Он позволяет получать наиболее адекватные данные о ситуации в коллективе, отслеживать признаки падения авторитета руководства, выявлять неформальных лидеров, получать самые разнообразные сведения вплоть до выяснения конкретных виновников тех или иных нарушений.

Обеспечение кадровой безопасности предполагает и контроль за «проблемным персоналом» «Проблемный» – это персонал, который может выступать потенциальным источником причинения ущерба организации. Мотивация действий последних может быть различной: месть, карьеризм, зависимость, азарт, зависть и т.п. В то же время типичной ошибкой является деление работников на тех, кто создает угрозы безопасности организации, и кто не представляет такого рода опасности, автоматически занося первых в разряд «проблемного» персонала.

Попадание работника в категорию «проблемный» в основном зависит от конкретной ситуации, складывающейся в организации. В связи с этим необходимо своевременно обращать внимание на следующие факторы:

- 1) отсутствие действенной системы материальных стимулов;
- 2) отсутствие гарантии долговременной занятости работников;
- 3) отсутствие возможностей для карьерного роста;
- 4) расстановка сотрудников без учета их способностей и желаний;
- 5) отношение к сотрудникам как к простым исполнителям воли руководства;

6) использование взысканий в качестве инструмента стимулирования работоспособности;

7) психотравмирующая практика увольнений.

Рассмотрим некоторые группы работников, которые могут быть отнесены к числу потенциально опасных для корпоративной безопасности (рисунок 28).

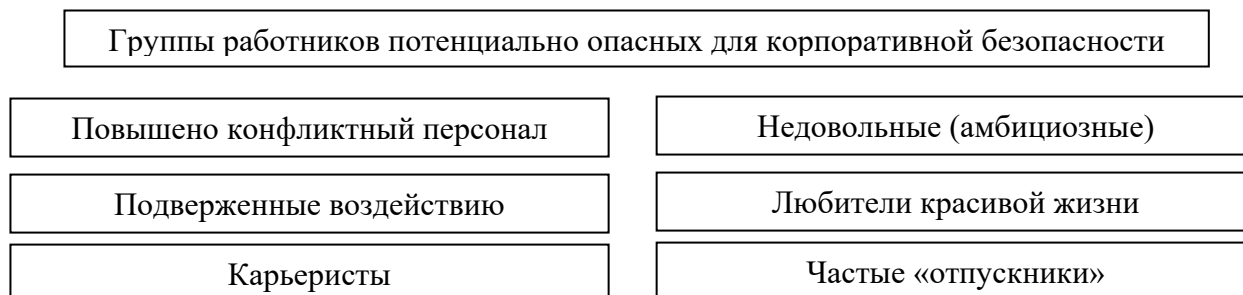


Рис. 28. Группы работников потенциально опасных для корпоративной безопасности

1) Повышено конфликтный персонал. Конфликты в организации всегда имели место. Однако больший риск заложен не столько в самом конфликте, сколько в его причинах и постконфликтной ситуации.

Далеко не всегда развитие конфликта осуществляется по схеме «начальник всегда прав». Золотое правило руководителя в таком случае – признав ошибочность, несостоятельность своих решений, действий, предупредить развитие конфликта. Серьезную опасность в рассматриваемом аспекте несут те конфликты, которые оставляют «осадок» обиды, незаслуженного наказания со стороны руководителя. Такого рода работники, как правило, в большей степени восприимчивы к наказанию, у них значительно развито чувство несправедливости. И тогда они способны из чувства мести (реже зависти, корысти) дезорганизовать деятельность если не всей организации, то отдельного ее подразделения.

2) Подверженные воздействию. В этих случаях мы сталкиваемся с лицами сильной внушаемости, имеющими определенного рода зависимость, которая обременительна для их личного бюджета (наркомания, алкоголизм, азартные игры). Именно значительная сила внушения и зависимости заставляет последних менять свои жизненные приоритеты, принципы, ценности.

3) Карьеристы. Для достижения поставленных целей и «освоения новых высот» могут не побрезговать никакими способами и средствами. Повышенную опасность представляют они в том случае, если в силу занимаемого положения получают доступ к информации о персонале компании. Главная их цель – выслужиться, завоевать более высокий социальный статус.

4) Недовольные (амбициозные). К данной группе относятся работники, обладающие завышенной самооценкой, имеющие определенные знания, навыки, опыт, но в силу объективных (субъективных) причин не могут их реализовать на работе. В таких случаях возможны два варианта:

а) человек вырос из рамок своей должности (профессии), но ему не дают развиваться дальше;

б) человек не способен к дальнейшему росту, но жаждет всеобщего признания (почета, уважения, славы и т.п.).

В первом случае дело чаще всего заканчивается тем, что такой работник переходит на работу в другую организацию, не исключен вариант, что и к конкурентам. Во втором случае данный сотрудник, используя складывающуюся ситуацию, обладая достаточной информацией о деятельности организации, не получая поощрения от руководства, может оказывать негласное содействие конкурентам.

5) Любители красивой жизни – работники, чей уровень жизни явно не соответствует их доходам.

6) Частые «отпускники» – работники, которые под разными предлогами часто выходят в непродолжительные отпуска (например, в связи с заболеванием родственников, собственной болезни и т.п.).

