МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ»

КАФЕДРА УПРАВЛЕНИЯ ПЕРСОНАЛОМ

К.А. ПРОЗОРОВСКАЯ

КАДРОВАЯ БЕЗОПАСНОСТЬ ОРГАНИЗАЦИИ

Под редакцией доктора экономических наук, профессора В.К. Потемкина

ИЗДАТЕЛЬСТВО САНКТ-ПЕТЕРБУРГСКОГО ГОСУДАРСТВЕННОГО ЭКОНОМИЧЕСКОГО УНИВЕРСИТЕТА
2018

ББК 65.291.2
П78

Прозоровская К.А.

П78 Кадровая безопасность организации / К.А. Прозоровская ; под ред. д-ра экон. наук, проф. В.К. Потемкина. – СПб. : Изд-во СПбГЭУ, 2018. – 75 с.

ISBN 978-5-7310-4358-8

Монография посвящена вопросам обеспечения безопасности организации от возможных угроз со стороны своих сотрудников и мерам по их нейтрализации.

Монография может быть полезна управленцам всех уровней, менеджерам по персоналу, сотрудникам служб безопасности, студентам, магистрантам, аспирантам направления «Управление персоналом», «Менеджмент».

The monograph examines the problem of ensuring the security of the organization against possible threats from its employees and measures to neutralize them.

The monograph can be useful to managers of all levels, personnel managers, security personnel, students, undergraduates, graduate students in the direction of «Personnel Management», «Management».

ББК 65.291.2

Рецензенты: канд. социол. наук, доцент **М.А. Петров**
канд. социол. наук, доцент **В.С. Тестова**

ISBN 978-5-7310-4358-8

Оглавление

Введение

Неотъемлемая составная часть деятельности предприятия – обеспечение безопасности, устойчивого функционирования предприятия, активного противодействия разным негативным явлениям. Наиболее опасным видом являются преступления со стороны менеджеров и работников компаний, поскольку из мировой практики известно, что большая часть материального ущерба (почти 80%) причиняют компании ее собственные сотрудники.[1] Они либо сами делают это, либо своими действиями провоцируют на это внешние силы. Сотрудникам организации легче, чем посторонним, найти доступ к активам предприятия, проще преодолеть систему охраны, защиту баз данных, узнать секреты организации и в результате нанести ей значительный вред. При этом более половины преступлений обнаруживаются случайно.

Специалисты считают, что сохранность ресурсов предприятия и его секретов на 80% зависит от правильного подбора, расстановки и воспитания кадров.[2] Это неслучайно, поскольку в системе управления предприятием подсистема обеспечения безопасности тесно связана с подсистемой управления персоналом. Поэтому кадровая безопасность – это одно из существенных направлений деятельности в сфере безопасности предприятия.

Для прояснения проблемы кадровой безопасности можно поставить следующие вопросы:

- Как понимать сам термин «кадровая безопасность»?
- Кто конкретно обеспечивает безопасность предприятия?
- Как взаимодействуют служба персонала и служба безопасности?
- Как правильно осуществить подбор персонала?
- Как обеспечить лояльность персонала?
- Как контролировать работающий персонал?

Целью монографии является ответ на эти и другие вопросы, связанные с обеспечением безопасности организации от возможных угроз со стороны персонала.

---

[1] Любавская Л.И., Беляйкин Д.В. Кадровая безопасность как фактор конкурентоспособности в сфере банковского предпринимательства: Учебное пособие. – Новосибирск: НФ РГТЭУ, 2010. С. 12.

[2]Шегельман И.Р. Кадровая безопасность: учебно-методическое пособие / И.Р. Шегельман, М.Н. Рудаков. Петрозаводск: Изд-во ПетрГУ, 2006. С. 5

Глава 1. ОПРЕДЕЛЕНИЯ КАДРОВОЙ БЕЗОПАСНОСТИ, ЕЕ СУЩНОСТЬ. ПОНЯТИЕ УГРОЗЫ

1.1. Сущность кадровой безопасности, ее объект и субъект

Федеральный закон «О безопасности» 1992 года дал следующее определение безопасности: «Безопасность – состояние защищённости жизненно важных интересов личности, общества и государства от внутренних и внешних угроз».[3]

Объектами безопасности в организации являются: персонал; финансовые средства, материальные ресурсы, технологии; информационные ресурсы (коммерческая тайна, другая информация с ограниченным доступом).[4] Объектом кадровой безопасности можно считать негативные внутренние риски и угрозы, связанные с деятельностью персонала.

Персонал является весьма специфическим ресурсом, который является одновременно и объектом безопасности и источником возможных угроз. Конкретно его специфика, в которой может быть заложена угроза, заключается в следующем:

- Уникальность личности, что затрудняет оценку, понимание конкретного человека
- Наличие интеллекта, который может быть направлен на совершение преступлений, требующих хорошего ума
- Эмоциональность, иррациональность, чувственность, субъективизм, что может привести к конфликтам, непониманию ситуации, неадекватным реакциям
- Плохо прогнозируемое поведение, непредвиденные реакции на воздействие, что затрудняет вообще процесс управления
- Трудно диагностируемый и прогнозируемый потенциал, в результате чего могут быть ошибки при найме сотрудников
- Способность к разрушению (например, порчи имущества) и саморазрушению (алкоголизму, наркомании)
- Подверженность влиянию группы, конформизм, который может способствовать совершению преступлений «за компанию»
- Наличие собственных интересов и целей, которые могут не совпадать с интересами и целями организации

---

[3] Закон “О безопасности” РФ № 2446-1 от 05 марта 1992 года (ныне утратил силу, а в новой редакции отсутствует определение безопасности) (в ред. Закона РФ от 25.12.1992 № 4235-1, Указа Президента РФ от 24.12.1993 №2288, Федеральных законов от 25.07.2002 № 116-ФЗ, от 07.03.2005 № 15-ФЗ)

[4] Рыжов Р.О. Кадровая безопасность: опыт социологической концептуализации / Инвестиции, бизнес и право: сборник научных трудов // http://www.ibl.ru/konf/151211/kadrovaja-bezopasnost.html

Основными субъектами кадровой безопасности, которые ответственны так или иначе за обеспечение безопасности организации, являются в первую очередь служба управления персоналом (менеджер по персоналу) и служба безопасности организации (менеджеры по безопасности). К ним можно еще так же добавить сотрудников информационно-аналитических отделов, системных администраторов, другой технически персонал, которых обслуживает системы коммуникаций и линии связи организации. Каждый из субъектов кадровой безопасности имеет свои полномочия и ответственность в области кадровой безопасности.

Использование социологического инструментария позволило ответить на вопрос, какое подразделение первично при работе с персоналом. Исследования, проведённые среди сотрудников органов государственной власти, свидетельствуют о существенном влиянии на работу с персоналом со стороны непосредственного руководства органа (64,3%), на втором месте отмечается служба собственной безопасности (49,8%), при этом кадровая служба как субъект управления персоналом указываются только пятой частью опрошенных.[5]

Объектом в первую очередь является персонал, причем понятие «персонал» ассоциируется с теми, кто работает в настоящее время. Но на самом деле и бывшие работники и будущие. Источником угроз могут быть не только сотрудники, работающие в настоящее время, но и бывшие работники, и будущие, а именно соискатели вакантной должности. После увольнения или непосредственно перед увольнением «обиженный» работник может предпринять действия против организации: уничтожить необходимые для работы документы, стереть нужную информацию с ПК, начать распространять клевету или негативную информацию о фирме, передавать информацию конкурентам, уводить клиентов, жаловаться в государственные органы на серые или черные схемы выплат заработной платы. В самых патологических случаях он может попытаться осуществить физическую расправу над лицами, которых он считает виновными в своих проблемах, примеры этого периодически возникают в новостях.[6]

Опрос сотрудников 100 российских компаний с оборотом от 100 млн. руб. показал, что людей часто увольняют так, что они считают себя несправедливо обиженными и на волне эмоций начинают мстить. О желании отомстить бывшему работодателю заявило три четверти участников анонимного опроса. Правда, только 2% сказали, что готовы к

---

[5] Кадровая политика и кадровая безопасность в современной России: Сборник научных трудов / Под ред. Турчинова А.И. – М.: МАКС Пресс, 2011. С. 102.

[6] Месть бывшему работодателю стала мотивом убийства в офисном центре в США // https://ria.ru/incidents/20091107/192329743.html

активным действиям и лишь 1% уже воплотил план мести в жизнь.[7] Но достаточно одного случая мести, чтобы нанести компании ущерб материальный или репутационный.

По отзывам экспертов, негативные отзывы о бывшем работодателе в социальных сетях или на сайтах, где размещаются черные списки работодателей, – один из самых популярных способов отомстить компании. 25% таких мстителей стремятся отомстить не столько компании, сколько своему руководителю персонально – они, например, размещают фотографии и контактные данные бывшего босса на сайтах знакомств. Еще 7% анонимно сообщают близким людям бывшего начальника неприятные подробности его личной жизни, о которых родственники не знают.[8] В Интернете можно найти огромное количество статей с советами и обсуждениями на тему «как отомстить бывшему работодателю».

Опасность могут представлять и соискатели вакантной должности. Например, «псевдосоикателей» засылают конкурирующие организации, криминальные структуры, хедхантеры. Но и обычные соискатели, не довольные системой отбора, могут потом оставить негативные отзывы о компании в социальных сетях.[9] Для руководителя это не праздный вопрос – с кем он будет работать через 5-10 и т.д. лет? Многие работодатели потребительски относятся к своим работникам, основное внимание уделяют лишь тем, кто трудятся на предприятии в настоящее время. Учитывая благоприятную обстановку на рынке труда для них, немногие работодатели вкладывают средства в развитие персонала, и редко кто из них заботиться о работе с теми, кто рано или поздно уходит из предприятия. Однако отношение к ушедшим работникам, особенно пенсионерам, много лет проработавшим на предприятии, сильно влияет на мотивацию работающих.

Если работник хорошо трудился много лет, но сейчас не справляется с обязанностями, лучше найти ему подходящую работу. Было бы несправедливо оставлять его на прежнем месте, но и просто так от него отделаться после стольких лет хорошей работы несправедливо. Перед стареющими работниками остаются моральные обязательства.

Какова же роль кадровой безопасности в системе экономической безопасности предприятия? Целью обеспечения экономической безопасности предприятия является достижение максимальной стабильности его функционирования, а также создание основы и перспектив роста для выполнения целей бизнеса – т.е. извлечения прибыли, вне зависимости от

---

[7] Таранин А. Как работодателям мстят обиженные сотрудники // https://www.vedomosti.ru/management/articles/2016/12/08/668700-rabotodatelyam-mstyat-sotrudniki

[8] Таранин А. Указ. соч.

[9] Кузнецова Н.В. Кадровая безопасность организации: сущность и механизм обеспечения / Н.В. Кузнецова. – Иркутск: Изд-во БГУЭП, 2013. С. 18

объективных и субъективных угрожающих факторов (негативных воздействий, факторов риска).[10]Кадровая безопасность является одной из составляющих экономической безопасности (наряду с другими – финансовой, силовой, информационной, технико-технологической, правовой, экологической). Ее иногда называют ещё «кадровой и интеллектуальной» составляющей экономической безопасности предприятия.

Сначала рассмотрим кратко основные элементы экономической безопасности предприятия:

Финансовая безопасность обеспечивает вопросы финансово-экономической состоятельности предприятия, устойчивости к банкротству, определяет параметры платежеспособности и другие финансовые характеристики. *Силовая* безопасность занимается режимами безопасности, физической охраной объектов и личной охраной руководства, противодействием криминалу, взаимодействием с правоохранительными и другими государственными органами. *Информационная* безопасность обеспечивает защиту собственной информации, проводит деловую разведку, информационно-аналитическую работу с внешними и внутренними субъектами и т.д. *Технико-технологическая* безопасность предполагает создание и использование такой технической базы, оборудования и основных средств производства, и таких технологий и бизнес-процессов, которые усиливают конкурентоспособность предприятия.

Правовая безопасность подразумевает всестороннее юридическое обеспечение деятельности предприятия, грамотную правовую работу с контрагентами и властью, решение иных правовых вопросов.[11]

Авторы определяют кадровую безопасность в зависимости от оценки места в организации как «элемент корпоративной безопасности компании или как первичную подсистему безопасности компании».[12]

Кадровая безопасность имеет характер системы, которая имеет следующие характеристики: это система стохастическая, с высоким уровнем динамики. Стохастический характер обусловлен большим количеством и сложностью поведения взаимодействующих подсистем, элементов и внешних факторов, а также недостаточным знанием законов ее поведения. Это система открытая, поскольку на нее влияют внешние по отношению к ней системы (экономическая, информационная, интеллектуальная и т.д.). Это система целезаданная, которая может быть эффективной или неэффективной. В качестве цели выступает реализация и защищенность жиз-

---

[10] Царенко Ю. Кадровая безопасность компании // «Кадровик. Кадровое делопроизводство», N 7, июль 2006 г. // http://123-job.ru/content/articles_1132/

[11] Бекряшев А. К., Белозеров ИЛ. Электронный учебник «Теневая экономика и экономическая преступность» с 115

[12] Костусенко И.И., Куракина Л.Ю. Кадровая безопасность организации: учеб. пособие. – Великий Новгород: НовГУ им. Я. Мудрого, 2015. С. 7.

ненно важных интересов всех участников социально-трудовых отношений от внешних и внутренних угроз через достижение сбалансированности интересов каждого из участников отношений.[13]

Кадровая безопасность влияет на такие частные виды безопасности, как экономическая, информационная и т.п. по той причине, что все из них обеспечиваются, прежде всего, людьми, сотрудниками, персоналом. Вся деятельность служб персонала может быть разложены на этапы (поиск, отбор, прием. адаптация и т.д., вплоть до увольнения) и на каждом этапе присутствует масса вопросов безопасности, решаемых именно сотрудниками службы кадров. Любое действие HR-менеджера по персоналу на любом этапе – это либо усиление либо ослабление безопасности компании по ее главной составляющей – кадрам.[14]

Любавская Л.И. и Беляйкин Д.В. дают следующее определение кадровой безопасности: «должная степень защищенности организации от любых угроз, связанных с ее персоналом».[15]Данные авторы отмечают, что такие угрозы имеют двухвекторный (или встречный) характер. С одной стороны персонал в лице конкретных сотрудников организации может стать объектом реализации таких распространенных угроз как переманивание конкурентами, коммерческий подкуп или шантаж, угрозы физического насилия со стороны криминала. С другой стороны предприниматели регулярно сталкиваются с угрозой нелояльного, часто – откровенно преступного поведения со стороны работников.[16]Любое направление экономической безопасности предприятия, так или иначе, связана с персоналом и его поведением, поэтому работа с людьми первична, она доминирует над всеми.

Кузнецова Н.В. дает следующее определение кадровой безопасности – это состояние системы социально-трудовых отношений, обеспечивающее возможность полной реализации и защищенность жизненно важных интересов ее участников (работодателей, работников, государственных и иных общественных институтов) от внешних и внутренних угроз через достижение сбалансированности интересов каждого и участников отношений, а также способствующее эффективному и гармоничному развитию человеческих ресурсов. В данном определении автор оперирует понятием "интерес" и подчеркивает, что организация находится в состоя-

---

[13] Кузнецова Н.В. Кадровая безопасность организации: сущность и механизм обеспечения / Н.В. Кузнецова. – Иркутск: Изд-во БГУЭП, 2013. С. 21.

[14] Кадровая политика и кадровая безопасность в современной России: Сборник научных трудов / Под ред. Турчинова А.И. – М.: МАКС Пресс, 2011. С. 102

[15] Любавская Л.И., Беляйкин Д.В. Кадровая безопасность как фактор конкурентоспособности в сфере банковского предпринимательства: Учебное пособие. – Новосибирск: НФ РГТЭУ, 2010. С. 12.

[16] Там же.

нии кадровой безопасности, если ее жизненно важные интересы гармонизированы с интересами участников социально-трудовых отношений – работников, государства, иных субъектов.[17]

Следует отметить, что полной безопасности достичь невозможно, всегда есть риски. Поэтому обеспечение кадровой безопасности – это процесс минимизации рисков, связанных с возможным негативным воздействием кадровой составляющей корпоративных ресурсов на комплексную безопасность компании.

Кадровая безопасность – это такое состояние организации, которое достигается посредством деятельности, направленной на формирование качественных и количественных характеристик кадрового потенциала, обеспечивающих достижение целей организации, отсутствие рисков экономических потерь. По сути – это защищённость организации от деструктивного профессионализма, угроз и рисков непрофессионализма, сохранения и наращивания профессионального потенциала посредством активной кадровой политики организации, грамотного руководства организацией.

Кадровая безопасность имеет отраслевую специфику. В организациях, относящихся к той или иной сфере деятельности, существенно различаются масштабы потенциальных потерь от реализации соответствующих угроз. Например, финансовые преступления со стороны собственных сотрудников в сфере крупного бизнеса всегда чреваты большим ущербом, чем на малом предприятии.[18]Приводятся данные о том, что сфера общественного питания всегда отличалась угрожающими масштабами злоупотреблений – в кафе и ресторанах объем потерь за счёт махинаций персонала составляет от 30 до 60 % выручки. По поводу работников магазина есть более резкие высказывания: «Если у работников магазина есть шанс украсть товар или деньги, они их украдут».[19]

Затем, не одинакова сама вероятность реализации любых угроз имущественной безопасности (можно сравнить торговлю и прикладную науку). В зависимости от отраслевой принадлежности организации существенно варьируется количество рабочих мест, со стороны которых могут быть реализованы угрозы информационной безопасности работодателя. Так, можно сопоставить удельный вес сотрудников-«секретоносителей» на предприятиях сферы услуг и оборонно-промышленного комплекса.[20]

---

[17] Кузнецова Н.В. Кадровая безопасность организации: сущность и механизм обеспечения / Н.В. Кузнецова. – Иркутск: Изд-во БГУЭП, 2013. С. 21-22.

[18] Любавская Л.И., Беляйкин Д.В. Кадровая безопасность как фактор конкурентоспособности в сфере банковского предпринимательства: Учебное пособие. – Новосибирск: НФ РГТЭУ, 2010. С. 14.

[19] Шегельман И.Р. Кадровая безопасность: учебно-методическое пособие / И.Р. Шегельман, М.Н. Рудаков. Петрозаводск: Изд-во ПетрГУ, 2006. С. 6

[20] Любавская Л.И., Беляйкин Д.В. Указ. соч., с. 14

Есть связь экономической преступности с объемами оборота. Самая большая доля в совокупности ущерба приходится на предприятия с большими объемами оборота. Важнейшей причиной растущей преступности многие фирмы называют возрастающую сложность деловых операций. 45% правонарушений совершалось, по полученным данным, сотрудниками фирм, 38% – деловыми партнерами и остальные – совместно обеими категориями.[21]

1.2. Виды угроз и кадровых рисков

Кадровая безопасность представляет собой процесс предотвращения угроз. Закон РФ "О безопасности от 5.03.1992 дал следующее определение угрозы: "Угроза безопасности – совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства".[22]

Угрозы в нашем случае – это негативные воздействия, отрицательно влияющие на состояние безопасности предприятия, способные привести к убыткам предприятия. Поэтому необходимо проводить постоянную работу, направленную на предотвращение угроз, вызывающих экономические потери. В таком понимании безопасность – это предотвращение убытков предприятия.

Что может угрожать предприятию? О каких угрозах, предотвращать которые должны кадровая служба, идет речь в определении понятия «кадровая безопасность»? Начнем с классификации угроз. Классификация помогает спрогнозировать воздействие угроз по времени, по объектам, по месту воздействия и т.д. Анализ и обобщение литературных данных и опыта работы ряда предприятий по управлению персоналом с целью обеспечения экономической безопасности, проведенные разными авторами, показали, что на уровне предприятия угрозы можно классифицировать следующим образом.[23]

По направлению воздействия: внутренние (персонал предприятия); внешние (конкуренты, контрагенты, злоумышленники и др.).

По возможности прогнозирования: прогнозируемые (вероятностные); непрогнозируемые (случайные).

По степени вероятности угроза оценивается как невероятная, маловероятная, вероятная, весьма вероятная и вполне вероятная.

---

[21] Шегельман И.Р. Указ. соч. С. 6

[22] Закон “О безопасности” РФ № 2446-1 от 05 марта 1992 года (в ред. Закона РФ от 25.12.1992 № 4235-1, Указа Президента РФ от 24.12.1993 №2288, Федеральных законов от 25.07.2002 № 116-ФЗ, от 07.03.2005 № 15-ФЗ) (ныне утратил силу)

[23] http://uslugi-po-zaschiteinformacii.ru/ponjatie_ugrozy_i_bezopasnosti.html

По величине возможного ущерба: незначительные (до 10% от всех средств); значительные (от 10 до 50%); фатальные (свыше 50%).

По вероятности реализации: потенциально возможные угрозы (угрозы со хедхантеров «увести» ценного работника); реально существующие (хищения).

По месту воздействия: общие (на весь объект защиты); локальные (на элемент объекта защиты).

По времени воздействия: постоянно действующие (хищения); эпизодические (сезонные потери); разовые, одномоментные (перевозка грузов).

По объекту посягательств:

1. персонал;
2. финансовые средства;
3. материальные средства;
4. информационные средства;
5. средства информатизации;
6. технические средства охраны.

По природе возникновения: геополитические (кризис); конкурентные; контрагентные; криминальные; техногенные.

Кроме последней классификации, угрозы делят по природе их возникновения на два класса:

1. естественные (объективные), т.е. вызванные стихийными природными явлениями, не зависящими от человека (наводнения, землетрясения, ураганы и т.п.);

2. искусственные (субъективные), т.е. вызванные деятельностью человека, непреднамеренные (неумышленные) и преднамеренные (умышленные) угрозы.[24]

По виновнику (субъекту) выделяют угрозы со стороны:

- конкурентов самой организации
- клиентов, бизнес-партнеров организации
- криминальных структур
- индивидуальных злоумышленников
- надзорных, контролирующих и фискальных органов государства
- собственных сотрудников

По времени выявления выделяют угрозы:

- находящиеся в стадии подготовки к реализации
- находящиеся в процессе реализации
- полностью реализованные[25]

---

[24] Мак-Мак В.П. Служба безопасности предприятия // http://www.opvodopad.ru/docs/security_school/busin/16__luzhba_bezopasnosti_predpriyatiya.pdf С. 2.

[25] Любавская Л.И., Беляйкин Д.В. Кадровая безопасность как фактор конкурентоспособности в сфере банковского предпринимательства: Учебное пособие. – Новосибирск: НФ РГТЭУ, 2010. С. 16.

Угрозы, связанные с личностью сотрудника:

- угроза жизни и здоровью владельцев предприятий и ключевых сотрудников;
- деструктивные конфликты с участием ключевых сотрудников;
- дискредитация системы управления;
- внезапное увольнение ключевого сотрудника;
- причинение вреда репутации компании;
- разглашение информации по неосторожности;
- хищения.

Угрозы, обусловленные особенностями коллектива:

- сопротивление нормам, ценностям и требованиям компании;
- имитация профессионального поведения;
- забастовка;
- массовые увольнения;
- саботаж;
- неподчинение.[26]

Потенциальные угрозы со стороны собственного персонала могут классифицироваться по причине практической реализации:

- угрозы, инициативно реализуемые по злому умыслу сотрудника;
- угрозы, сознательно реализуемые сотрудником под воздействием сторонних для организации субъектов;
- угрозы, реализуемые в силу безответственности сотрудника.[27]

Еще выделяют:

- преднамеренные и непреднамеренные со стороны лица, совершающего преступление;

- корыстные (мошенничество, кражи, грабежи, разбои, вымогательства) и некорыстные (халатность);

- технические (профессиональные) ошибки (случайные или систематические).

Напряженность угрозы отражается в двух измерениях:

- нормальная, повышенная, близкая к пределу (порог), избыточная;
- рост, стабильность или снижение.[28]

Основная причина угроз со стороны персонала – это его особая роль. Угрозы в рамках корпоративного управления возникают на почве:

---

[26] Костусенко И.И., Куракина Л.Ю. Кадровая безопасность организации: учеб. пособие. – Великий Новгород: НовГУ им. Я. Мудрого, 2015. С. 25.

[27] Любавская Л.И., Беляйкин Д.В. Кадровая безопасность как фактор конкурентоспособности в сфере банковского предпринимательства: Учебное пособие. – Новосибирск: НФ РГТЭУ, 2010. С. 17.

[28] Мак-Мак В.П. Служба безопасности предприятия // http://www.opvodopad.ru/docs/security_school/busin/16__luzhba_bezopasnosti_predpriyatiya.pdf С. 2.

- полиролевого поведения человека по отношению к ресурсам организации (владение, распоряжение, пользование);

- морально-этических установок и экономических предпочтений человека (мотивация, профессионализм);

- психики человека, т.е. свойств его личности (характер межличностных отношения, волевые качества).[29]

Любые угрозы организации обусловлены человеческим фактором (кроме природных катаклизмов и техногенных, если последние не были вызваны чей-то халатностью). Все проблемы предприятия – это проблемы управления человеческими ресурсами. Какие бы то ни были отклонения от нормы в работе организации – это не обособленные явления, с которыми надо бороться, а последствия упущений в управлении персоналом. Возникает понятие «кадровые риски» – это риски, связанные с вероятностью реализации антропогенных угроз, т.е. угроз, исходящих от людей. Учитывая, что человеческий фактор опосредует все стороны экономических отношений в организации, можно определить кадровые риски как комплексные, важнейшими их которых являются риски утраты конфиденциальной информации, коммерческие риски.[30]

Остановимся подробнее на внешних и внутренних угрозах:

Внешние угрозы – это явления или процессы, не зависящие от воли и сознания сотрудников предприятия и опосредованно влекущие нанесение ущерба. К таковым можно отнести:

- деятельность конкурентов, направленная на подрыв деловой репутации организации, на переманивание к себе самых опытных и профессионально подготовленных сотрудников, а также промышленный шпионаж;

- рейдерские захваты;

- корпоративный шантаж в отношении организации, так называемый гринмейл (от англ. greenmail, производное от green – «деньги» и blackmail – «шантаж»);

- действия физических лиц из личной неприязни к организации в целом, его руководителям или сотрудникам, направленные на причинение материального ущерба или подрыв деловой репутации;

- неправомерные действия работников государственных органов (налоговых, силовых), в том числе случаи сговора конкурентов с такими работниками с целью нанесения финансового ущерба;

- инфляция и иные макроэкономические процессы, которые могут влиять на экономическое положение организации и на заработную плату;

- давление на сотрудников предприятия извне с целью побудить их совершить неправомерные действия;

---

[29] Копейкин Г.К., Потемкин В.К. Менеджмент экономической безопасности. – СПб.: Терция, 2004. С. 83.

[30] Копейкин Г.К., Потемкин В.К. Указ. соч. С. 11.

- попадание сотрудников в различные виды внешней зависимости (например, в секты, о чем речь пойдет ниже);

- наличие работодателей, у которых условия труда лучше и к которым работники имеют возможность уйти.

Что касается последней угрозы, то служба персонала должна проводить мониторинг зарплат и обеспечивать привлекательность своей организации как работодателя. Совместно со службой безопасности необходимо отслеживать действия конкурентов, направленные на переманивание специалистов и давать советы работодателю, как это предотвратить.

К внутренним угрозам относятся умышленные или неосторожные действия, а также бездействия сотрудников, влекущие причинение ущерба:

- все виды правонарушений работников, направленные на причинение материального ущерба организации или подрыв ее деловой репутации;

- нарушения работниками трудовой дисциплины;

- ошибки персонала вследствие недостаточной квалификации сотрудников и/или несоответствие квалификации сотрудников предъявляемым к ним со стороны работодателя требованиям, из-за чего возникает ущерб как имуществу, так и деловой репутации организации);

Немногие компании имеют четкую и продуманную кадровую политику. К внутренней угрозе относится пассивная кадровая политика и в целом слабый менеджмент, который выражается в следующем:

- плохая организация труда, отсутствие системы нормирования и регламентирования, в результате чего нет ясного понимания того, что должны делать сотрудники, каковы их обязанности, где границы их ответственности, что приводит к существованию зон безответственности;

- неэффективная, несправедливая система стимулирования и мотивации, когда оплата труда слабо связана с результатами, эффективность работы не влияет на зарплату, т.е. работнику платят за время, проведенное на рабочем месте, а не за качество или квалификацию. Несправедливость приводит с желанию «добрать недоданное», «убивает» лояльность, может привести ущербу бездействием, явному или скрытому саботажу;

- высокая текучесть среди квалифицированных сотрудников (далеко не всегда квалифицированные работники уходят за лучшей долей – зарплатой. Чаще всего их переход в другие компании спровоцирован либо некорректным отношением к ним со стороны работодателя, либо отсутствием внимания к их проблемам, игнорированием их предложений и т.п.);

- ошибки при подборе персонала, а именно некачественные проверки кандидатов при приеме на работу.

Турчинов А.И. добавляет к серьезным угрозам в многонациональном обществе для полиэтнических организаций такие процессы и факторы, как:

- неинституциализированные и неконституированные кадровые процессы и отношения (например, прием на работу по принципу землячества, продвижение «своих»;

- дисбаланс в кадровом составе в системах управления, сферах профессиональной деятельности представителей различных этнических групп;

- низкий уровень знания культуры, традиций, религиозных верований этнических обществ другими служащими.[31]

1.3. Деструктивные формы поведения персонала

Перед тем, как описать опасные типы личности для организации, рассмотрим вкратце "безопасного" работника, шансы которого вовлечь в служебные злоупотребления крайне невелики. Это работник, удовлетворенный работой, должностью, взаимоотношениями с руководством, лояльность которого к работодателю находится на уровне выше среднего. Ему нравится работа и окружение, поэтому он хочет работать в организации и далее. Он осознанно относится к правилам и процедурам в организации, связанными с требованиями безопасности, понимает, почему их надо соблюдать. Отклоняющееся поведение считает для себя недопустимым, может работать и вести себя только в рамках норм.[32] Другие авторы безопасный тип личности определяют как личность, способную анализировать риски, предвидеть опасности и угрозы, зависящие и независящие от его деятельности, избегать опасности и опасные ситуации и в случае необходимости действовать рационально и со всей ответственностью и пониманием происходящего.[33]

Деструктивными формами поведения называют те форм, которые имеют отрицательные последствия, снижают эффективность деятельности групп и организаций, поскольку основным его содержанием является разрушение объектов и систем.

Разновидностей деструктивной формы поведения довольно много:

Противоправное – при несоблюдении норм права (превышение и злоупотребление в личных целях своими правами и полномочиями, невыполнение прямых обязанностей и т.п.)

Дисфункциональное – некомпетентное, человек не на своем месте. Непрофессионализм, некомпетентность приводят к ошибкам сотрудников,

---

[31] Турчинов А.И. Кадровая безопасность и глобализация // http://www.nbuv.gov.ua/old_jrn/Soc_Gum/Vcndtu/2012_58/47.htm

[32] Кузнецова Н.В. Кадровая безопасность организации: сущность и механизм обеспечения / Н.В. Кузнецова. – Иркутск: Изд-во БГУЭП, 2013. С. 54

[33] Соломанидина Т.О., Соломанидин В.Г. Кадровая безопасность компании. – М.: Изд-во «Альфа-Пресс», 2011. С. 210.

вызванных неграмотным использованием предоставленных полномочий, средств, оборудования и т.п. ресурсов, а это имеет прямое отношение к проблеме кадровой безопасности.

Отдельно от дисфункционального выделяют *имитационное* – имитирование деятельности, псевдоактивность. Феномен «имитационной деятельности» или «деятельностного дилетантизма» возникает из-за ошибок в найме, когда на работу берут сотрудников без нужных знаний и навыков**.** В таких ситуациях и возникает имитационная деятельность, когда работник только имитирует качественное выполнение обязанностей.

Руководители фирм могут интуитивно чувствовать наличие проблемы «имитационной деятельности», однако выделить ее на крупных предприятиях не всегда возможно из-за сохраняющихся иерархических структур власти в организации.

«Имитационная деятельность» (или дилетантизм) очень вредна, так как порождает необоснованные амбиции, подстегивает развитие гипертрофированного самомнения и безответственности; трансформирует ценности и интеллект в их псевдозаменители; приводит к фальсификации результатов деятельности.

Эгоистическое, индивидуально-целевое – преследование своих личных интересов в ущерб коллективным.

Групповое деструктивное поведение – групповой эгоизм и фаворитизм.

Консервативное – противоположно инновационному.