В приведенный перечень могут быть также включены сотрудники, заключившие срочный трудовой договор и планирующие в ближайшее время его расторгнуть. Повышенное внимание следует обращать и на руководящий состав организации. Последние имеют довольно большие информационные возможности. Также следует отметить лиц, работающих по совместительству, занимающихся научной, преподавательской или творческой деятельностью сверх основной работы. Они порой неосознанно могут переносить значимую для организации информацию от одного работодателя к другому.

Таким образом, основными задачами организации контроля персонала организации выступают:

- оценка общей эффективности управления обеспечением безопасности организации;

- контроль над лояльностью конкретных сотрудников;

- выявление конкретных нарушений и их виновников.

Данная работа осуществляется службой безопасности одновременно по нескольким направлениям.

Профилактический контроль над соблюдением правил обеспечения безопасности в трудовых коллективах проводится с использованием различных методов и процедур, в частности:

- плановых и внезапных проверок, в процессе которых служба безопасности проверяет соблюдения в структурных подразделениях правил работы с конфиденциальной информацией, хранения денежных и иных ценностей, а также работоспособность технических средств защиты;

- мониторинга ситуации с использованием специальных технических средств наблюдения (например, видеокамер, первоначально установленных в качестве технических средств защиты имущества и персонала);

- мониторинга ситуации силами нештатных информаторов службы безопасности из числа сотрудников соответствующих подразделений организации (подобная практика широко используется службами безопасности

предприятий и органов государственного управления, хотя обычно и не рекомендуется в открытых учебных материалах).

По результатам контроля служба безопасности готовит специальные отчеты для руководства, информационные записки на имя руководителей структурных подразделений. При необходимости она организует проведение специальных совещаний, собраний в трудовых коллективах подразделений, готовит проекты приказов о поощрениях или взысканиях.

Контроль личной лояльности персонала осуществляется службой безопасности в отношении сотрудников:

- занимающих ключевые рабочие места (кроме должности руководителя), обеспечивающие доступ к особо конфиденциальной информации или возможность принимать решения стратегического характера;
- привлечших внимание службы безопасности своим поведением или иными фактами, ставящими под сомнение их лояльность.

Обязательным условием организации такого контроля является соблюдение требований действующего законодательства, прежде всего, Закона РФ «О частной детективной и охранной деятельности в РФ», а также конституционных гарантий неприкосновенности прав граждан.

В зависимости от цели и используемых методов контроля могут быть выявлены прямые нарушения в деятельности сотрудника, являющиеся основанием для передачи соответствующего иска в судебные или заявления в правоохранительные органы, увольнения, иных форм дисциплинарных взысканий. К числу подобных нарушений относятся подтвержденные соответствующими документами или иными материалами факты:

- проникновения в закрытые компьютерные базы данных и операционные системы с целью их копирования или проведения несанкционированных операций по счетам;
- любых попыток хищения денежных средств или материальных ценностей;
- коррупции в форме получения взяток от клиентов или партнеров банка;
- успешной вербовки сотрудника субъектами потенциальных угроз;
- склонения подчиненных к нарушению доверия работодателя;
- нарушений правил внутренней безопасности банка, в том числе и не приведших к реализации соответствующих угроз.

Кроме того, по результатам персонифицированного контроля служба безопасности может выявить факторы, определяющие сомнения в потенциальной лояльности сотрудника, например:

- необъяснимое объективными причинами внезапное улучшение его материального положения или контактирующих с ним родственников;
- не вызванные служебной необходимостью контакты с представителями субъектов потенциальных угроз (конкурирующих банков, криминальных структур, налоговой полиции и т.п.);
- изменение образа жизни сотрудника или появление привычек и личностных качеств, делающих его уязвимым для вербовки и шантажа;

– зафиксированные регулярные высказывания недовольства работодателем, служебным положением, доходами и т.п.

В этом случае, в зависимости от занимаемого сотрудником служебного положения, профессиональных качеств, отзывов руководителя, к нему могут быть применены разнообразные методы воздействия. По отношению к малоценным для компании работникам рекомендуется невозобновление трудового контракта после истечения его срока, а до этого момента постоянный контроль над их поведением. В остальных случаях с сотрудником должна быть проведена индивидуальная профилактическая работа силами непосредственного руководителя, психолога службы персонала или специалиста службы безопасности.

Результаты персонифицированного контроля должны отражаться в системе специального учета самой службы безопасности и в индивидуальном досье сотрудника.

Выявление уже реализованных угроз безопасности организации с участием собственного персонала может осуществляться силами штатных специалистов службы безопасности, приглашенных сотрудников частных охранных структур, государственных правоохранительных органов. При этом используются разнообразные оперативно-следственные мероприятия.

Одна из современных особенностей контроля персонала в процессе трудовой деятельности и обеспечения кадровой безопасности связана с формированием системы слежения за сотрудниками. Чтобы добиться повышения эффективности, в организации идут на любые меры, в том числе на изучение деловой и личной переписки, прослушивание телефонных разговоров, наблюдение за посещением интернет-сайтов.

Служба безопасности может отслеживать и оперативно ставить в известность HR-менеджеров о негативных явлениях в организации со стороны сотрудников. В частности, речь может идти:

– о намеренном разжигании конфликтных ситуаций со стороны некоторых работников;

– нарушениях требований корпоративной политики использования информационных ресурсов;

– нелояльном поведении отдельных работников – рассылке резюме, назначении встреч с новыми работодателями, незаконной передаче за пределы компании информации ограниченного доступа;

– негативном поведении отдельных сотрудников, выражающемся в грубости, оскорблениях, моббинге по отношению к другим работникам.