Манипулятивное – деструктивная эгоистическая форма поведения, достижение человеком целей за счет других.

Девиантное – отклоняющееся от норм, предписаний, требований дисциплины. Данный вид поведения имеет в свою очередь много разновидностей – асоциальное (пьянство на рабочем месте), аморальное (непорядочность по отношению к коллегам), криминальное (воровство, мошенничество).

Суицидное поведение – подвергают свою (и рядом находящихся людей) жизнь риску.

Нарцисстическое поведение – повышенная чувствительность к оценкам других людей, отсутствие достаточного чувства сопереживания, дистанцирование от коллектива (как следствие, неприятие его норм и требований).[34]

Аддиктивное поведение. Уход от реальности путем изменения своего психического состояния, с помощью наркотиков, алкоголя или постоянной фиксации внимания на определенных предметах или видах деятель-

[34] Соломанидина Т.О., Соломанидин В.Г. Кадровая безопасность компании. – М.: Изд-во «Альфа-Пресс», 2011. С. 8.

ности (карты, тараканьи бега), для получения интенсивных эмоций. Эти процессы управляют жизнью человека, делают его беспомощным, лишают воли. Для достижения своих целей субъект может пожертвовать, чем угодно.

Нелояльность персонала как угроза безопасности.

Конформистское поведение. Исполнение воли «авторитета», приспособленчество, не критичность, неспособность принимать решения, брать на себя ответственность.

Фанатическое поведение. Слепая приверженности 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.[35]

Я полагаю, что к ним еще можно отнести лиц с характерологическим поведением, о которых речь пойдет ниже.

К деструктивному поведению, связанному с эмоциональным насилием на работе, можно отнести так называемые моббинг и буллинг, которые по сути являются травлей сотрудника со стороны коллег, руководителей ли подчиненных (клевета, непрекращающаяся критика, запугивание, высмеивание, утаивание необходимой для работы информации, социальная изоляция и т.п.). Только буллингом принято называть преследование "один на один", т.е. оно носит индивидуальный характер, а моббингом – коллективный психологический террор в отношении работника. И тот и другой вид "психологического террора" приводит к снижению эффективности работы организации, к потерям рабочего времени, переводя трудовые отношения с объекта труда на эмоциональное содержание межличностного взаимодействия.[36] Противодействие моббингу входит в число задач по обеспечению кадровой безопасности. В число организационных причин, способствующих моббингу, относится: отсутствие обратной связи, попустительское отношение руководства к любителям интриг и закулисных игр, плохая организация информационных потоков, расплывчатые границы ответственности и служебных обязанностей, отсутствие системы кадрового продвижения, превалирование интимных и родственных связей между подчиненными и руководством.[37]

---

[35] Староверов Д. Лояльность персонала как фактор безопасности бизнеса // http://www.amulet-group.ru/page.htm?id=

[36] Асадов А. Н., Покровская Н. Н., Саядян Н. М., Спивак В. А. Этика деловых отношений: учебное пособие. – СПб: Изд-во СПбГУЭФ, 2006. С. 187.

[37] Вражнова М.Н., Терновая Л.О. Социология кадровой безопасности: Учебное пособие. – М.: Международный издательский центр "Этносоциум", 2017. С. 220.

К деструктивным формам поведения относятся и такие сравнительно «невинные» поступки, как частые перекуры, использование техники и ресурсов предприятия в своих целях, длительное «зависание» в социальных сетях в рабочее время. В сумме это может приносить значительный ущерб организации.

К деструктивным формам поведения относится сопротивление нововведениям – любые действия человека (или группы), направленные на дискредитацию, задержки или противодействие осуществлению перемен (начиная с простой критики до открытого саботажа). Эта форма поведения возникает при нововведениях из-за того, что большинство людей психологически склонно к консерватизму, не любят перемен и часто подозрительно относятся к ним. При плохой организации процесса нововведений эти подозрения могут показаться оправданными, что в следующий раз может вызвать ещё большее противодействие.

Основная причина сопротивления переменам – связанные с ними психические и эмоциональные затраты. В некоторых случаях высокие издержки эмоционально-психического характера негативно воздействуют не только на психологическое, но даже на физическое состояние работников (вызывать мигрени, скачки давления, язву желудка).

Негативные проявления со стороны персонала может носить умышленный и непреднамеренный характер.

Проявления умышленного характера:

- воровство
- мошенничество
- частичная порча или уничтожение имущества
- злоупотребление служебным положением
- продажа информации конкуренту
- нарушения установленных норм и правил, в том числе нарушения техники безопасности
- нецелевое использование ресурсов
- провоцирование конфликтов

Негативные проявление непредумышленного характера:

- утрата
- непреднамеренная порча
- нарушение законодательства или мер безопасности из-за незнания
- принятие непродуманных, ошибочных решений
- низкое качество товаров или услуг
- несвоевременное реагирование на изменение ситуации
- эмоциональные срывы, психозы
- болезнь или смерть сотрудника
- непредвиденные ситуации различного происхождения

Масштаб ущерба от негативной реализации угроз кадровой безопасности сильно варьируется. Основная часть наиболее распространенных угроз со стороны собственных сотрудников – мелкие хищения, разглашение конфиденциальных сведений о деятельности организации, которые способны нанести работодателю только ограниченный, локальный ущерб. Но в самых тяжелых случаях противоправные или нелояльные действия сотрудников способны нанести её интересам катастрофический или фатальный ущерб, вынуждающий покинуть рынок. Пример – отзыв государственной лицензии на право осуществления предпринимательской деятельности, основанием для которого стала передача сотрудником компрометирующей работодателя информации в соответствующие надзорные органы.[38]

Одними из наиболее распространенных преступлений со стороны сотрудников являются воровство и мошенничество. Отечественные специалисты приводят данные о том, что от 45 до 85 % краж в магазинах, кафе, ресторанах осуществляют не посетители, а сотрудники – продавцы, повара, официанты. Психологи утверждают, что только 10-20 % сотрудников при любых обстоятельствах сохранят верность работодателю, такой же процент сотрудников совершит кражу при первой же возможности, остальные будут действовать по обстоятельствам.[39]

С советских лет известен такой типаж как "несун" – работник предприятия, совершающий на месте работы кражи сырья, продукции и других материальных ценностей, находящихся на предприятии и принадлежащих предприятию. Этот типаж есть и на Западе, где многие сотрудники уносят с работы разные мелочи для личного использования. В английском языке мелкое воровство имеет название pilferage. Известно, что шести крупным больницам Нью-Йорка в период 1998-2000 гг. недобросовестные сотрудники нанесли ущерб на сумму более 400 тысяч долларов, вынося почти всё – от перчаток и простыней до компьютеров и медицинского оборудования. При этом их поступки зачастую не расследуются должным образом, так как руководство учреждений опасается за свою репутацию.[40]

По масштабам воровство авторы классифицируют на три типа: мелкие разовые хищения, систематические хищения среднего размера, "внутреннее предпринимательство". Первый тип экономике предприятия не наносит заметный ущерб, однако, как правильно отмечают авторы, их

---

[38] Любавская Л.И., Беляйкин Д.В. Кадровая безопасность как фактор конкурентоспособности в сфере банковского предпринимательства: Учебное пособие. – Новосибирск: НФ РГТЭУ, 2010. С. 13

[39] Шегельман И.Р. Кадровая безопасность: учебно-методическое пособие / И.Р. Шегельман, М.Н. Рудаков. Петрозаводск: Изд-во ПетрГУ, 2006. С. 5.

[40] Вражнова М.Н., Терновая Л.О. Социология кадровой безопасности: Учебное пособие. – М.: Международный издательский центр "Этносоциум", 2017. С. 223.

опасность в другом: развращение персонала и вероятность перехода привыкшего к таким хищениям человека на следующий уровень.[41] Во втором случае хищения имеют характер "прибавки к зарплате" носят систематический характер и, как правило, обеспечивают постоянный доход, в результате чего предприятию наносят существенный ущерб. Важная психологическая особенность этого типа воровства – отсутствие у ворующих чувства вины, которое подавлено такими мотивами, как "так делают все", "мне мало платят, а руководство жирует" и т.п. Наиболее опасен третий тип, когда сотрудники имеют возможность распоряжаться крупными суммами и самостоятельно принимать финансовые решения. Формально работая на организацию, такие люди создают на ее основе внутренний "частный бизнес".[42]

В Уголовном кодексе РФ в ст. 159 мошенничество определяется как хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием. В народе люди, занимающиеся мошенничеством, метко названы «кидалами», аферистами, плутами, жуликами и т.д. Их основная цель – корыстный обман. Оленев Р.Г. дает такое определение мошенничества: поведение одного, группы или общности субъектов, в котором их экономические цели (приобретение и (или) реализация их имущественных прав) достигаются не просто нарушением норм экономического поведения (что характерно для почти любого вида экономического поведения в ситуации аномии), а путем обмана или злоупотребления доверием.[43] Он же утверждал, что в абсолютном выражении экономический ущерб от мошенничеств значительно превышал в те годы производство продукции и национальный доход России.[44]

В организационном поведении выделяют шесть типов мошенничества в зависимости от субъекта мошенничества:

1. Растраты или хищение со стороны наемного работника, например, фальсификация кассовых книг и сумм на банковских счетах, фальсификация транспортных накладных, использование подставных поставщиков, искажение расходов в отчетах о командировках и т.п.

2. Мошенничество со стороны руководителей или менеджеров, например, создание параллельного бизнеса и перекачивание туда активов и средств компании. Наиболее частый обман = манипуляции с финансо-

---

[41] Соломанидина Т.О., Соломанидин В.Г. Кадровая безопасность компании. – М.: Изд-во «Альфа-Пресс», 2011. С. 10.

[42] Соломанидина Т.О., Соломанидин В.Г. Указ. соч. С. 11.

[43] Оленев Р.Г. Мошенничество как вид девиантного экономического поведения : Автореф. дис. на соиск. учен. степ. к.э.н. : Спец. 22.00.03 / С.-Петерб. гос. ун-т экономики и финансов. – СПб., 2000. С. 11.

[44] Оленев Р.Г. Указ. соч., с.8.

вой отчетностью, в которой искажаются данные о доходности и дебиторских задолженностей фирм[45].

3. Аферы с инвестициями со стороны руководителей инвестиционных компаний. Мошенничество связано с предложением инвесторам сделать инвестиции в "липовые" проекты" (пример – финансовые пирамиды), которые со временем разваливаются, принося мошенникам средства на их личные счета.

4. Мошенничество со стороны поставщиков, например, недопоставка уже оплаченной партии, поставка товара более низкого качества.

5. Мошенничество с заказчиками или клиентами – например, получение платы за не проделанную работу, поставку ненужных вещей, не предусмотренных договором.[46]

Зарубежные сотрудники, впрочем, не лучше. Согласно данным журнала союза немецких банков «DieBank» каждое второе предприятие в Германии становится жертвой «внутренних» преступлений, таких как обман, мошенничество, сокрытие доходов.[47]

Это только часть угроз со стороны персонала, которые оказывают влияние на процессы внутри предприятия, на его безопасность.

Однако деструктивными могут быть действия не только персонала в отношении работодателей, но и наоборот. "Черный менеджмент" и "черный найм" – первый означает использование фирмы менеджерами для прикрытия незаконных целей деятельности; второй – использование работодателями недобросовестных приемов по отношению к нанимаемым сотрудникам, чаще всего выражаясь в невыполнении работодателями заявленных обязательств.[48] Как указывает Кузнецова Н.В., наибольший ущерб интересам участников социально-трудовых отношений наносит параллельная и встречная девиация, т.е. когда установленные нормы и правила нарушаются как работником, так и работодателем, например, бесконтрактный найм, "серые" зарплаты, неуплата налогов, обман при трудоустройстве и т.п. [49] Найм без оформления трудового договора, "серые" схемы оплаты являются примером девиантных трудовых отношений, получивших название сговор – соглашение работодателя и работников, заключенное в обход действующего трудового законодательства, цель кото-

---

[45] Соломанидина Т.О., Соломанидин В.Г. Кадровая безопасность компании. – М.: Изд-во «Альфа-Пресс», 2011. С. 9.

[46] Соломанидина Т.О., Соломанидин В.Г. Указ. соч. С. 9.

[47] Шегельман И.Р. Кадровая безопасность: учебно-методическое пособие / И.Р. Шегельман, М.Н. Рудаков. Петрозаводск: Изд-во ПетрГУ, 2006. С. 5.

[48] Вражнова М.Н., Терновая Л.О. Социология кадровой безопасности: Учебное пособие. – М.: Международный издательский центр "Этносоциум", 2017. С. 228.

[49] Кузнецова Н.В. Кадровая безопасность организации: сущность и механизм обеспечения / Н.В. Кузнецова. – Иркутск: Изд-во БГУЭП, 2013. С. 42.

рого получить материальные и иные (властные, ролевые, статусные) преимущества для сторон, участвующих в нем.[50]

Как правильно отмечает Кузнецова Н.В., демонстрация руководителем примеров деструктивного поведения зачастую не позволяет рассчитывать на иное поведение со стороны работника. Оценивая поступки высшего руководства компании, персонал выстраивает свою линию поведения, определяет рамки допустимого. Вороватый начальник вряд ли может рассчитывать на честное поведение своих подчиненных.[51]

1.4. Группы риска

Еще один аспект кадровой работы, требующий внимательного отношения – это так называемые «группы риска». Существуют несколько подходов к выделению групп риска:

1) на основании критерия положения сотрудника в компании,

2) согласно критерию личностных особенностей сотрудника,

3) в зависимости от мотивов обманывать компанию.

Первая категория включает:

- руководящий состав организации (топ-менеджмент), обладающий наиболее полной информацией о деятельности фирмы и имеющей значительные полномочия для влияния;

- вспомогательный персонал, имеющий доступ к закрытой информации (секретари, сотрудники канцелярии);

- вспомогательный персонал, обладающий знаниями об обеспечении охраны (сторожа, водители, сотрудники службы безопасности);

- сотрудники, работающие с посетителями организации;

- бывшие сотрудники.[52]

Сотрудники, имеющие доступ к конфиденциальной информации и которые умышленно или неумышленно ее распространяют за пределами компании, получили называние инсайдеры. Инсайдерская информация (англ. insider information) – существенная, публично не раскрытая служебная информация компании, в случае ее раскрытия способная повлиять на рыночную стоимость ценных бумаг компании (например, информация о готовящейся смене руководства, о слиянии компании; материалы финансовой отчетности, прогнозы, свидетельствующие о трудностях компании

---

[50] Копейкин Г.К., Потемкин В.К. Менеджмент экономической безопасности. – СПб.: Терция, 2004. С. 90.

[51] Кузнецова Н.В. Указ. соч. С. 45.

[52] Чумарин И.Г. Кадровая безопасность – представители групп риска в организации // Персонал-Микс. – 2001. – № 6.

и т.п.). Выделяют несколько типов инсайдеров, угрожающих кадровой безопасности организации:

"Буратино" – действуют из любопытства, вредят по неосторожности;

"Неуловимые мстители" – бывшие сотрудники, не смирившиеся со своим увольнением. 49,5 % уволенных согласны передать конфиденциальную информацию своему новому боссу.

"Павлики Морозовы" – имеют корыстные (реже – идейные) мотивы. Опасны тем, что используют легальные пути добычи сведения.

"Серые кардиналы" – топ-специалисты, готовы на все ради продвижения по карьерной лестнице.[53]

По мнению специалистов, борьба с инсайдерами – это новый фронт за кадровую безопасность. Есть портрет типичного инсайдера, составленного компанией Pricewatehouse-Coopers, – это мужчина в возрасте от 31 до 40 лет, имеет высшее образование, работает в фирме 3-4 года, занимает достаточно высокую должность, разбирается в информационных технологиях.[54]

Вторая категория – это группы риска согласно личным особенностям сотрудника, к ней относятся:

- лица с криминальными наклонностями;
- адепты сект и религиозных течений;
- лица, склонные к алкоголизму;
- наркоманы;
- лудоманы;
- лица с отклонениями в психике;
- носители заболеваний.[55]

Для любого предприятия крайне нежелательно присутствие в коллективе – на производстве, в органах управления организацией, в партнерских организациях – работников, которые входят или потенциально могут войти в ту или иную группу риска. Изучением зависимостей, или аддикций, занимаются сразу несколько наук (психология, социология, медицина и др.), на стыке которых образовалась новая – аддиктология, или наука о зависимостях. Аддиктивное поведение связано с желанием человека уйти от реальности путем изменения состояния своего сознания.[56]Сегодня аддиктология изучает такие зависимости, как наркотическую

---

[53] Вражнова М.Н., Терновая Л.О. Социология кадровой безопасности: Учебное пособие. – М.: Международный издательский центр "Этносоциум", 2017. С. 211.