Сегодня работодатели располагают современными электронными системами учета и регистрации рабочего времени, которые позволяют практически определить затраты рабочего времени непосредственно на работу, на отдых, потери рабочего времени по вине работника и по вине организации. Это осуществляется через системы контроля доступа, видеонаблюдение (может носить скрытый и открытый характер) и т.д.

Обычной практикой большинства корпоративных служб безопасности в настоящее время становится использование DAP-систем. Основная задача

подобных систем – сбор и протоколирование всей информации о деятельности сотрудника в автоматизированной системе организации, а также обработка этой информации для выявления инсайдерства, мошенничества и других подозрительных действий.

Специалисты отмечают, что, согласно статистике, сегодня около трети крупных российских компаний внедряют использование систем «контроля» за деятельностью своих работников. В связи с этим возникает вопрос о законности и оправданности подобного контроля.

В трудовом договоре между работодателем и работником обычно записано, что все созданное сотрудником принадлежит компании. Если сотрудник в рабочее время (оплачиваемое фирмой) занимается личными делами, то этим он наносит урон работодателю, а если пользуется Интернетом в своих целях, то еще и крадет деньги. Поэтому в любой серьезной организации, в которой не принято доверять сотрудникам, есть юрист, который любой, даже чрезмерный, контроль объяснит заботой о подчиненных.

К сожалению, контроль может перейти в тотальную слежку. Поэтому единственным пунктом, который может использовать сотрудник при защите своих прав, является обязанность работодателя при найме работников сообщать о том, что все их коммуникации в рабочее время не являются конфиденциальными, а работники обязаны подписать соответствующий документ, подтверждающий их согласие с корпоративными правилами. Такая система предполагает, что, с одной стороны, работодатель имеет право внедрять всевозможные системы контроля за деятельностью своих сотрудников, а с другой – обязан осуществлять контроль открыто, что может стать важным элементом концепции обеспечения кадровой безопасности организации.

Известно, что подавляющая часть компаний, независимо от организационной формы, несет огромные убытки, напрямую связанные с нечестностью собственного персонала. Становится это ясно сразу после совершения противоправных действий или после банкротства фирмы через пару лет и зависит, как правило, только от «профессионализма» мошенников, примененного к конкретной ситуации.

Корпоративное мошенничество – это умышленное неправомерное действие или бездействие сотрудников частных или государственных компаний, направленное на получение личной выгоды против интересов компании. Рискам корпоративного мошенничества должно быть уделено особое внимание, если условия функционирования организации характеризуются:

- децентрализацией управления;
- сложной организационной структурой и, соответственно, разграничением обязанностей должностных лиц;
- неадекватной системой мотивации и вознаграждения по условиям работы и результатам труда;
- низкой заработной платой сотрудников;
- недостаточной гарантией занятости;

- непродолжительными отпусками;
- отсутствием возможности карьерного роста и признания заслуг сотрудника.

Мошенником в 55% случаев является сотрудник организации. Специалисты определили среднестатистический портрет мошенника: это мужчина (81%) в возрасте 30-40 лет, имеющий высшее образование (65%) и занимающий пост менеджера среднего звена (42%) или даже топ-менеджера (31%), проработавший в организации не менее 3-5 лет (39%).

В зоне риска мошенничества находятся сотрудники организации, которые:

- имеют существенные финансовые затруднения;
- увлекаются азартными играми;
- алкогольно и наркотически зависимы;
- имеют тяжелобольных близких родственников;
- часто меняют место работы;
- психически неуравновешенны.

При мониторинге ситуации в рабочем коллективе, с точки зрения наличия мошенников, индикаторами служат такие обстоятельства, как:

- внезапный активный интерес к конфиденциальной информации, функциям коллег, деятельности других подразделений организации;
- изменения в поведении сотрудника, например необоснованный страх, неуверенность, сомнения относительно обычно предпринимаемых действий, сосредоточенность или невнимательность и т.д.;
- превышение расходов сотрудника на приобретение недвижимости, автомобилей, драгоценностей над его доходами;
- необычайно частое посещение ресторанов, поездки в путешествия и т.п.

Прежде чем предупреждать явление и бороться с ним, следует разобраться в причинах, по которым оно совершается, и в способах его реализации. Конечно, можно совсем избавиться от мошенничества, избавившись от субъектов (сотрудников) или объектов (ценностей), что вряд ли удастся. Следовательно, надо понять, что является причинами, что возможностями, и как их устранять.

Возможности совершения мошенничества появляются в случае, если:

- а) отсутствуют контрольные меры (учет, ревизии, инвентаризации) и/или аудиторские проверки, либо технологические процессы построены таким образом, что контроль становится затрудненным или невозможным;
- б) имеют место управленческие (равнодушие, некомпетентность начальства) или коммуникативные (отношение коллектива к фактам обмана и пр.) проблемы.

Практика выработала несколько групп методов противодействия корпоративному мошенничеству (рисунок 29).

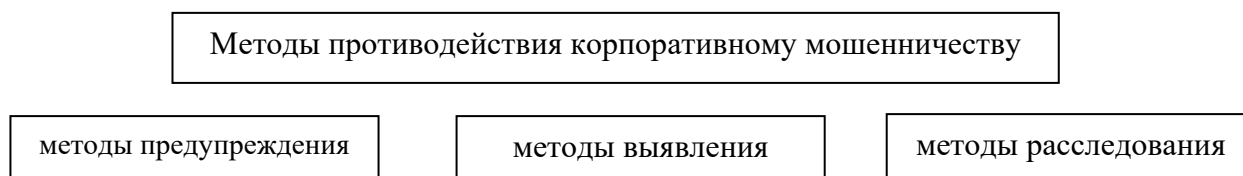


Рис. 29. Методы противодействия корпоративному мошенничеству

В каждой из трех групп можно выделить организационные и технические методы.

Наибольшую роль в выявлении и предотвращении мошенничеств в корпорациях играют организационные способы, основанные на развитой правовой и методической базе. В качестве организационных мер предупреждения выделяются:

- принятие нормативно-правовой документации, описывающей все типы запрещенных деяний и меры ответственности за них, ознакомление персонала с этими документами;
- создание в компании корпоративной культуры, полностью исключающей возможность совершения мошенничества;
- широкая практика привлечения к ответственности, как дисциплинарной, так и уголовной, всех виновных лиц;
- внесение в контракты сотрудников норм, позволяющих упростить их увольнение;
- создание в организации подразделений, отвечающих за контроль: службы экономической безопасности и внутреннего аудита.

Помимо этого, необходимо в качестве мер выявления регулярно проводить отдельные и полные проверки деятельности организации, ревизии, инвентаризации. Привлечение независимой аудиторской компании позволит получить доказательственную базу, на основе которой правоохранительные органы смогут возбудить уголовное дело.

Технические способы можно разделить на программные и иные. К программным средствам относятся все программные продукты, позволяющие:

- защищать информацию финансового характера от внесения в нее искажений;
- предотвращать утечку информации из компании;
- выявлять ошибки, несостыковки в отчетности и базах данных, указывающие на факт совершения мошенничества.

Защиту информационного периметра можно производить путем установки соответствующих программных продуктов. Кроме того, необходимо контролировать уровни доступа сотрудников, использовать такие степени защиты конфиденциальной информации и пароли, которые помогут выявить каждый факт несанкционированного вмешательства и своевременно информировать о нем службы безопасности.

При анализе отчетности и документации некоторые моменты поможет выявить программа Project Expert. Аудиторы имеют собственные методики, позволяющие сравнивать показатели разных лет и находить пиковые

искажения, которые могут свидетельствовать о совершении преступления и выводе активов.

Важную роль среди методов предотвращения корпоративного мошенничества играют оперативные методы. Конечно, компании в крайне редких случаях принимают решение приглашать специалистов из правоохранительных органов на стадии выявления деяния, имеющего признаки мошенничества. Самостоятельное же использование оперативных способов для служб безопасности компаний может стать поводом для нарушения законодательства. Тем не менее, допустимы такие меры, как:

- оборудование помещений системами видеоконтроля и звукозаписи;
- проведение контрольных закупок;
- не связанное с вторжением в частную жизнь изучение образа жизни сотрудника, заподозренного в мошенничестве.

Все эти способы помогают превратить подозрение в уверенность, но в большинстве случаев, в отличие от действий органов дознания, их результаты не смогут стать допустимыми доказательствами для суда в уголовном деле. Привлечение на самом раннем этапе органов дознания и следствия позволит использовать их наработанный аналитический аппарат, программные продукты, способы контроля сообщений СМС и переговоров в социальных сетях для того, чтобы собрать необходимые доказательства.

Профессионалы в процессе проведения оперативных действий смогут выявить:

- непосредственных виновников преступления и их пособников;
- мотивы совершения преступления; не всегда ими бывает только обогащение, иногда существенными факторами становятся внешнее давление, угроза, запугивание;
- механизм совершения преступления, характер и размер ущерба.

Важно, что правоохранительные органы могут работать в тесной связке с внутренними субъектами, отвечающими за защиту компании от мошенников. К ним могут относиться:

- сотрудники служб безопасности;
- ревизоры, аудиторы;
- представители членов Совета директоров, осуществляющие корпоративный контроль.

Спецификой российского бизнеса становится частое использование в схемах фирм-однодневок. Их выявление возможно при работе в тесном контакте с налоговыми органами. Часто выявление одной частной схемы приводит к вскрытию развернутой сети, в рамках которой происходит обналичивание, отмывание денег, подкуп государственных служащих.

Корпоративное мошенничество – серьезная проблема. Кардинальным средством ее решения является разработка и проведение в жизнь концепции безопасности кадрового развития организации, включающей в себя два важнейших аспекта – внешний и внутренний.

К внешним аспектам можно отнести неукоснительное соблюдение всеми работниками организации Конституции, законов страны, Трудового кодекса.

Организация может провозгласить себя свободной от любых форм насилия и дискриминации. В рамках этой философии вполне уместно и заявление о том, что организация осуществляет внимательную проверку всей информации и рекомендаций претендента при приеме на работу, чтобы не создавать угрозу для всего персонала. Ложная информация является основанием для увольнения.

Помимо внешних аспектов концепция безопасности кадрового развития содержит и важнейшие положения внутриорганизационной безопасности. Важнейшим условием успешного развития любой организации является умение защищать свои внутренние основы, поэтому концепция безопасности предусматривает выявление причин сопротивления работников корпоративным нормам, факторов угроз и кадровых рисков, наличие в организации групп риска, определение степени их влияния на персонал организации и разработку стратегии предупреждения негативных последствий такого влияния.