[54] Костусенко И.И., Куракина Л.Ю. Кадровая безопасность организации: учеб. пособие. – Великий Новгород: НовГУ им. Я. Мудрого, 2015. С. 70

[55] Чумарин И.Г. Кадровая безопасность – представители групп риска в организации // Персонал-Микс. – 2001. – № 6. – С. 18-21. http://mir-diplom.ru/Kadrovaya-bezopasnostj-na-predpriyatii.html

[56] Кадровая безопасность на предприятии // http://mir-diplom.ru/Kadrovaya-bezopasnostj-na-predpriyatii.html

(включая токсикоманию), алкогольную, табачную, компьютерные, игровые (включая и компьютерные игры), трудовые зависимости, а также и экзотические – пищевые, любовные и сексуальные, а сверх того – зависимости от людей, предметов, событий и многие другие.[57] Таким образом речь идет о лицах, имеющих тот или иной вид зависимостей: наркоманы, алкоголики, игроки (гэмблеры, лудоманы), члены религиозных новообразований, сетевого маркетинга и финансовых пирамид. Хотя, как отмечает автор, в «группу риска» следует включать всех, чье поведение влечет за собой различные виды материального и нематериального ущерба.[58]

Очевидна повышенная социальная опасность таких видов зависимостей как алкогольная и наркотическая: пребывание в состоянии опьянения или похмелья в те моменты, когда требуется выполнение важных заданий или когда употребление препаратов сопряжено с риском для жизни, в том числе окружающих.

Возможные риски: перманентная угроза производственной и информационной безопасности, в том числе несчастных случаев при работе, связанной с источниками повышенной опасности; совершение преступных деяний в связи с алкоголизмом; использование материальных и финансовых ресурсов предприятия для утоления потребности в алкоголе (воровство) и т.д.[59] Добывание препарата наркоманами связано с криминальными деяниями, включая физическое насилие, высока вероятность разглашения информации, сотрудничества с третьими лицами, совершения иных противоправных деяний аддиктами этой группы ради получения дозы препарата.[60]

К группам риска относят членов религиозных новообразований (РНО), которые, став частью трудового коллектива, часто (но не всегда), будут пытаться распространить влияние своей «религии» на окружающих. Более активно такой сотрудник будет действовать, если ему прямо поставлена такая задача, либо если он является агентом влияния РНО, имеющего свои коммерческие интересы в отношении предприятия. Однако есть РНО, члены которых вовлечены внутрь только своей организации и полностью безопасны для предприятия.[61]

Повышенный экономический ущерб несут такие зависимости как патологический гэмблинг, шоппингомания. Поскольку гэмблинг (от англ.

---

[57] Слободской А.Л. Управление рисками «человеческого фактора»: учебное пособие / А.Л. Слободской. – СПб.: Типография ПГУПС, 2008. С.64.

[58] Смирнов А.В. Аддикции и кадровая безопасность / Учебное пособие.- Екатеринбург: Изд-во Урал. гос. пед. ун-та, 2009. С. 3

[59] Слободской А.Л. Управление рисками «человеческого фактора»: учебное пособие / А.Л. Слободской. – СПб.: Типография ПГУПС, 2008. С.67.

[60] Смирнов А.В. Указ. соч.. С. 9.

[61] Слободской А.Л. Указ. соч. С.66.

gambling – играние) и патологический шопинг связаны с крупными и постоянными финансовыми тратами, эти виды зависимости могут быть тесно связаны со спектром как криминальных правонарушений, так и других экономических последствий: хищения информации, мошенничество, воровство, продиктованных необходимостью покрыть карточный долг или срочно приобрести дорогую вещь; потери организации от неэффективной работы сотрудника после ночи, проведенной в казино.[62] Слободской А.Л. описывает ситуацию, как конкуренты могут сделать зависимыми игроками топ-менеджеров организаций, специально создав условия, когда начинающие игроки крупно выигрывают, а выиграв много, им уже не остановиться. Как правило, первые выигрыши тут же снова пускаются в игру и дело заканчивается серьезным и опасным проигрышем.[63]

Интернетомания по степени ухода о реальности также напоминает аналогичную тягу к наркотикам, алкоголю, азартным играм. Нахождение аддикта на сайтах или форумах, не имеющих отношения к делу, абсолютно непродуктивно для работы, и просто вредно, поскольку такие аддикты срывают производственный цикл, тормозят выполнение производственных задач и наносят прямой ущерб, включая затраты на оплату счетов за посещение сайтов в Интернете.[64]

Опросы показали, что сотрудники, которые попадают в группу риска (азартные игроки, пьяницы, недовольные или увольняющиеся) есть в каждой компании. За этими людьми отдел информационной безопасности следит пристальнее всего – например, контролирует, кто сколько времени и на каких сайтах проводит, с кем общается по почте и в соцсетях, что и кому пишет.[65]

Уход от реальности всегда сопровождается сильными эмоциональными переживаниями. В данном случае человек фактически зависит не от препарата (как наркоманы), а от эмоций. Эмоции являются составной частью зависимости, человеком очень легко управлять.

Почему следует рассматривать присутствие таких зависимых людей в организации как риск для кадровой безопасности? В данном случае риск, и не малый, заключается в следующем:

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

---

[62]Смирнов А.В. Аддикции и кадровая безопасность / Учебное пособие.- Екатеринбург: Изд-во Урал. гос. пед. ун-та, 2009. С. 10.

[63] Слободской А.Л. Управление рисками «человеческого фактора»: учебное пособие / А.Л. Слободской. – СПб.: Типография ПГУПС, 2008. С.69.

[64]Смирнов А.В. Указ. соч. С. 12

[65]Таранин А. Как работодателям мстят обиженные сотрудники // https://www.vedomosti.ru/management/articles/2016/12/08/668700-rabotodatelyam-mstyat-sotrudniki

— Попытки зависимого распространить влияние своих пристрастий на окружающих, поиск или формирование им круга единомышленников, то есть увеличение количества представителей группы риска в организации.

— Удовлетворение своих зависимостей за счет материальных ресурсов работодателя.

— Использование рабочего времени для удовлетворения своих пристрастий.

— Разрушение стабильного работоспособного коллектива (команды).

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

Авторы также выделяют группу зависимостей не прямого причинения различных видов ущерба, к которым причисляют сексуальные, любовные зависимости и зависимости отношений. Выделение этих зависимостей в отдельную группу обусловлено тем, что аддикты данной группы, как правило, не сами причиняют ущерб, а ущерб причиняется благодаря манипулированию аддиктом, использованию его положения и возможностей со стороны третьих лиц, специально использующих его зависимость. Эти третьи лица могут легко склонить его вступить в деловые отношения для осуществления задач и достижения своих целей, используя его положение и ресурсы. Зависимый человек, ради удовлетворения патологической потребности и будучи зависимым от объекта своей страсти, может совершить что угодно – подписать бумагу, совершить преступление, разгласить информацию и т.п.[66]

Турчинов добавляет еще такие типажи как «послушные умники и неумные послушники», «творцы кадровой серости», «позвоночники». Первые всегда могут по запросу субъекта управления всё что угодно «научно» обосновать, а другие бездумно и слепо выполнить любое указание. Профессиональные и нравственные люди в этой среде не задерживаются.

Не меньшую опасность представляют творцы «кадровой серости». Взойдя на вершины управленческой пирамиды, непрофессионалы создают вокруг себя такое убогое в профессиональном отношении окружение, на фоне которого они выглядят куда более или менее похожими на профессионалов.

Так называемые «позвоночники» – это земляки, друзья, родственники, клановики. Социальная солидарность этих групп людей в организациях порождает такую интимную болезнь кадровой политики как протекционизм. Он, в свою очередь, ведет к социомонополизации видов деятельности, одной из которых выступает этномонополизация.[67]

---

[66] Смирнов А.В. Аддикции и кадровая безопасность / Учебное пособие. – Екатеринбург: Изд-во Урал. гос. пед. ун-та, 2009. С. 11.

[67] Турчинов А.И. Кадровая безопасность и глобализация // http://www.nbuv.gov.ua/old_jrn/Soc_Gum/Vcndtu/2012_58/47.htm

Интересна также характеристика опасного работника – это работник, которого хотят, но не решаются уволить, поскольку он посвящен в важные секреты, может угрожать компроматом, открыто или завуалированно шантажирует работодателя, требуя отступные за свою лояльность в виде должностей и денег.[68]

1.5. Характерологическое поведение. Опасные личные качества

Среди деструктивных следует упомянуть **характерологическое поведение**, когда особенности характера, открытая демонстрация эмоций и своего психического состояния определяют трудовое поведение человека в организации.

Ряд авторов, занимающихся психотерапией и конфликтологией, называют типы «трудных людей» в организации, поведение которых не выходит за рамки поведения психически здоровых людей, однако они провоцируют своими поступками и эмоциями психологически трудные, конфликтные ситуации.

Дадим краткое описание некоторых из типов[69]:

«Взрывной ребенок» – взрывается неадекватно ситуациям, не считает нужным контролировать свои эмоции, не владеет или не хочет владеть собой. Главная особенность – эгоистичность, своими капризами и взрывами добивается своих целей, по сути, манипулирует окружающими.

«Паровой каток» – напористый, нахальный, своей агрессией давит на всех, не считает нужным считаться ни с кем, не замечает, что испортил отношения и настроение кому-то.

«Жалобщик» – постоянно ноет, жалуется, паразитирует на чужих эмоциях, ждет постоянного сочувствия и помощи. По сути, манипулирует другими на жалости.

«Вечный пессимист» – болезненные меланхолики, у которых всегда «все плохо», с неустойчивой эмоциональной сферой. Ждут только плохого, создают негативный эмоциональный фон для общения.

«Тихони», «молчуны» – крайне закрытые люди, у которых в отличие от предыдущих типов все эмоции, мысли и чувства спрятаны. Невозможно понять их отношение, мнение, намерения, что создает сложности при взаимодействии. Партнер должен догадываться, что у него на уме.

---

[68] Кузнецова Н.В. Кадровая безопасность организации: сущность и механизм обеспечения / Н.В. Кузнецова. – Иркутск: Изд-во БГУЭП, 2013. С. 54

[69] Психология менеджмента: Учебник для вузов / Под ред. Г.С. Никифорова. – 2-е изд. – СПб.: Питер, 2004. – С 465-469.

«Сверхпокладистый» – изначально очень приятный тип – со всеми соглашается, всем поддакивает, никому не возражает, всё обещает, а потом ничего не делает. Очень ненадежный в работе типаж.

«Всезнайка» – «всё знает», а потому для него не существует ничьего мнения, кроме его собственного. Считает, что всегда прав.

«Нерешительный», «стопор» – не в состоянии принять решения, все советуется и советуется. Он в самом деле нуждается в помощи.

«С ума сводящий» – крайне непоследователен в поведении, в эмоциональных реакциях. Начинает что-то, обещает, потом бросает, начинает другое, опять бросает, таким образом своим партнерам создает эмоциональное напряжение. Никогда не оправдывает надежд, с ним сложно что-то планировать.

Известна классификация характеров К. Леонгарда, основанная на оценке стиля общения человека с окружающими людьми. Не будем приводить все типы за, а только те, которые наиболее потенциально склонны к предательству организации, а именно: демонстративный тип, гипертимический, возбудимый и застревающий. Согласно исследованиям 80 % серьезных нелояльных действий совершено этими типами (крупные хищения, взятки, передача конкурентам коммерческой тайны). Лишь в 7 % случаев у виновных не выявлены психологические качества ни одного из этих типов.[70]

Демонстративный тип. Главные черты: беспредельный эгоцентризм, жажда внимания к своей особе, восхищений, почитания, сочувствия. Неизменно стремление добиваться для себя всевозможных льгот и послаблений за счет других (семьи, коллег и т.д.). Попытки его реализации идут по двум направлениям: во-первых, предпринимаются шаги с целью вызвать по отношению к своей персоне как можно больше симпатии, уважения, восхищения и т.д.; во-вторых, если не срабатывает первый способ, со стороны окружающих стимулируются чувства сострадания и сочувствия. На случай неудачи резервируется еще и третий путь – эпатаж, паясничание, нарушения дисциплины, короче – привлечение к себе внимания через негатив.[71]

Гипертимический (гипертимный) тип. Людей этого типа характеризует чрезмерная контактность, разговорчивость. У таких людей возникают эпизодические конфликты из-за недостаточно серьезного отношения к своим служебным и семейным обязанностям. Они часто сами бывают инициаторами конфликтов и обижаются, если им делают замечания по этому поводу. Представители данного типа характеризуются энергично-

---

[70] Соломанидина Т.О., Соломанидин В.Г. Кадровая безопасность компании. – М.: Изд-во «Альфа-Пресс», 2011. С. 219.

[71] Демонстративный тип // http://psylist.net/praktikum/demotip.htm

стью, потребностью в деятельности. Одновременно они легковерны, склонны к аморальным поступкам, отличаются повышенной возбудимостью. Они тяжело переносят условия строгой дисциплины, однообразную деятельность, вынужденное одиночество.

Возбудимый тип. Характеризуется низкой контактностью в общении, замедленностью вербальных и невербальных реакций. Нередко мрачные, склонны к брани и конфликтам, в которых сами выступают как активная, провоцирующая сторона. Они не уживаются в коллективе, поскольку не ищут путей к примирению, им не хватает терпимости. В эмоционально спокойном состоянии люди данного типа часто добросовестные, аккуратные. В состоянии эмоционального возбуждения бывают раздраженные, плохо контролируют свое поведение.

Застревающий тип. Представители этого типа умеренно коммуникабельны, занудны, склонны к морализации, неразговорчивы. В конфликтах выступают инициаторами, активной стороной. Пытаются достичь высоких показателей в любом деле, за которое берутся. Предъявляют высокие требования к себе. Люди этого типа чувствительны к социальной справедливости, вместе с тем они обидчивые, подозрительные, уязвимы, мстительны. Иногда, чрезмерно самоуверенны, амбициозны, ревнивы, предъявляют непомерные требования к близким и к подчиненным на работе.[72]

То, что именно лица, которых можно отнести к данным типам и их сочетаниям, оказываются потенциально более склонными к предательству, можно объяснить тем, что многие из них слишком любят деньги и материальные ценности, не отличаются стойкостью убеждений, не особенно склонны следовать принятым в обществе морально-этическим нормам, часто являются карьеристами, легкомысленны, болтливы, обидчивы, необязательны, завистливы, мстительны, неравнодушны к спиртному.[73]

И, наконец, в третью категорию – в зависимости от мотивов наносить вред организации – выделяют следующие группы риска:

- сотрудники, готовые наносить вред организации по причине личной выгоды;

- сотрудники, готовые наносить вред организации по причине эмоционального состояния (стрессы, эмоциональное истощение);

- сотрудники, готовые наносить вред организации по причинам идеологии;

---

[72] Акцентированные черты характера // http://psyznaiyka.net/view-xarakter.html?id=akcentirovannye-cherty-haraktera

[73] Соломанидина Т.О., Соломанидин В.Г. Кадровая безопасность компании. – М.: Изд-во «Альфа-Пресс», 2011. С. 219.