Исследования проблем безопасности ряда российских организаций показывают, что процент сотрудников, которые видят причину своей неуверенности в завтрашнем дне в сложившейся в компании ситуации, достаточно велик. Поэтому столь важна проработка внутренних аспектов концепции безопасности кадрового развития организации. В концепцию органично впишется положение о сохранении работником конфиденциальности информации, строгой рабочей этике и отказе от интриг, положение об отношении сотрудника к имуществу и интересам организации, о внутриорганизационной «горячей линии связи», о поведении в критических ситуациях.

Регламентирующие документы должны быть исчерпывающими. В них должна быть четко определена ответственность служащего за совершенные действия, а также за подачу заведомо ложных заявлений. Эти регламенты, как правило, являются локальными нормативными правовыми актами, содержащими важнейшие информационно-нормативные положения, принятые в организации. Обычно к ним относят порядок приема на работу, увольнения, аттестации, рассмотрения трудовых споров, виды и размер компенсаций работникам, предотвращение дискриминации, рабочее время, дисциплина труда, охрана здоровья, охрана собственности организации, охрана коммерческой тайны, этические нормы поведения, виды и условия социального страхования и т.п.

В рамках такой концепции необходимо проводить определенные мероприятия, целями которых являются устранение причин и возможностей мошенничества и неправомерных действий со стороны персонала. Службе безопасности более свойственна функция контроля, которая реализуется ею во взаимодействии с другими контролирующими и учетными подразделениями (отделом персонала, аудитом, ревизионной комиссией и др.).

Среди подобных мероприятий следует выделить следующие:

- 1) ликвидация элементов технологической политики, способствующих мошенничеству;
- 2) предупредительная работа с партнерами (клиентами, поставщиками и др.);

3) создание системы полного контроля.

Внедрение указанных мероприятий будет способствовать уменьшению числа случаев корпоративного мошенничества.

Профилактическая работа с персоналом должна вестись непрерывно. Необходимо практиковать использование различных приемов, направленных на то, чтобы линейный персонал постоянно ощущал состояние определенной «подконтрольности».

Контрольные вопросы и задания

1. Какие мероприятия в обеспечении кадровой безопасности компании при подборе и отборе персонала осуществляет служба персонала?

2. Охарактеризуйте функции службы безопасности при подборе и отборе персонала.

3. Какие основные федеральные законы входят в состав нормативно-методического обеспечения системы управления кадровой безопасностью?

4. Каковы условия безопасного для организации увольнения сотрудника?

5. Что такое лояльность персонала? Как она связана с его благонадежностью?

6. Какой уровень лояльности персонала является необходимым для эффективности и безопасности организации?

7. Как повысить лояльность персонала?

8. Охарактеризуйте виды контроля персонала. Как и когда они реализуются при обеспечении кадровой безопасности организации?

9. Каковы особенности контроля персонала в рабочем режиме?

10. Как осуществляется контроль за проблемным персоналом?

11. Охарактеризуйте методы и мероприятия по предупреждению корпоративного мошенничества.

Тестовые задания

1. Кадровая безопасность зависит от трех основных факторов:

А) найм, лояльность, контроль

Б) отбор, найм, лояльность

В) найм, лояльность, увольнение

2. Комплекс мер безопасности при приеме на работу и прогнозирование благонадежности сотрудников – это...

А) найм

Б) лояльность

В) контроль

Г) отбор

3. Рейдерский захват – это метод....

А) целенаправленного воздействия

Б) тайного принуждения

В) информационно-психологического воздействия

4. Конкурентная разведка – это метод ...
А) целенаправленного воздействия
Б) тайного принуждения
В) информационно-психологического воздействия
5. Дискриминация – это метод ...
А) целенаправленного воздействия
Б) тайного принуждения
В) информационно-психологического воздействия
6. Является ли следующее утверждение верным?
Лояльность иногда отождествляют с благонадежностью персонала
7. Принятие, положительное отношение человека к чему-то конкретному – это...
А) жизнеспособность организации
Б) благонадежность сотрудника
В) лояльность
8. Несоблюдение норм права, что преследуется законом и является результатом неблагонадежности работника – это...
А) деликвентное поведение
Б) административно-управленческое деструктивное поведение
В) дисфункциональное поведение
Г) эгоистическое, индивидуально-целевое деструктивное поведение
Д) консервативное поведение
Е) имитационное поведение
Ж) девиантное поведение
9. Некомпетентность, несоответствие занимаемой должности – это...
А) деликвентное поведение
Б) административно-управленческое деструктивное поведение
В) дисфункциональное поведение
Г) эгоистическое, индивидуально-целевое деструктивное поведение
Д) консервативное поведение
Е) имитационное поведение
Ж) девиантное поведение
10. Скрытая (тайная) нелояльность:
А) -1
Б) -2
В) 0
Г) 1
Д) 2
Е) 3
11. Лояльность на уровне поступков и действий:
А) -1
Б) -2

- В) 0
- Г) 1
- Д) 2
- Е) 3

12. С профессиональной компетентностью связана

- А) скрытая (тайная) нелояльность
- Б) демонстративная (открытая) лояльность
- В) нулевая лояльность
- Г) лояльность на уровне поступков
- Д) лояльность на уровне действий
- Е) лояльность на уровне убеждений
- Ж) лояльность на уровне внешних атрибутов

ГЛОССАРИЙ

Безопасность компьютерных сетей организации – совокупность мер по обеспечению защиты их от несанкционированного доступа в целях перехвата информации, ее искажения или уничтожения, а также вмешательства в финансовые операции.