- сотрудники, готовые наносить вред организации по причинам воздействия со стороны руководителя;
- сотрудники, готовые наносить вред организации по причинам воздействия со стороны организации;
- сотрудники, готовые наносить вред организации по причине воздействия со стороны мира (общества) в целом.[74]

Авторы приводят личные качества, потенциально опасные:
- эмоциональное расстройство;
- неуравновешенность поведения;
- неадекватные реакции;
- повышенная конфликтность;
- разочарование в себе и своих способностях;
- отчужденность от коллег по работе;
- недовольство своим служебным положением;
- ущемленное личное самолюбие;
- желание выделиться за счет других;
- крайне эгоистическое поведение;
- отсутствие достаточного благоразумия;
- нежелание или неспособность защищать информацию;
- нечестность;
- финансовая безответственность;
- любовь к вещам, к жизни на «широкую ногу»;
- повышенная внушаемость;
- незаинтересованность в результатах труда;
- употребление наркотиков или других стимуляторов;
- отрицательное воздействие алкоголя, приводящее к болтливости, необдуманным поступкам и т.д.[75]

Однако следует помнить, что деструктивные виды поведения могут быть не столько свойством личности, но и реакцией на организационные факторы – несправедливость к себе, в частности в вопросах оплаты, авторитарный стиль управления. В таком случае простои, перекуры, мелкое воровство воспринимаются работниками как «справедливая» компенсация того, что им «недодало» руководство. По статистике, 49,5% уволенных согласны передать конфиденциальную информацию своему новому боссу.[76]

---

[74] Костусенко И.И., Куракина Л.Ю. Кадровая безопасность организации: учеб. пособие. – Великий Новгород: НовГУ им. Я. Мудрого, 2015. С. 11.
[75] Шегельман И.Р. Кадровая безопасность: учебно-методическое пособие / И.Р. Шегельман, М.Н. Рудаков. Петрозаводск: Изд-во ПетрГУ, 2006.Сс. 21, 29.
[76] Костусенко И.И., Куракина Л.Ю. Указ. соч. С. 71

1.6. Производственные стрессы и эмоциональное истощение как кадровая угроза

К деструктивным формам поведения могут привести такое часто встречающееся явление как стрессы. Под стрессом понимают комплекс физических, химических и психологических реакций человека на стрессовые факторы (стрессоры) в окружающей обстановке. Длительный стресс приводит к состоянию вялости, апатии, безнадежности, к потере контроля за ситуацией, неадекватным реакциям, в том числе агрессивного характера.

Психическое (профессиональное) выгорание – долговременная стрессовая реакция или синдром, возникающий вследствие продолжительных профессиональных стрессов средней интенсивности. **Эмоциональное истощение** – снижение эмоционального тонуса, утрата интереса к окружающему, равнодушие, могут быть вспышки агрессивных реакций, гнева, депрессии. Эмоциональному истощению наиболее подвержены профессии по типу «человек-человек» – все профессии, связанные с работой с людьми – руководители всех рангов, представители «помогающих» профессий: врачи и медперсонал (особенно психиатрических больниц), учителя, консультанты, психологи, психиатры, полицейские, представители сервисных профессий, адвокаты, страховые агенты. В «группе риска» также работники внутренних органов (тюремные надзиратели, следователи).

Люди, в течение долгого времени помогающие другим, начинают чувствовать разочарование, если не удается добиться того эффекта, которого он ожидали. Это сопровождается потерей психической энергии, приводит к психосоматической усталости (изнурению) и эмоциональному истощению. В случае с работниками органов, полицейскими, следователями эмоциональное истощение может возникнуть вследствие постоянного эмоционально сложного общения со специфическим контингентом, коим является преступный мир.

Выражается эмоциональное истощение в равнодушии к «объекту труда», неадекватных реакциях на людей, вспышках раздражения, гнева, злобы. Причем, «сгоранию» больше подвержены те, кто работает увлеченно, с особой мотивацией. *Показатели наличия стрессов в коллективе*: рост жалоб, конфликты (особенно межличностные); неадекватная реакция на предложения, замечания руководителя; немотивированный отказ от работы; рост заболеваемости, абсентизма и производственного травматизма; уменьшение производительности труда.

Признаки стресса, внутриличностного конфликта у работника:

- Заметно снижается мотивация прежде трудолюбивого и активного сотрудника.

- Работник становится критически настроенным, ворчливым по отношению ко всему, всем недоволен, часто бывает в плохом настроении, отказывается от общения.
- Реакции работника становятся неадекватными, проявляется агрессивность.
- Он делает гораздо больше ошибок, чем обычно, становится невнимательным, теряет способность сосредоточиваться.
- Сотрудник начинает нетрезвым появляется на работе, тайно или открыто пьет в рабочее время.
- Начинает в больших количествах принимать лекарства.
- Надежный, добросовестный работник начинает нарушать сроки, становится неаккуратным, учащаются случаи отсутствия на работе.

Работники в состоянии стресса или эмоционального истощения представляют угрозу организации. Во-первых, «выгоревшие» работники смотрят на организацию как на врага и психологически удаляются от нее. У них есть тенденция сводить работу к минимуму, не выполнять свои профессиональные обязанности. Во-вторых, они своим дурным настроением заражают остальных сотрудников, провоцируют конфликты. В-третьих, работники в состоянии стресса чаще получают увечья в результате несчастного случая из-за нервного напряжения. В-четвертых, такой работник может в прямом смысле слова быть опасным, если это, например, полицейский, имеющий оружие, находящийся при этом в состоянии стресса или сильного эмоционального истощения.

Причин производственного стресса много. Одним из наиболее значимых является соотношение двух факторов – ответственность и степень контроля. Стрессовой является такая работа (профессия), в которой работник при большой ответственности имеет недостаточный контроль за способами и результатами выполнения заданий. К таким можно отнести руководителей высшего ранга, которые ответственны за все происходящее в организации, но по объективным причинам не в состоянии держать под контролем все участки работы. Стресс может возникнуть также в тех случаях, когда рабочая ситуация предъявляет человеку требования выше, чем его способности и ресурсы (или человек так воспринимает ситуацию). Здесь возникает такое понятие как рабочая нагрузка. Стрессовые реакции могут возникать тогда, когда работнику приходится работать длительный период в условиях высокой рабочей нагрузки.

Есть понятие количественной (слишком большое количество работы) и качественной (работа слишком сложная) перегрузки. Есть девять различных симптомов психологической и физиологической направленности, связанных с количественной и качественной перегрузкой: отсутствие удовлетворенности трудом, трудовая напряженность, низкий уровень самооценки, агрессивность, ощущение дискомфорта, высокий уровень холе-

стерина в крови, повышение частоты сердечных сокращений, изменение КГР и увеличение дозы курения.[77]

Так же есть взаимосвязь между стрессами, рабочей нагрузкой и свободой действий: чем больше свобода действий (под которой понимают возможность саморегуляции и самоконтроля), тем меньше стресса при одинаковой нагрузке. Действие такого стрессора как рабочая нагрузка можно уменьшить при возможности выбора способов выполнения работы. Плохое психической состояние связано с ограничением возможности управлять условиями внешней среды.

Другим важным источником профессионального стресса является неуверенность. Многие типы стрессоров имеют общую черту – их воздействие сопровождается чувством неуверенности в решении поставленной задачи, в последствиях принимаемых решений, в выборе способов реагирования на возникшую ситуацию. Неуверенность, важность задачи (результата) и длительность воздействия стресс-факторов в своем сочетании определяют силу стрессовой ситуации на работе.

Чтобы смягчать удары стрессовых факторов (стрессоров), нужно уметь распознавать их заранее, научиться чувствовать стрессовую ситуацию по нарастающим признакам.

---

[77] Бодров В.А. Информационный стресс: Учебное пособие. – М.: ПЕР СЭ, 2000. – С. 133.

Глава 2. ОБЕСПЕЧЕНИЕ КАДРОВОЙ БЕЗОПАСНОСТИ

2.1. Подходы и принципы обеспечения кадровой безопасности

Важнейшие подходы к обеспечению безопасности:

- информационно-аналитическая разведывательная деятельность по выявлению и прогнозированию возможных угроз;
- контрразведывательные мероприятия по борьбе с агентурным экономическим шпионажем, предотвращение сбора конфиденциальной информации техническими средствами, а также через персонал в окружении коммерческих структур;
- обеспечение безопасности финансово-экономической деятельности от экономических преступлений, афер, мошенничества, злоупотреблений со стороны собственного персонала, партнеров, акционеров, сторонних организаций;
- режимно-административные меры по обеспечению секретности и конфиденциальности внутренней и иной коммерческой информации;
- физическая, техническая и "электронная" защита зданий и помещений коммерческих структур и их сотрудников, разработка и обеспечение контрольно-пропускных режимов, выполнение охранно-постовых и патрульно-караульных функций;
- охрана руководящих сотрудников коммерческих структур, а также лиц, прибывающих для встреч и переговоров из других городов, районов, в т.ч. из-за рубежа;
- выработка и реализация антикризисных планов деятельности коммерческих структур, предусматривающих выход из различных типовых чрезвычайных ситуаций;
- кадрово-административные, режимно-нормативные и специальные меры при подборе, проверке, подготовке, переподготовке, расстановке, увольнении персонала.[78]

Существенным и необходимым в области кадровой политики в системе государственного и муниципального управления, кадровой политики в отношении управленческих кадров в государственных предприятиях и организациях является создание технологий реализации ее важнейшего принципа – профессионализма и компетентности.

Организация и функционирование системы безопасности должны осуществляться на основе следующих принципов:

Комплексность. Она предполагает обеспечение безопасности персонала, материальных и финансовых ресурсов, информации от всех воз-

[78] Рыжов Р.О. Кадровая безопасность: опыт социологической концептуализации / Инвестиции, бизнес и право: сборник научных трудов // http://www.ibl.ru/konf/151211/kadrovaja-bezopasnost.html

можных угроз всеми доступными законными средствами и методами, в течение всего жизненного цикла и во всех режимах функционирования, а также способностью системы к развитию и совершенствованию в процессе функционирования. Каждый сотрудник должен в рамках своей компетенции участвовать в обеспечении безопасности предприятия.

Надежность. Различные зоны безопасности должны быть одинаково надежными с точки зрения вероятности реализации угрозы.

Своевременность. Способность системы носить упреждающий характер на основе анализа и прогнозирования угроз безопасности и разработке эффективных мер противодействия им. Должен быть приоритет мер предупреждения.

Непрерывность. Отсутствие перерывов в действии систем безопасности, вызванных ремонтом, заменой, профилактикой и т.д.

Законность. Разработка систем безопасности на основе существующего законодательства. Локальные правовые акты предприятия не должны противоречить законам и подзаконным актам.

Разумная достаточность. Установление приемлемого уровня безопасности, при котором вероятность и размер возможного ущерба будут сочетаться с предельно допустимыми затратами на разработку и функционирование системы безопасности. Стоимость финансовых затрат на обеспечение безопасности не должна превышать тот оптимальный уровень, при котором теряется экономический смысл их применения.

Централизация управления. Самостоятельное функционирование системы безопасности по единым организационным, функциональным и методологическим принципам.

Компетентность. Система безопасности должна создаваться и управляться лицами, имеющими профессиональную подготовку, достаточную для корректной оценки обстановки и адекватного принятия решения, в том числе в условиях повышенного риска.

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

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

Системность. Этот принцип предполагает учет всех факторов, оказывающих влияние на безопасность предприятия, включение в деятель-

ность по его обеспечению всех сотрудников подразделений, использование в этой деятельности всех сил и средств.[79]

Главными группами критериев кадровой безопасности можно назвать:

- показатели численного состава персонала и его динамики;
- показатели квалификации и интеллектуального потенциала;
- показатели эффективности использования персонала;
- показатели качества мотивационной системы.

Для всех этих показателей должны быть определены пороговые значения (по должностям, по подразделениям и в целом по предприятию), здесь неблагоприятные процессы могут быть выражены, в частности, в отклонении величин установленных контрольных показателей от пороговых в отрицательную (а в отдельных случаях в положительную) сторону и в чрезмерном увеличении амплитуды динамики установленных показателей.

2.2. Найм персонала, обеспечение безопасности при найме

2.2.1. Процедура привлечения персонала. Ошибки на данном этапе

Все эксперты сходятся во мнении о том, что обеспечение кадровой безопасности зависит от трех основных факторов: отбор персонала, лояльность и обеспечение контроля.

Начнем с привлечения и отбора персонала. На этом этапе угроза ресурсам организации состоит в приёме на работу лица, не обладающего соответствующей квалификацией, или же способного на совершение девиантных поступков, вплоть до корпоративного мошенничества, похищение конфиденциальной информации. Есть даже риск нанять шпиона недобросовестных конкурентов или рейдеров.[80]

На этапе привлечения возможны следующие ошибки, которые в конце концов приводят к тому, что привлекается «не тот» кандидат, либо вообще никто не откликается либо затраты на привлечение оказываются неадекватно высокими и т.п.:

* Нет четких требований к кандидату. Это бывает в случае, когда не проводится работа по аттестации рабочих мест, должностные инструкции устарели или не соответствуют реальности.

* Нарушения ТК в части требований к кандидатам. Наиболее частые нарушения – это гендерные и возрастные ограничения. Объявление типа:

---

[79] Мак-Мак В.П. Служба безопасности предприятия // http://www.opvodopad.ru/docs/security_school/busin/16__luzhba_bezopasnosti_predpriyatiya.pdf С.3-4

[80] Глебовский А.Ю. Кадровая безопасность: фильтры грубой и тонкой очистки // http://www.hr-journal.ru/articles/hrs/filtry-kadrovoj-bezopasnosti-Glebovskij.html

«Требуется продавец-консультант – мужчина, возраст до 35 лет» – грубое нарушение законодательства, а именно возрастная и гендерная дискриминация. Конечно, есть перечень должностей в некоторых отраслях с подобными ограничениями (например, силовые структуры, тяжелое машиностроение), но он весьма ограничен.

* «Приукрашивание» фирмы, ложные сведения о фирме, утаивание информации. Наиболее часто «приукрашиваются» зарплата и перспективы роста, утаивается информация о финансовом положении организации. Объявление типа «зарплата до 50 тысяч в месяц» может содержать подвох: такая зарплата возможна, но без единого штрафа (который начисляется за малейшие нарушения), если работать без перерывов и выходных и при прочих подобных условиях, которые в реальности невыполнимы. А реально достижимая зарплата оказывается, например, 15 тысяч. В результате подобные объявления вводят в заблуждение кандидатов и в будущем разочарованный работник, скорее всего, уволится, проработав всего пару месяцев. И всю процедуру приема придется начинать сначала.

* Неправильный выбор источников набора. Неправильный выбор может привести к тому, что будет либо излишний наплыв кандидатов и тогда будет потрачено много времени на их отбор и отсев либо, наоборот, их окажется слишком мало. Например, неэффективно искать кандидата на высокооплачиваемую должность менеджера через агентов-распространителей, раздающих объявления у выхода из метро, т.к. потенциальные кандидаты, скорее всего, в метро не ездят.

* Не учтены интересы своих работников. В коллективе, возможно, есть работники, желающие сменить поле деятельности и игнорирование их интересов приведет к разочарованию. Отсутствие перспектив профессионального роста – одна из основных причин увольнений. И не надо забывать, что приход нового работника может ухудшить морально-психологический климат. Иногда лучшей стратегией бывает распределение обязанностей освободившейся должности на других работников (с соответствующей добавкой к зарплате), а не поиск нового работника.

Далее идет этап отбора, цель которого – отобрать наиболее подходящего кандидата из резерва. Недостаток информации о кандидате может привести к очень неприятным для работодателя последствиям, поэтому очень важная процедура на данном этапе – прохождение кандидатом фильтра (сита) отбора. Для специалистов разных рангов эти фильтры будут различными, но в целом, чем тщательнее изучен кандидат не только с позиции его профессионализма, но и с точки зрения корпоративной безопасности, тем меньше вероятность проникновения в компанию лиц с деструктивными намерениями.[81] Для этого необходимо собрать информацию о кандидатах.

---

[81] Глебовский А.Ю. Кадровая безопасность: фильтры грубой и тонкой очистки // http://www.hr-journal.ru/articles/hrs/filtry-kadrovoj-bezopasnosti-Glebovskij.html

Основные методы сбора информации, требующейся для принятия решения при отборе: анализ документов (анкетных данных, трудовых книжек, рекомендаций, характеристик); собеседование, отборочные испытания; наведение справок.

Начинается процесс с анализа документов, который нужен для сравнительной оценки уровня квалификации кандидатов. *Недостатки метода*: содержит факты из прошлого и трудно оценить потенциал и состояние человека сегодня. Здесь встречается такая крайность, особенно характерная для предприятий с высокой текучестью кадров, когда кандидатов совсем дополнительно не проверяют, веря их словам и записям в трудовой книжке. Логика менеджеров по персоналу в подобных ситуациях такая: зачем утруждать себя, если есть испытательный срок, а если человек не справится, то через небольшой срок всё равно придётся искать замену.[82]

2.2.2. Меры безопасности при найме на работу

Оценка соискателя в процессе собеседования

Собеседования бывают разных видов:

1. *Биографическое собеседование* строится вокруг фактов из жизни. Ограниченность метода – трудно оценить способности, потенциал и мотивацию кандидата. Достоинство в том, что задавая кандидату вопросы, ответы на которые противоречат друг другу, можно выявить ложь, о чем более подробно будет сказано ниже.

2. *Ситуационное собеседование*. Кандидату предлагается решить одну или несколько проблем (практических ситуаций), связанных с будущей деятельностью. Оценивается как результат, так и методы, с помощью которых кандидат находит решение. Способности кандидата, интеллект можно определить по сложности задач, которые человек решает и по способности человека связно, грамотно выражать свои мысли.

В ходе собеседования представитель организации должен ответить на два вопроса: 1) может ли кандидат успешно работать в должности (способности кандидата); 2) будет ли кандидат успешно работать в должности (мотивация кандидата).

Следует различать между качествами, которые необходимы сразу при занятии позиции, и теми, которые можно приобрести достаточно быстро в процессе работы после назначения на должность. Оценивается также психологическая совместимость кандидата с организацией. В процессе собеседования возможна оценка кандидата по внешним данным, по невербальным сигналам, которая может выявить у него желание что-то

[82] Глебовский А.Ю. Указ. соч.

скрыть, наличие негативных качеств, в том числе аддикций (об этом будет далее).

Рекомендации, как при приеме на работу, в частности при проведении собеседования выявить недостоверность сведений со стороны кандидата, его желание что-то скрыть и откровенную ложь.

1. Вариант «поймать на противоречиях», а именно выявить противоречия в анкете и/или в ответах в процессе собеседования. В анкету (интервью) вставляют вопросы, совпадающие по сути, но разные по формулировке. Например: «опишите ваши функции, которые вы могли бы выполнять лучше всего», «какая работа была бы для вас идеальной?». Или: «как вы представляете свое будущее через 5 лет?», «какую должность вы хотели бы занять в будущем?». Если даются разные ответы, то в одном из ответов кандидат лжет.

2. Попросить рекомендацию и понаблюдать за реакцией человека. Например, спросить телефоны бывших сотрудников, начальника, которые могли бы дать характеристику личных и деловых качеств претендента. Если человек уклоняется от просьбы, то надо насторожиться и навести справки.

3. Наблюдение за невербальными сигналами. Многие жесты, движения и другие сигналы тела человека выдают ложь. Например: прикрытие рта, прикосновение ко рту, носу, потирание глаз, почесывание носа; отведение взгляда или частые моргания; нервные неконтролируемые движения (например, человек внезапно начинает поправлять одежду, прическу, смахивать что-то, переставлять мелкие предметы). [83]

4. Изменение речи также свидетельствует о лжи: хрипота и покашливание (ложь создает горловой мышечный спазм); повышение тембра голоса (голос высокого тембра идет от головы, от ума, а голос низкого тембра – от сердца, от чувств. Если человек прилагает усилия для построения фразы, его голос повышается, что может быть признаком неискренность).

5. Еще признак – неоконченные фразы. Человек недоговаривает некоторые фразы и делает после этого паузы. Это свидетельствует о внутреннем столкновении с препятствием в виде информации, которую хотели бы скрыть.[84]

6. Наконец, могут быть противоречия между анкетными данными и какими-то личными свойствами кандидата. Например, «красный» диплом, а речь – примитивная, человек не способен грамотно выражать свои мыс-

---

[83] Подробно об этом написано в многократно переиздававшемся бестселлере Аллана Пиза «Язык телодвижений: Как читать мысли окружающих по их жестам». Пер. с англ.

[84] Копейкин Г.К., Потемкин В.К. Менеджмент экономической безопасности. – СПб.: Терция, 2004. С. 85.

ли. В данном случае можно подозревать, что либо диплом фальшивый, либо оценки этот студент получал не за знания (и то и другое, к сожалению, иногда случается).

Смирнов А.В. предлагает учитывать следующие признаки при выявлении негативных качеств соискателя:

1. Внешний вид, по которому можно судить о некоторых видах зависимостей, например, алкогольной – сизый нос с раздутыми порами. Неопрятный стиль одежды, татуировки могут говорить о принадлежности к андеграундной культуре. Данный метод диагностики способен выявить примерно 43% зависимостей, а эффективность такого метода приближается к 50%.[85] У наркоманов со «стажем» внешние признаки: часто неряшливый вид, сухие волосы, отекшие кисти рук; осанка чаще всего сутулая; периодические уходы с рабочего места, после которых появляются отклонения в поведении. Слободской А.Л. при этом отмечает, что эти внешние признаки не подходят к опознанию наркоманов с небольшим стажем.[86]

2. Мимика, позы, жесты. Этим способом можно выявить наркомана под дозой, компьютерную, зависимость, лудоманию, адренолиноманию. У наркоманов неуклюжие и замедленные движения при отсутствии запаха алкоголя; признаки потери контроля над собой. Напряженная поза, наличие напряжения в руке могут указывать на компьютерного геймера. Данный метод диагностики способен выявить примерно 50% зависимостей, а эффективность такого метода также приближается к 50%.[87]

3. Речь (жаргон, речевые обороты, ритм речи, словарный запас, умение излагать и строить мысли). У наркоманов невнятная, «растянутая» речь; раздражительность, резкость и непочтительность в ответах на вопросы. У аддиктов формируется определенное реагирование при взаимодействии с внешней средой в виде специфики речевых оборотов, темпа речи, формирования жаргона. Этим методом можно выявить те же зависимости: компьютерную зависимость, лудоманию, адренолиноманию, а эффективность его такая же, как и в предыдущем случае.

4. Проверка предоставляемых документов и заполнение анкет. Здесь важно проводить соотношение информации из предоставляемых документов кандидата и анкет и той информации, которую он проговаривает. Рассогласование информации может указывать на факт фальсификации документов, косвенно указывать на наличие криминальной и асоциальной девиантности.

---

[85] Смирнов А.В. Аддикции и кадровая безопасность / Учебное пособие.- Екатеринбург: Изд-во Урал. гос. пед. ун-та, 2009. С. 14.

[86] Слободской А.Л. Управление рисками «человеческого фактора»: учебное пособие / А.Л. Слободской. – СПб.: Типография ПГУПС, 2008. С. 67.

[87] Смирнов А.В. Указ соч. С. 15.

У наркоманов наблюдается явное стремление избегать встреч с представителями руководства и службы безопасности. Кроме того, наркоманы знают свою уязвимость, которая заключается в том, что экспертиза может выявить факт употребления наркотиков. Поэтому, если при приеме на работу возникли соответствующие подозрения, следует попросить кандидата принести справку из наркологического диспансера. Скорее всего, он больше не придет. Если по профилю деятельности организации проводятся предварительные или периодические медицинские осмотры, следует договориться со стационаром о применении экспресс-тестов на наличие наркотиков.[88]

Наведение справок

Полезной процедурой, хотя и не без изъянов является наведение справок, которое может быть в виде письменного запроса или по телефону. Глебовский А.Ю. приводит пример – приём на работу IT-специалиста, который на собеседовании с будущим руководителем показал очень высокий уровень профессиональной подготовки. Кадровики и сотрудники службы безопасности сосредоточились только на проверке профессионализма кандидата и не обратили внимания на сомнения его прежнего работодателя в личной порядочности бывшего подчинённого. Впоследствии этот высококлассный специалист взломал личную переписку одного из собственников компании, собрал на него обширный компромат интимного свойства, а потом передал эти сведения недоброжелателям. Результатом стала атака шантажистов.[89]

Недостатком данного метода является то, что рекомендации могут быть необъективными, кроме того при наведении справок нередки случаи категорических отказов охарактеризовать бывших сотрудников на основе позиции – никому не давать никакой информации. При этом нередко идет обоснование определением персональных данных, которое даётся в ст. 3 Федерального закона от 27 июля 2006 года N 152-ФЗ «О персональных данных» (действующая редакция от 23.07.2013). В соответствии с ним персональными данными является любая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных).

Однако когда кандидат заполнил анкету, он добровольно предоставил тот объём информации о себе, который позволяет его персонифицировать (ФИО, год и место рождения, серия и номер паспорта и т. д.), в соответствии с требованиями закона «О персональных данных», дал своё письменное согласие на обработку этой информации.

---

[88] Слободской А.Л. Управление рисками «человеческого фактора»: учебное пособие / А.Л. Слободской. – СПб.: Типография ПГУПС, 2008. С.68.

[89] Глебовский А.Ю. Кадровая безопасность: фильтры грубой и тонкой очистки // http://www.hr-journal.ru/articles/hrs/filtry-kadrovoj-bezopasnosti-Glebovskij.html

Когда кадровик или сотрудник службы безопасности звонит бывшему работодателю кандидата, он не спрашивает идентификационные сведения кандидата, поскольку соискатель их сам дал, а его интересует информация: насколько профессионален работник, не является ли кандидат алкоголиком, не замечен ли он в мошенничестве и т. д. Но эта информация не относится к идентифицирующим данным**.** Эта информация относится к обстоятельствам, связанным с деловыми качествами работника, и, следовательно, её можно и нужно собирать при заключении трудового договора, получение её не противоречит федеральному закону о персональных данных и трудовому кодексу.

А раз дано такое право, то, следовательно, бывший работодатель кандидата вправе эту информацию предоставить.[90]

Алавердов А.Р. отмечает возможность применения для профилактики возможных кадровых угроз не в полной мере легитимных методов. Так, законодательство категорически не допускает использования работодателями таких методов проверки как слежка за человеком, 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. Подобные методы нельзя отнести к этичным, поскольку они предполагают вмешательство в частную жизнь, вместе с тем они не являются нелегитимными.[91]

Вопрос о том, насколько эффективен метод наведения справок. Проверка по информационным базам службы безопасности и МВД (ФСБ) может не дать результатов, если человек не совершил правонарушений, «не засветился» иным образом. Метод страдает субъективностью, оценки могут завышаться или занижаться и даже выступать как выгораживание или преднамеренный оговор. Всё зависит от отношений, которые складывались у опрашиваемого с проверяемым лицом. Кроме того, любовные и сексуальные аддикты тщательно скрывают свою зависимость даже от родственников. Таким образом, по мнению некоторых исследователей, метод наведения справок не всегда дает результаты.[92]

Сбор информации о кандидате в Интернете

Эффективный современный способ проверки соискателя – использование Интернета, а именно социальных сетей или объявлений. Случай из практики: СЭБ рекомендовала отказать в трудоустройстве кандидату, на

---

[90] Глебовский А.Ю. Указ. соч.

[91] Алавердов А.Р. Управление кадровой безопасностью организации: учебник / А.Р. Алавердов. – М.: Маркет ДС, 2008. С. 33.

[92]Смирнов А.В. Аддикции и кадровая безопасность / Учебное пособие.- Екатеринбург: Изд-во Урал. гос. пед. ун-та, 2009. С.16.

личной странице которого в соцсети было большое число фотографий с различных пьяных увеселений и «самоотчёт» о том, как он, оформив на работе больничный, неделю отдохнул в Таиланде.[93]

По адресу электронной почты и/или телефону в Интернете, который соискатель указал в анкете, может обнаружиться информация, позволяющая расширить представления о кандидате или информация, вызывающая подозрения. Глебовский А.В. приводит пример: человек устраивается на должность заведующего складом, а в сети номер его мобильного телефона привязан к объявлениям о срочной продаже автомашины, дачи и квартиры, возможно, что человек оказался в сложном материальном положении и ищет возможность ее поправить. Тогда закономерен вопрос, с какой целью он стремится трудоустроиться на складе?

Обязан ли менеджер по персоналу информировать кандидата о том, что он искал его следы в Интернете? Эта тонкость обработки персональных данных отражена в части 4 ст. 18 Закона «О персональных данных»: «Оператор освобождается от обязанности предоставить субъекту персональных данных сведения, предусмотренные частью 3 настоящей статьи, в случаях, если: <...> персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника». Интернет – общедоступный источник. Если человек выложил там информацию о себе, то он изначально предполагал, что с ней ознакомится большое число чужих ему лиц.

Проверка кандидата с использованием полиграфа

Особым способом проверки кандидата является его проверка на полиграфе (ОИП), по поводу которого есть разные мнения о его эффективности и законности применения**.**

Что касается законности, то уже выработаны правовые условия, позволяющие активно использовать полиграф на этапе кадрового отбора**.** ТК РФ предоставляет работодателю право осуществлять отбор нанимаемого на работу персонала и указывает, что «не являются дискриминацией установление различий, исключений, предпочтений, а также ограничение прав работников, которые определяются свойственными данному виду труда требованиями, установленными федеральными законами...» (ч. 3 ст. 3 ТК РФ)**.** На необходимость проведения проверки работников указывает также п. 11 ч. 1 ст. 81 ТК РФ, согласно которому работодатель вправе расторгнуть трудовой договор в случае**:** «представления работником работодателю подложных документов при заключении трудового договора»**.** Логика этой мысли законодателя говорит о том, что эта проверка может быть проведена ещё на стадии приёма на работу.

---

[93] Глебовский А.Ю. Указ. соч.

Что касается эффективности, то есть мнение, что полиграф можно обмануть. Опыт работы цитируемого автора в правоохранительных органах и службах экономической безопасности коммерческих компаний показывает, что это действительно так, однако возможно только в том случае, если «обманщик» прошёл длительную высокопрофессиональную подготовку в учебных заведениях для сотрудников органов госбезопасности.[94]

У этого метода есть ошибки, но они бывают скорее тогда, когда приглашен плохой специалист. Работа с полиграфом предъявляет к специалисту определенные требования: фундаментальные знания по психофизиологии, психологии личности, психологии мотивации, криминологии, психологии допроса и т.д. Работающий с полиграфом должен уметь выстраивать психологический портрет личности и прогнозировать ее поведение, грамотно готовить вопросы и проводить собеседование с работником.[95]

Проводить проверку на полиграфе целесообразно после того, как менеджер по персоналу или сотрудник службы безопасности провёл с кандидатом собеседование, в процессе которого могут возникнуть определённые подозрения, которыми он поделится со специалистом-полиграфологом, а тот, в свою очередь, постарается эти подозрения разрешить при помощи полиграфа).[96]

Кроме того, само по себе включение ОИП в систему проверки отбивает охоту проникнуть в компанию у лиц с деструктивными установками (промышленные шпионы, рейдеры, мошенники, наркоманы и т. д.). Да и сам факт отказа от прохождения ОИП о многом говорит кадровику и сотруднику службы безопасности.

Использование полиграфа эффективно при выявлении истинных намерений человека. Например, в случае попытки недобросовестного конкурента внедрить своего агента («подставу») в фирму с целями выведывания коммерческих секретов, составления компромата на фирму, для выявления среди работников фирмы тех, кто согласился бы тайно сотрудничать в пользу другой фирмы и др.[97]

Негативная информация о человеке, как правило, всплывает при запросе первых рекомендаций. Некоторые компании, как выяснили иссле-

---

[94] Глебовский А.Ю. Кадровая безопасность: фильтры грубой и тонкой очистки // http://www.hr-journal.ru/articles/hrs/filtry-kadrovoj-bezopasnosti-Glebovskij.html

[95] Смирнов А.В. Аддикции и кадровая безопасность / Учебное пособие.- Екатеринбург: Изд-во Урал. гос. пед. ун-та, 2009. С. 18.

[96] Глебовский А.Ю. Кадровая безопасность: фильтры грубой и тонкой очистки // http://www.hr-journal.ru/articles/hrs/filtry-kadrovoj-bezopasnosti-Glebovskij.html

[97] Шегельман И.Р. Кадровая безопасность: учебно-методическое пособие / И.Р. Шегельман, М.Н. Рудаков. Петрозаводск: Изд-во ПетрГУ, 2006. С. 22.