Безопасность персонала организации – совокупность мер по обеспечению защиты сотрудников (прежде всего – руководства и высококвалифицированных специалистов) от потенциальных угроз в форме переманивания конкурентами, вербовки, шантажа, прямых угроз жизни и здоровью, покушений.

Вербовка – действия со стороны представителей конкурентов, криминальных группировок, правоохранительных органов государства, направленные на то, чтобы склонить конкретного работника к нарушению доверия со стороны работодателя, например, в форме передачи конфиденциальных сведений (в зависимости от ситуации могут осуществляться различными методами – подкупом, шантажом, угрозами).

Высоколиквидные активы – элементы имущества организации, особо привлекательные для потенциальных злоумышленников (наличные денежные, в том числе валютные, средства, золото, ликвидные ценные бумаги на предъявителя).

Гриф конфиденциальности – специальная отметка на конфиденциальных документах (базах данных), определяющая степень защиты содержащихся в них сведений.

«Двойная бухгалтерия» (сленговое выражение) – метод обмана налоговых органов и (или) собственников организации путем фальсификации бухгалтерских документов путем их дублирования с отражением в одном комплекте документов подлинных данных, а в другом – умышленно искаженных

Допуск – установленное режимом безопасности организации для конкретного сотрудника, клиента, пользователя право доступа в защищенные от несанкционированного проникновения компьютерные сети и базы данных, входа в охраняемые помещения, работы с конфиденциальными документами (дифференцируется в зависимости от степени секретности объекта защиты).

Заказ (сленговое выражение) – обращение к криминальным структурам или индивидуально действующим киллерам с целью физического устранения конкретного предпринимателя или должностного лица за фиксированное вознаграждение.

Имущественная безопасность организации – совокупность мер по обеспечению защиты имущества от угрозы насильственного (ограбление) и ненасильственного (кражи) хищения, а также повреждения или уничтожения (саботаж, терроризм).

Информационная безопасность организации – совокупность мер по обеспечению защиты конфиденциальной информации от перехвата, разглашения, искажения или уничтожения.

Информационно-аналитический отдел – структурное подразделение службы безопасности организации, основной задачей которого является сбор и анализ информации о возможных угрозах ее безопасности, а также разработка рекомендаций по защите от них.

Кадровый агрессор – организация-работодатель, кадровая стратегия которой предполагает стратегическую ориентацию на активное переманивание лучших сотрудников у конкурентов.

Канал утечки информации – конкретная форма атаки на конфиденциальную информацию в целях ее перехвата. Наиболее распространенные способы: подслушивание, перехват электромагнитных излучений, проникновение в компьютерные сети, фотографирование, хищение документов и их носителей, вывод из строя технических и программных средств информационной защиты.

Клиентская тайна – разновидность конфиденциальной информации, находящейся в распоряжении организации, разглашение которой способно нанести имущественный или неимущественный ущерб ее клиентам или партнерам по хозяйственной деятельности.

Коммерческая тайна – разновидность конфиденциальной информации, находящейся в распоряжении организации, разглашение которой способно нанести ей имущественный или неимущественный ущерб как хозяйствующему субъекту.

Конфиденциальная информация – информация, доступ к которой ограничивается в целях защиты коммерческой или клиентской тайны, а также другие сведения, разглашение которых по каким-либо причинам нежелательно для конкретной организации.

Конфиденциальная информация – информация, доступ к которой ограничивается в целях защиты коммерческой или клиентской тайны, а также другие сведения, разглашение которых по каким-либо причинам нежелательно для конкретной организации.

Коррупция сотрудников – одна из форм нарушения доверия организации – работодателя нелояльными сотрудниками, в корыстных целях (т.е. за определенное вознаграждение) совершающих действия, наносящие ему имущественный или неимущественный ущерб.

Коррупция сотрудников – одна из форм нарушения доверия организации – работодателя нелояльными сотрудниками, в корыстных целях (т.е. за определенное вознаграждение) совершающих действия, наносящие ему имущественный или неимущественный ущерб.

Кража – хищение имущества организации в ненасильственной форме.

Нелояльный сотрудник – работник организации, способный либо в собственных имущественных или неимущественных интересах, либо в силу общей безответственности нарушить доверие работодателя и нанести ущерб его безопасности.

Неорганизованная преступность – криминальная деятельность с участием индивидуально действующих злоумышленников (хакеров, взломщиков, мошенников), а также преступных групп, деятельность которых

не имеет профессионально организованного характера (например, молодежные преступные группировки).

«Несун» (сленговое выражение) – сотрудник организации, систематически совершающий мелкие хищения ее имущества.

Ограбление – хищение имущества организации в насильственной форме.

Организованная преступность – криминальная деятельность с участием организованных преступных групп, особенно опасных в силу высокого профессионализма своих членов и наличия обширных неформальных связей с коррумпированными чиновниками, а также легальным бизнесом.

Откат (сленговое выражение) – форма проявления коррупции сотрудниками организации, вознаграждение которых за соответствующие противоправные действия определяется в процентах от суммы сделки, совершающейся с их прямым или косвенным участием.

Перехват информации – получение несанкционированного доступа к конфиденциальным сведениям организации, осуществляемое с использованием различных методов компьютерного, технического и организационного характера.

Саботаж – умышленное уничтожение или повреждение нелояльным сотрудником организации ее имущества, включая электронные базы данных и деловые документы.

Саботаж – умышленное уничтожение или повреждение нелояльным сотрудником организации имущества организации.

Слив информации (сленговое выражение) – форма реализации угрозы информационной безопасности организации путем разового или систематического (регулярного) разглашения ее сотрудниками конфиденциальных сведений.