дователи, даже начали применять на собеседованиях тестирование на детекторе лжи, лишь бы узнать о человеке правду.[98]

Наилучшим образом истинные намерения обнаруживаются при полиграфных обследованиях для решения следующих задач:

- определение стимула к работе;
- степень принятия собственного решения человеком;
- проверка анкетных данных;
- выявление скрываемой информации общего содержания;
- проверка и подтверждение конкретной информации;
- определение источников дохода;
- определение причин ухода (увольнения с предыдущего места работы);
- выявление совершенных преступлений, противоправных действий;
- выявление совершенных нарушений в предыдущих местах работы;
- выявление незаконно хранящегося огнестрельного оружия;
- проверка кандидата на работу (работающего) на лояльность и благонадежность;
- выявление склонности к азартным играм на деньги;
- выявление алкогольной или наркотической зависимости;
- определение психоэмоционального фона, психопатических черт личности, моральных аспектов, уровня самооценки, сильных и слабых сторон опрашиваемого;
- определение общей мотивационного направленности и ценностной ориентации личности.[99]

Полиграфная методика позволяет диагностировать все виды зависимостей на уровне надежности 85-95.[100] Устройство с высокой степенью точности (до 75%) выявляет лживые ответы, кроме того использование полиграфа является намного менее трудоемкой, затратной и продолжительной по времени процедурой, нежели любые другие виды кадровых проверок.[101]

---

[98] Таранин А. Как работодателям мстят обиженные сотрудники // https://www.vedomosti.ru/management/articles/2016/12/08/668700-rabotodatelyam-mstyat-sotrudniki

[99] Шегельман И.Р. Кадровая безопасность: учебно-методическое пособие / И.Р. Шегельман, М.Н. Рудаков. Петрозаводск: Изд-во ПетрГУ, 2006. С. 22.

[100] Смирнов А.В. Аддикции и кадровая безопасность / Учебное пособие.- Екатеринбург: Изд-во Урал. гос. пед. ун-та, 2009. С. 18.

[101] Алавердов А.Р. Управление кадровой безопасностью организации: учебник / А.Р. Алавердов. – М.: Маркет ДС, 2008. С.80-81.

Отборочные испытания

Измерение способности выполнения задач. Например, демонстрация умения работать на ПК, за станком, навыки вождения и т.п. В процесс испытаний для проверки честности кандидата можно применить вариант «ловушка». Попросить продемонстрировать те навыки, которые кандидат указал в анкете (например, владение иностранным языком, знание компьютерных программ). Если в резюме человек указал «свободное владение английским», а при этом еле говорит на нем, то можно на полном основании сомневаться в достоверности и других его сведений о себе.

Психологическое тестирование. Есть много автоматизированных методик. Недостатки: высокие издержки, необходима помощь профессионалов со стороны; условность и ограниченность тестов, не дающих полного представления о человеке. Люди, хорошо справляющиеся с тестами, не всегда успешно справляются с работой. Психологическое тестирование целесообразно проводить только в тех случаях, когда соответствующие психофизиологические особенности человека не могут восполняться путем обучения. В этих случаях экономические вложения в проведение психологического отбора себя оправдывают. Многие профессионально важные качества можно развить до определенного уровня путем обучения, тренировок (например, оперативная память, концентрация внимания). Есть качества, которые невозможно развить (интуиция, способность прогнозировать).

Испытания методом моделирования ситуаций. Используются деловые игры, исполнение заданной роли. Например, имитируется собрание без председательствующего. Кандидатов оценивают по умению выступать, настойчивости, коммуникабельности. Метод дорог и применяется только крупными компаниями.

Достаточно эффективным для отсева непригодных кандидатов считается *метод «вычисления» и метод «стимулирования самоотбора*». Метод вычисления начинается с анализа работы (вакантного рабочего места). В результате исследования составляется оптимальная характеристика лица, способного занять эту должность. Перечисленные в характеристике качества в виде вопросов заносятся в подробную анкету, которая предлагается для заполнения претенденту на вакантное место. Полученные ответы позволяют дать довольно точную оценку, в какой мере претендент отвечает критериям нанимателя. В заключение проводится собеседование, ставящее главной целью уточнить, позволят ли личные качества кандидата успешно вписаться в коллектив. Второй метод: кандидат получает максимум информации о будущей вакансии и должен сопоставить требования должности со своими возможностями. Кандидат должен сам сделать вывод о собственной профпригодности.

Такие методы отбора как отборочные испытания, а также последние два названные позволяют отсеять только кандидатов, которые не подходят по профессиональным качествам, которые при этом способны себя адек-

ватно оценить. Но методы, конечно, бессильны перед дилетантами с неадекватно завышенными притязаниями, а уж тем более перед шпионами из конкурирующих организаций.

Еще одним методом диагностики является графологический, хотя существуют различные точки зрения относительно эффективности графологической диагностики. Она используется для определения трудно проверяемых с помощью собеседования качеств. Например, анализ почерка дает информацию о характере и темпераменте человека. Возможность графологической экспертизы распространяется на сферу следующих оценочных критериев:

- личностный портрет кандидата, например эгоизм, терпение, веселый нрав, холодность, чувство низкой самооценки, бесцеремонность и т.д.;
- рабочий портрет кандидата, например, умение приспосабливаться, сообразительность, выдержка, чувство долга;
- рабочие помехи, например, агрессивность, высокомерие, небрежность, нервозность и проч.[102]

В Израиле без графологического анализа почерка практически невозможно получить работу в "интеллектуально-продвинутых" сферах профессиональной деятельности. За 40 долл. любой предприниматель может проверить кандидата на честность и добросовестность. До полутора тысяч долларов стоит углубленная проверка по 160 характерным особенностям натуры человека.[103]

Смирнов А.В. утверждает, что им удалось создать валидную графологическую диагностическую методику применительно к изучению аддикций с широким спектром возможностей и коэффициентом надежности в пределах 90-92%. Исследования проводились в отношении таких зависимостей как наркомания, алкоголизм, игромания, трудоголия, аддикция отношений.[104].

2.2.3. Взаимодействие менеджеров по персоналу, руководителей и службы безопасности при найме

Служба безопасности (СБ) – подразделение, обеспечивающее или организующее безопасность компании. В большинстве компаний принято считать, что подбором и увольнением персонала должен заниматься кадровик, а служба безопасности – только безопасностью.

---

[102] Кибанов А. Я., Дуракова И. Б. Управление персоналом организации: отбор и оценка при найме, аттестация : учеб. пособие по специальностям "Менеджмент орг." и "Упр. персоналом" / А. Я. Кибанов, И. Б. Дуракова; Гос. ун-т упр. – Изд. 2-е, перераб. и доп. – М. : Экзамен, 2005. С. 125.

[103] Алавердов А.Р. Управление кадровой безопасностью организации: учебник / А.Р. Алавердов. – М.: Маркет ДС, 2008. С.82.

[104]Смирнов А.В. Аддикции и кадровая безопасность / Учебное пособие. – Екатеринбург: Изд-во Урал. гос. пед. ун-та, 2009. С. 21.

Служба персонала первична в работе с персоналом, это более важный субъект в кадровой безопасности, чем служба безопасности. На каждом этапе деятельности служб персонала (поиск, подбор, отбор, оформление на работу, адаптация, работа с кадрами, расторжение трудовых отношений) присутствует масса вопросов безопасности, которые решаются именно кадровиками. Любое действие кадровика на любом этапе может привести либо к усилению, либо к ослаблению безопасности компании по главной из ее составляющих – по кадрам.[105]

На самом деле вопросы должны решаться в тесном сотрудничестве со службой безопасности. Действия двух подразделений пересекаются на выполнении функции оценки потенциальной угрозы от деятельности работника.

Потемкин В.К. и Копейкин Г.К. утверждают, что службы безопасности сами по себе оказываются не в состоянии обеспечить надежную защиту экономических интересов организации, таких как, экономическая эффективность и финансовая устойчивость. В основе этого суждения лежат причины:

- экономическая безопасность – это многоплановое направление менеджмента, где в сферу внимания попадают все виды ресурсов предприятия, что требует участия всех служб;

- на первый план выходят функциональные и психологические отношения работников, столкновение их экономических интересов. Поэтому акцент делается на организационных и психологических аспектах экономической безопасности, что является прерогативой кадровых служб.[106]

Все авторы сходятся на том, что полноценное обеспечение кадровой безопасности предприятия возможно лишь при тесном взаимодействии всех заинтересованных служб, которое позволяет более эффективно управлять персоналом, а также регулировать и контролировать трудовую деятельность сотрудников.[107]

Служба безопасности предприятия, работая в плотном взаимодействии со службой персонала, должна использовать свои оперативные методы и средства в работе по части предварительной и попутной проверки кандидатов и сотрудников на предмет выявления личностных и деловых качеств, так или иначе влияющих на производственный процесс. Эта работа должна носить системный характер, схема взаимодействия в этом направлении должна быть прописана в определенный регламент.[108]

---

[105] Царенко Ю. Кадровая безопасность компании // «Кадровик. Кадровое делопроизводство», № 7, июль 2006 г. // http://123-job.ru/content/articles_1132/

[106] Копейкин Г.К., Потемкин В.К. Менеджмент экономической безопасности. – СПб.: Терция, 2004. С. 5.

[107] Костусенко И.И., Куракина Л.Ю. Кадровая безопасность организации: учеб. пособие. – Великий Новгород: НовГУ им. Я. Мудрого, 2015. С. 44.

[108] Рыжов Р.О. Кадровая безопасность: опыт социологической концептуализации / Инвестиции, бизнес и право: сборник научных трудов // http://www.ibl.ru/konf/151211/kadrovaja-bezopasnost.html

Служба безопасности может перестраховываться, руководствуясь установкой, что проще не взять на работу лицо, в жизни которого есть «неясные» места, чем, взяв, потом думать – что с ним делать. В результате представители служб безопасности отвергают кандидатуры только потому, что нет возможности реально проверить человека, или в другом случае желание «вывести на чистую воду» соискателя превращается в доминирующую составляющую, подменяя этим проверку его профессионализма.

Так ошибкой многих предпринимателей приводившей к краху или «закату» компании было то, что вместо поиска и подбора талантливых людей и отбора действительно профессионалов, они доверяли «последнее слово» при подборе кадров службе безопасности, роль которой, безусловно, важна, но однако не может ни подменить, ни заменить кадровую службу.[109]

Служба IT также несет ответственность за кадровую безопасность. Ее роль:

- участие в обучении персонала правилам обеспечения безопасности компьютерных сетей и баз данных

- участие в контроле над соблюдением сотрудниками организации правилам обеспечения IT-безопасности

- разработка и внедрение новых IT и иных методов, повышающих защищенность компьютерных сетей и баз данных от несанкционированного доступа и иных противоправных действий, в том числе – со стороны сотрудников организации

- выявление фактов попытки несанкционированного доступа к закрытым компьютерным сетям и базам данных со стороны сотрудников организации

- взаимодействие со службой безопасности при выявлении фактов соответствующих нарушений и должностных преступлений со стороны сотрудников организации.

Основной недостаток в процессе сбора информации о кандидате – отсутствие чётких регламентов взаимодействия между службой экономической безопасности и кадровым подразделением.

Иногда менеджер по персоналу надеется на испытательный срок, в процессе которого, как он полагает, кандидат себя проявит. Но это рискованная позиция с точки зрения корпоративной безопасности, поскольку может быть человек устроился в компанию по заданию конкурентов или рейдеров. Трёхмесячного испытательного срока ему будет достаточно для выполнения шпионских заданий или организации какой-либо диверсии типа «случайный» выход из строя сервера в самый канун участия компании в конкурсе на получение госзаказа, похищение ноу-хау и т. д.

---

[109] Царенко Ю. Кадровая безопасность компании // «Кадровик. Кадровое делопроизводство», № 7, июль 2006 г. // http://123-job.ru/content/articles_1132/

Чтобы такие ситуации свести к минимуму, достаточно разработать порядок взаимодействия со службой безопасности, распределить функции между её специалистами и работниками отдела кадров.

Суть такого взаимодействия схематично выглядит так:

1. Менеджер по персоналу собирает как можно больше сведений о кандидате – они становятся базой для последующей проверки в службе безопасности. Кадровику нужно подготовить ответы на такие вопросы службы безопасности, как:

а) Откуда появился этот кандидат (найден рекрутинговым агентством, обратился сам, рекомендован кем-то из действующих сотрудников и т. д.).

б) Какое впечатление произвёл кандидат на сотрудника службы персонала и на своего потенциального руководителя.

в) Незамечены ли у претендента попытки приукрасить информацию о себе или сообщить явно ложную.

г) Не выявлены ли признаки подделки представленных кандидатом документов.

д) Каковы перспективы кандидата в случае приёма на работу (руководящая должность после прохождения испытательного срока, работа с наличными денежными средствами, доступ к конфиденциальной информацией и т. д.).

2. Одновременно с этим будущий руководитель кандидата проверяет его профессиональные качества и убеждается в компетентности принимаемого.

3. Затем сотрудники службы безопасности законными способами проводят проверку информации о кандидате.[110]

2.2.4. Ошибки при проведении процедуры отбора

Ошибки, связанные с организацией отбора:

1. Отсутствие системы отбора («фильтра»)
2. Нет четких критериев отбора
3. Метод отбора неадекватен целям оценки
4. Спешка (горящая вакансия)

Согласно исследованиям есть ряд проблем, снижающих эффективность собеседования.

Эффект первого впечатления. Мнение большинства людей об окружающих очень часто основывается на первом впечатлении, которое складывается в первые несколько минут знакомства. В большинстве слу-

[110] Глебовский А.Ю. Кадровая безопасность: фильтры грубой и тонкой очистки // http://www.hr-journal.ru/articles/hrs/filtry-kadrovoj-bezopasnosti-Glebovskij.html

чаев интервьюеры принимают решение о кандидате в течение первых минут знакомства. *Особенно важны:* первые слова, общее поведение (страх, неуверенность, напряженность, любопытство), выражение лица, жесты, поза, тембр голоса, погрешности в одежде. Физическая привлекательность кандидата оказывает существенное влияние на мнение эксперта о соответствии кандидатов предлагаемой работе (неосознанно). Люди с хорошими внешними данными часто считаются более социально желательными, более удачливыми в работе и карьере – и мужчины, и женщины.

Гало – эффект (эффект "ореола"). Влияние на восприятие и отношение к личности специфической установки, имеющейся у оценивающего человека. Специфическая установка может возникнуть у оценивающего на основе ранее полученной информации о статусе, личных качествах, репутации человека и эта установка служит "ореолом", мешающим видеть реальные черты. Одно или несколько качеств человека воздействуют на восприятие других свойств. Это качество служит "ореолом", мешающим видеть реальные черты. Может проявляться в тенденции давать завышенную оценку под воздействием какого-либо привлекательного показателя, произведшего на оценивающего сильное впечатление, либо, наоборот, пониженную, если какие-либо отдельные качества кажутся непривлекательными.

Преждевременное заключение. Информация о человеке может настроить против него еще до личного знакомства. Чтение заявления, анкет может настроить против кандидата еще до собеседования. (Это случается очень часто – согласно исследованиям в 85% случаев). Заполненное заявление и внешний вид оказываются причиной предубеждения. Особенно сильное впечатление производит негативная информация. Мнение скорее изменится к худшему. Мы ищем подтверждение своего мнения о человеке, которое уже сложилось. Часто интервью представляет собой поиск негативной информации. Рекомендуется читать отзывы и характеристики после отборочного собеседования. Использовать заявление только для определения вопросов, которые будут задаваться.

Предубежденность. Влияние на оценку индивидуальных свойств проходящих тестирование (возраст, пол, национальность, раса и др.). Представители каких-либо социальных групп могут оцениваться ниже или выше. Особенно сильна этническая предубежденность.

Оценка по своим качествам (сравнение с собой). Есть тенденция оценивать лучше тех людей, которые похожи на нас по своим личным и деловым качествам, внешнему виду, манерам, статусу. Часто люли считают только свои деловые качества в наибольшей степени соответствующими содержанию работы и ситуации. И подбор они осуществляют с ориентацией на свои методы работы и личные свойства. Результативнее осуществляют подбор лица, обладающие способностью самокритично оценивать свои методы и личные качества.

Последовательность приема кандидатов. Это очень важная проблема. Тенденция оценивать кандидата в сравнении с лицом, с которым проводилось собеседование непосредственно перед этим (если предыдущий выглядел плохо, то этот будет выглядеть хорошо).

Необходимость в найме. Чем выше, тем критичнее оцениваются.