Служба безопасности – специализированное структурное подразделение организации, созданное для обеспечения ее защиты от возможных угроз (организационная структура, функции, полномочия, выделяемые ресурсы данной штабной инстанции зависят от избранного конкретной организацией варианта стратегии собственной безопасности).

Служба режима – структурное подразделение службы безопасности организации, основной задачей которого является определение внутренних норм и правил обеспечения безопасности и контроль над соблюдением их сотрудниками.

Служба физической защиты – структурное подразделение службы безопасности организации, основными задачами которого является защита должностных лиц (группа телохранителей) и имущественных комплексов.

Служба физической защиты – структурное подразделение службы безопасности организации, основными задачами которого является защита должностных лиц (группа телохранителей) и имущественных комплексов.

Стратегия адекватного ответа на угрозы – один из вариантов стратегии обеспечения кадровой безопасности организации, предполагающий возможность использования всего комплекса легитимных методов профилактики и отражения потенциальных угроз.

Стратегия пассивной защиты от угроз – один из вариантов стратегии обеспечения кадровой безопасности организации, предполагающий приоритетную ориентацию на защиту со стороны государства в лице правоохранительных и судебных органов.

Стратегия управления кадровой безопасностью – одно из направлений стратегии организации, определяющее совокупность долгосрочных целей и управленческих подходов, реализация которых обеспечивает ее защиту от угроз разглашения конфиденциальной информации, а также нанесения ей любых других форм ущерба имущественного и неимущественного характера.

Стратегия упреждающего противодействия угрозам – один из вариантов стратегии обеспечения безопасности организации, предполагающий возможность использования наиболее активных и не всегда легитимных методов профилактики и противодействия возможным угрозам.

Хакер – специалист в области компьютерных систем, способный скрытно для объекта угрозы проникать в защищенные сети и базы данных в целях последующего перехвата информации, ее повреждения или проведения незаконных финансовых операций (чаще всего – с целью хищения денежных средств).

Человеческий фактор – управленческий термин, используемый для указания на влияние на какой либо процесс или событие участвующего в нем человека или коллектива. В рамках данной дисциплины может использоваться для оценки влияния сотрудника или группы сотрудников организации на ее безопасность.

«Черный нал» (сленговое выражение) – не отражаемые в открытой системе бухгалтерского учета и налоговой отчетности организации наличные денежные средства.

Шантаж – один из методов вербовки сотрудников организации с использованием угрозы разглашения компрометирующей их информации (об уже совершенных должностных нарушениях, ранее скрытой от работодателя информации, бытовых проблемах и т.п.)

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Алавердов А.Р. Управление кадровой безопасностью организации: учебник. – Москва: Маркет ДС, 2018. – 176 с.
2. Балынская, Н.Р., Коптякова, С.В., Зиновьева, Е.Г., Дремов В.В. Управление кадровым потенциалом организации: учеб. пособие (электронный ресурс). – Магнитогорск: ФГБОУ ВО «МГТУ», 2020.
3. Духновский С.В. Кадровая безопасность организации: учебник и практикум для вузов. – Москва: Издательство Юрайт, 2020. – 245 с. – (Высшее образование). – Текст : электронный // ЭБС Юрайт [сайт]. – URL: <https://urait.ru/bcode/456040> (дата обращения: 24.07.2020).
4. Жигулин Г.П., Бузинов А.С., Шабает Р.И. Моделирование и прогнозирование информационных угроз. – Санкт-Петербург: СПб ГУ ИТМО, 2020.
5. Зиновьева Е.Г. Государственное регулирование труда: учебное пособие (электронное издание). – Магнитогорск: Изд-во Магнитогорск. гос. техн. ун-та им. Г.И. Носова, 2021.
6. Зиновьева Е.Г., Аитова Е.В. Способы мотивации персонала // Актуальные проблемы экономики, социологии и права в современных условиях: тезисы докладов 8-й Межд. научно-практ. конф. – Пятигорск: Международная академия финансовых технологий, 2010. – С. 8–11.
7. Зиновьева Е.Г., Гончарова И.А. Современная система мотивации персонала // Маркетинг: теория и практика: сб. статей Всероссийской научно-практ. конф. – Магнитогорск: Изд-во Магнитогорск. гос. техн. ун-та им. Г.И. Носова, 2012. – С. 39–43.
8. Зиновьева Е.Г., Коптякова С.В. Performance management: эффективность использования персонала // Актуальные вопросы экономики и управления: сб. материалов Межд. научно-практ. конф.; под общ. ред. Н.Р. Балынской. – Магнитогорск: Изд-во Магнитогорск. гос. техн. ун-та им. Г.И. Носова, 2019. – С. 52–57.
9. Зиновьева Е.Г., Кузнецова М.В. Разработка мероприятий по закреплению кадров в организации на основе анализа состава персонала и причин его текучести // Научное обозрение: теория и практика. – 2021. – Т. 11. – № 2 (82). – С. 576–589.
10. Зиновьева Е.Г., Кудрявцева Н.Г. Система KPI как один из способов мотивации персонала // Актуальные вопросы экономики и управления: сб. материалов Межд. научно-практ. конф.; под об. ред. Н.Р. Балынской. – Магнитогорск: Изд-во Магнитогорск. гос. техн. ун-та им. Г.И. Носова, 2019. – С. 58–64.
11. Зиновьева Е.Г., Лимарева Ю.А. Основы организации труда персонала: учебное пособие (электронное издание). – Магнитогорск: Изд-во Магнитогорск. гос. техн. ун-та им. Г.И. Носова, 2021.
12. Зиновьева Е.Г., Петунин В.И. Организационные конфликты в современных условиях // Психолого-социальная работа в современном обществе: проблемы и решения: сб. материалов Межд. научно-практ. конф. –

Санкт-Петербург: Санкт-Петербургский государственный институт психологии и социальной работы, 2012. – С. 97–99.

13. Зиновьева Е.Г., Рахимов Д.О. Планирование развития человеческих ресурсов компании // Актуальные вопросы экономики и управления: сб. материалов Межд. научно-практ. конф.; под об. ред. Н.Р. Балынской. – Магнитогорск: Изд-во Магнитогорск. гос. техн. ун-та им. Г.И. Носова, 2019. – С. 65–68.

14. Зиновьева Е.Г., Шкурко Н.С., Ефимова А.Д. Анализ региональных рынков труда (на примере Уральского федерального округа) // Экономика и предпринимательство. – 2021. – № 2 (127). – С. 461–469.

15. Зиновьева Е.Г., Усманов А.И. Анализ конфликтов в организации // Современная модель управления: проблемы и перспективы: материалы IV Всероссийской (национальной) научно-практ. конф.; под общ. ред. Н.В. Кузнецовой. – Магнитогорск: Изд-во Магнитогорск. гос. техн. ун-та им. Г.И. Носова, 2020. – С. 110–118.

16. Коптякова С.В., Зиновьева Е.Г., Шкурко Н.С. Анализ системы управления персоналом на предприятии ООО «ММК-Информсервис» // Муниципалитет: экономика и управление. – 2019. – № 2 (27). – С. 47–56.

17. Коптякова С.В., Зиновьева Е.Г. Кадровая политика государства и организации: учеб. пособие (электронный ресурс). – Магнитогорск: ФГБОУ ВО «МГТУ», 2019.

18. Коптякова С.В., Зиновьева Е.Г. Оценка экономической и социальной эффективности управления персоналом организации : учебно-метод. пособие (электронный ресурс). – Магнитогорск : ФГБОУ ВО «МГТУ», 2019.

19. Коптякова С.В., Зиновьева Е.Г. Регулирование современных социально-экономических отношений : учеб. пособие (электронный ресурс). – Магнитогорск: ФГБОУ ВО «МГТУ», 2019.

20. Кузнецова Н.В. Кадровая безопасность организации. Сущность и механизм обеспечения. – Иркутск: Изд-во БГУЭП, 2019. – 285 с.

21. Кузнецова Н.В. Кадровая безопасность организации: сущность и механизм обеспечения: монография. – Москва : ИНФРА-М, 2019. – 286 с. – Текст : электронный. – URL: <https://znanium.com/read?id=347708>

22. Любавская Л.М., Беляйкин Д.В. Кадровая безопасность как фактор конкурентоспособности в сфере банковского предпринимательства: учеб. пособие. – Новосибирск: НФ РГТЭУ, 2018.

23. Махмудова И.Н. Кадровая безопасность: методы воздействия на персонал. В 2 ч. Ч.1. Принуждение и противодействие манипуляциям: учеб. пособие. – Самара: Изд-во Самарского ун-та, 2018. – 88 с.

24. Махмудова И.Н. Кадровая безопасность: методы воздействия на персонал. В 2 ч. Ч.2. Принуждение и противодействие манипуляциям: учеб. пособие. – Самара: Изд-во Самарского ун-та, 2018. – 88 с.

25. Соломанидина Т.О., Соломанидин В.Г. Кадровая безопасность компании. – Москва, 2018.

26. Селетков С.Н. Экономическая безопасность государства: учеб. пособие. – Москва: Евразийский открытый институт, 2019. – 70 с.

27. Трудовой кодекс Российской Федерации: от 30 дек. 2001 г. № 197-ФЗ (ред. от 31.07.2016) // Справочная правовая система «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_34683/. – Текст: электронный

28. Филина Е.А., Зиновьева Е.Г. Методы мотивации персонала и их практическое применение в МП Трест «Водоканал» (МО Магнитогорск) // Инновационные, финансовые и экономические аспекты информационной экономики XXI века: сб. научных трудов Международной научно-практической конференции; под ред. В.Н. Немцева, А.Г. Васильевой. – Магнитогорск: Изд-во Магнитогорск. гос. техн. ун-та им. Г.И. Носова, 2020. – С. 93–99.

29. Хорев А.И. Горковенко Е.В. Платонова И.В. Управление кадровой безопасностью организации // Актуальные проблемы гуманитарных и естественных наук. – 2014. – № 11. – С. 181–184.

Учебное текстовое электронное издание

Зиновьева Екатерина Георгиевна

КАДРОВАЯ БЕЗОПАСНОСТЬ ОРГАНИЗАЦИИ

Учебное пособие

0,94 Мб

1 электрон. опт. диск

г. Магнитогорск, 2021 год

ФГБОУ ВО «МГТУ им. Г.И. Носова»

Адрес: 455000, Россия, Челябинская область, г. Магнитогорск,
пр. Ленина 38

ФГБОУ ВО «Магнитогорский государственный
технический университет им. Г.И. Носова»

Кафедра государственного муниципального управления и управления персоналом

Центр электронных образовательных ресурсов и
дистанционных образовательных технологий

e-mail: ceor_dot@mail.ru