Риск неудачного подбора сотрудника возникает, когда в процессе поиска у кадрового агентства возникают следующие недоработки:

1. Недостаточное участие кадрового агентства при составлении заявки.
2. Профессиональные качества найденного кандидата не соответствуют требованиям, оговоренным в заявке.
3. Личные качества найденного кандидата не соответствуют требованиям, оговоренным в заявке.
4. Социально-психологические параметры найденного кандидата не соответствуют корпоративной культуре организации.
5. Мотивация кандидата основана только на материальной заинтересованности.
6. Недостаточное консультирование в составлении конкурентоспособного предложения кандидату (компенсационный пакет).
7. Недостаточная глубина поиска, рынок специалистов полностью не охвачен.
8. В процесс оценки не были выявлены стороны личности и предыдущий опыт, способные деструктивно повлиять на деятельность компании.[111]

Что касается ошибок, связанных с приемом на работу людей зависимых, то сложность выявления аддикции заключается в том, что на момент диагностики человек может не являться аддиктом, но предрасположенность к аддикции у него может быть, находится в латентном состоянии. Скрытая аддикция может начать развиваться в любое время од воздействием какого-то события (стресс, крупный выигрыш и т.п.)[112]

2.3. Контроль персонала

Контроль представляет собой комплекс мер из установленных для персонала регламентов, режимов, оценочных, контрольных и других операций, процедур безопасности, который непосредственно нацелен на со-

---

[111] Слободской А.Л. Управление рисками «человеческого фактора»: учебное пособие / А.Л. Слободской. – СПб.: Типография ПГУПС, 2008. С. 34-35.

[112] Смирнов А.В. Аддикции и кадровая безопасность / Учебное пособие. – Екатеринбург: Изд-во Урал. гос. пед. ун-та, 2009. С. 19.

блюдение установленных норм и ликвидацию возможностей причинения ущерба.[113]

Отсутствие должного внимания к контролю впоследствии приводит к тому, что приходится заботиться и тратить большие средства на ликвидацию последствий его отсутствия, на выявление и расследование обстоятельств причинения ущерба, процедуру его возмещения.[114]

По сути контроль – процесс наблюдения за работой и поведением подчиненного со стороны руководителя или специально для этого назначенных лиц. Контроль – сравнение того, что есть с тем, что должно быть (т.е. с правилами, изложенными в документах).

Кроме поведения объектами контроля со стороны службы безопасности выступают имущественное положение сотрудника, его образ жизни, новые привычки, стиль поведения, психологическое состояние и другие характеристики (в первую очередь здесь имеются ввиду ключевые сотрудники, занимающие рабочие места, наиболее опасные с позиций угрозы их вербовки). Их необъяснимое объективными причинами изменение может сигнализировать о том, что сотрудник имеет дополнительный доход от завербовавших его структур.[115]

Нормативную базу контроля составляют: Конституция РФ, Трудовой кодекс, коллективный договор, устав предприятия, Правила внутреннего трудового распорядка, Положение о дисциплине, положения и инструкции по охране труда и технике безопасности, трудовой договор, должностные инструкции, штатное расписание, графики работ (сменности), графики отпусков, другие локальные нормативные акты. Правила, разрабатываемые организацией для своих сотрудников, не должны противоречить законодательству Российской федерации, в т.ч. трудовому. Вопросы дисциплины труда регламентируются в главе 30 ТК РФ.

Основные документы, необходимые для обеспечения кадровой безопасности:

1. Положения о службе безопасности и о службе персонала
2. Должностные инструкции топ-менеджеров, возглавляющих соответствующие направления деятельности организации и всех начальников подразделений;
3. Инструкции, определяющие порядок работы с конфиденциальной информацией, правила проведения конфиденциальных переговоров;

---

[113] Рыжов Р.О. Кадровая безопасность: опыт социологической концептуализации / Инвестиции, бизнес и право: сборник научных трудов // http://www.ibl.ru/konf/151211/kadrovaja-bezopasnost.html

[114] Царенко Ю. Кадровая безопасность компании // «Кадровик. Кадровое делопроизводство», № 7, июль 2006 г. // http://123-job.ru/content/articles_1132/

[115] Алавердов А.Р. Управление кадровой безопасностью организации: учебник / А.Р. Алавердов. – М.: Маркет ДС, 2008. С. 83.

4. Инструкции, определяющие порядок работы с имущественными комплексами организации в части обеспечения их сохранности;

5. Рекомендация сотрудникам организации.[116]

Документы, непосредственно относящиеся к компетенции службы безопасности:

1. Документы, регламентирующие деятельность сотрудников в области безопасности: пропускной режим, порядок транспортировки материальных ценностей, порядок работы сотрудников с конфиденциальной информацией, порядок доступа персонала к сведениям коммерческого характера, другие регламентирующие безопасность документы, обязательство о неразглашении коммерческой тайны.

2. Дополнение к личному делу сотрудника: специальные анкеты на сотрудников; материалы расследований по личному составу; докладные, объяснительные записки, написанные самими сотрудниками; материалы, собранные на личный состав в процессе их работы; характеристики, результаты тестов, персональные рекомендации, ответы на запросы плюс запросы на сотрудника, подготовленные СБ в правоохранительные органы, госучреждения, предприятия и организации.[117]

Задачи контроля

1. Обнаружить нарушение дисциплины

Виды нарушений дисциплины: 1) неисполнение обязанностей, в том числе некачественное исполнение; 2) превышение прав, которое нарушает права и свободу других лиц; 3) сокрытие нарушений; 4) прямое неподчинение руководителю.

2. Выяснить причины нарушений

Типичные причины нарушения норм:

1) Недостатки в организации труда (например, отсутствие нормативных документов, асимметрия прав и обязанностей, двойное подчинение и т.п.).

2) Условия труда, которые способствуют нарушениям или даже вынуждают работника совершать нарушения.

3) Оплата труда не стимулирует дисциплинированную работу.

4) Бесконтрольность в процессе труда.

5) Безнаказанность работников.

6) Личная неорганизованность работника, низкие моральные и деловые качества.

7) Семейно-бытовые условия жизни человека.

---

[116] Костусенко И.И., Куракина Л.Ю. Кадровая безопасность организации: учеб. пособие. – Великий Новгород: НовГУ им. Я. Мудрого, 2015. С. 46.

[117] Кадровая безопасность на предприятии // http://uslugi-po-zaschiteinformacii.ru/voprosy_bezopasnosti_pri_kadrovom_deloproizvodstve.html

Выяснить причины необходимо для того, чтобы правильно определить пути исправления ситуации (например, устранить недостатки в организации труда, пересмотреть систему оплаты, наказать работника).

3. Создать нормы, например, правила внутреннего трудового распорядка.

4. Создание такого климата в организации, когда нарушать нормы – стыдно. Это самый сложный и длительный по времени процесс, но дает самые лучшие результаты.

Виды контроля. Тотальный контроль

Существуют разные виды контроля, в зависимости от того, что лежит в основе классификации.

1) Предварительный – до начала выполнения подчиненным работы: проверка качества правил внутреннего трудового распорядка, должностных инструкций, трудовых договоров и других нормативных документов. *Некачественная работа подчиненного может быть следствием отсутствия или плохой проработки нормативных документов.*

2) Текущий – в ходе выполнения подчиненным работы. Ведение дневника наблюдений за работником; заведение на каждого работающего информационной карточки (досье) с записями нарушений трудовой дисциплины. Досье содержит информацию конфиденциального характера. За ведение досье традиционно отвечает служба безопасности или кто-либо из заместителей руководителя. Основные цели ведения досье:

- для принятия более обоснованного управленческого решения.
- для предотвращения нарушений, краж, утечки информации.
- для более детального ознакомления руководителей со своими подчиненными, с историей их работы в компании.[118]

Текущий контроль может осуществляться как легитимными так и полулегитимными методами. К первой группе относится визуальный контроль над соблюдением сотрудниками правил обеспечения информационной, имущественной безопасности со стороны непосредственных руководителей и службы безопасности, применение камер видеонаблюдения с теми же целям и. Ко второй группе относится контроль, осуществляемый силами внештатных информаторов службы безопасности, использование скрытых от сотрудников средств видео- и аудиоконтроля, а также просмотр их электронной почты. Например, в 2006 г. Верховный суд Великобритании признал легитимной практику прослушивания работодателями телефонных разговоров сотрудников с

[118] Кадровая безопасность на предприятии // http://uslugi-po-zaschiteinformacii.ru/voprosy_bezopasnosti_pri_kadrovom_deloproizvodstve.html (дата запроса 04.06.2018)

рабочих мест в случае специального уведомления со стороны администрации.[119]

3) Заключительный – после завершения работ. Во время аттестации анализируется уровень трудовой дисциплины работника.

По объему контроль может быть *детальным* и *факторным*. Детальный контроль возникает там, где сотрудники работают «на глазах» руководителя (например, в одной комнате). Он может превратиться в мелочную опеку. Это порождает у сотрудников отрицательную реакцию на руководителя: подавленность, недовольство, агрессивность. Такая реакция сохраняется даже тогда, когда руководитель прав.

Детальный контроль приводит и к тому, что многие работники теряют самостоятельность, сомневаясь в своих способностях. Они начинают обращаться к руководителю по самым мелким вопросам, боясь решать что-либо самостоятельно. Такой контроль требует огромного напряжения сил у руководителя, и отнимает много времени.

В организации контроля важно исходить из закономерности: чем больше развито взаимодействие работников, тем более общим становится контроль. Для того, чтобы иметь представление о том, что делается вполне достаточно держать под контролем основные факторы, от которых зависят результаты в узловых видах деятельности. Это и есть факторный контроль. Для этого необходимо: определить ключевые виды деятельности; перечень возможных слабых звеньев во взаимодействии работников между собой; продумать систему наблюдения за ходом работ каждого.

Контроль управленческих решений может быть направлен на предупреждение возможных ошибок (анализ причин их возникновения), либо на поиск виновных (наказание допустивших ошибку). Если преобладает первая ориентация, то контроль развивается как упреждающий и действительно становится управленческим. Если вторая, то контроль отягощается конфликтными ситуациями. Работники тогда в большей степени заботятся о том, чтобы не быть наказанными, чем о самой работе.

Иногда руководители пытаются установить тотальный контроль за работниками, полагая, что тотальный контроль является важным фактором производительности и предотвращения нарушений. Причины тотального контроля прежде всего в личности руководителя. Тут могут быть две причины: «наслаждение властью» либо недоверие руководителя к подчиненным, когда руководитель полагает, что «без меня никто ничего не сделает».

Тотальный контроль достигается двумя способами: создается система технического слежения и система доносительства. Необходимо заметить, что затраты на такую тотальную систему контроля в 60% случаев

---

[119] Алавердов А.Р. Управление кадровой безопасностью организации: учебник / А.Р. Алавердов. – М.: Маркет ДС, 2008. С.84.

превосходят возможные потери. Но и она не дает результата. В ответ на это работники формируют четкую и хорошо отлаженную систему круговой поруки. Система доносительства формируется следующим образом: руководитель выделяет сотрудников, демонстрирующих личную преданность ему, и приближает их к себе. Для поддержания личной преданности он должен обеспечить их зависимость лично от себя, т.е. создать для них такие условия, которые они не смогут получить при их квалификации в других организациях.

При создании такой системы руководитель фактически делегирует функцию контроля над персоналом этим подчиненным, не наделяя их ответственностью, которая лежит все равно на нем, в том числе и за ошибки этих подчиненных. Постепенно руководитель оказывается зависим от доносов и бразды правления незаметно переходят к доносчикам. Таков первый негативный результат.

Второй – из организации начинают уходить работники, к которым плохо относятся доносчики (хорошо, если эти работники непрофессионалы, но чаще бывает наоборот). Третий негативный результат – в своей деятельности работники начинают ориентироваться не на работу, а на стремление угодить доносчикам, поэтому эффективность труда снижается. Четвертый – ни один доносчик не в состоянии в полной мере адекватно контролировать ни трудовые процессы, ни добросовестность работников, иначе бы они сами были руководителями, поэтому в коллективе возникают различные формы деструктивного поведения.

Поэтому доносительство – это средство контроля очень сомнительного свойства. Снимает одну проблему, но создает при этом массу других.

Правила организации контроля:

1. Контроль должен быть планомерным, всеохватывающим, комплексным, непрерывным.
2. Контроль должен учитывать необходимость индивидуального подхода к каждому сотруднику.
3. Контроль должен осуществляться на законных основаниях, не должен наносить какого-либо вреда (материального или морального) работникам.
4. Информация о сотрудниках должна постоянно пополняться сведениями, получаемыми в процессе их работы. Доступ к ней и ее использование должны быть строго регламентированы. [120]
5. Направлять контроль надо не на личность, а на рабочий процесс.
6. Контролировать лучше открыто, сотрудники должны знать, что именно контролируется.

---

[120] Виды контроля персонала // http://uslugi-po-zaschiteinformacii.ru/vidy_kontrolja_personala.html

7. Всем должна быть понятна цель контроля, он не должен быть самоцелью.
8. Контроль не должен быть тотальным, необходимо ограничиваться существенными моментами.
9. Контроль должен соответствовать характеру контролируемого процесса (не должен быть излишним или недостаточным).

На тип контроля работы персонала влияет, в частности, размер организации. Увеличивая свои размеры, организации проходят через несколько циклов. Малые организации (до 100 человек в одной фирме) применяют прямые формы контроля деятельности кадров. Менеджер или управленческий аппарат знают лично всех работников и могут контролировать их трудовую деятельность без всяких формальных структур. Когда организация достигает размеров 100 и более человек, возникает необходимость использовать формальные процедуры.

Когда в рамках одной фирмы работает от 500 до 1000 работников, контроль, как процедура, приобретает исключительное значение. Развитие получает, главным образом, выходной контроль, при котором власть передается руководителям подразделений, которые осуществляют основные производственные функции. На этом этапе можно осуществить контроль через развитие корпоративной культуры, подчеркивая важность ключевых ценностей организации. Контроль через культуру означает необходимость уделять особое внимание персоналу, его профессиональной подготовке и развитию карьеры работников.

2.4. Мониторинг персонала

Мониторинг персонала распадается на ряд направлений:

1. мониторинг эффективности (контроль за результатами работы)
2. мониторинг рабочего времени персонала (мониторинг прихода и ухода, использования рабочего времени);
3. мониторинг взаимоотношений в коллективе;
4. мониторинг удовлетворенности персонала;
5. программный мониторинг (контроль работы персонала за компьютером).

Основная цель мониторинга своих сотрудников – оптимизировать рабочий процесс и способствовать результативной работе компании.

Рассмотрим подробнее программный мониторинг. Примеры типичных офисных ситуаций, в которых полезно использование программного мониторинга персонала:

1. Сотрудника не устраивают условия работы в компании, он ищет работу, собираясь уволиться. Система мониторинга персонала может фик-

сировать посещения сайтов для трудоустройства и сообщать о них руководителю. Увольнения сотрудника можно избежать.

2. Сотрудник совмещает основную работу с дополнительной, посвящая ей своё рабочее время в офисе. Программа, осуществляющая мониторинг деятельности сотрудника, может перехватывать и сохранять письма, отправленные пользователем и список файлов и документов, с которыми он работал. Это позволит легко выявить недобросовестного сотрудника и повысить его продуктивность.

3. Сотрудник посвящает своё рабочее время разговорам с друзьями в социальных сетях, интернет-мессенджерах, по почте и скайпу. Играет в онлайн-игры, проводит время на развлекательных сайтах. Все эти способы снижения собственной продуктивности легко фиксируются специализированным программным обеспечением и в виде отчёта отправляются руководителю.

4. Сотрудник умышленно или из-за собственной небрежности создаёт угрозу информационной безопасности компании.

Раскрытие конфиденциальных данных – пожалуй, самый неприятный и потенциально опасный пример в этом списке, так как может нанести бизнесу урон совершенно непредсказуемого масштаба.[121]

Благодаря специальным функциям ПО для мониторинга персонала, позволяющим реагировать на ключевые фразы из документов (содержащих конфиденциальные данные компании) и мгновенно отправлять предупреждения руководству, ущерб от подобных инцидентов можно не только свести к минимуму, но и вовсе предотвратить.

Можно выделить ряд положительных моментов от использования подобных средств мониторинга:

- Укрепление корпоративной дисциплины
- Рост производительности труда
- Возможность более точного планирования
- Упреждение угроз информационной безопасности
- Возможность предотвращения серьёзных проблем и конфликтов в офисной среде.

Следует помнить, что наблюдение за сотрудниками при помощи компьютерных программ не должно нарушать права человека – такие, как право на неприкосновенность частной жизни и право на конфиденциальность личной корреспонденции. Меры, которые компания принимает для своей информационной безопасности, должны быть известны каждому сотруднику. Информированность позволит сотрудникам знать «правила игры» и чувствовать собственную ответственность за их соблюдение.

---

[121] Мониторинг персонала // https://www.mipko.ru/monitoring-personala

Какова польза и заинтересованность разных служб при применении программного мониторинга?

Руководитель с помощью подобного рода программ может наблюдать за сотрудниками в режиме реального времени, и отслеживать рациональность использования рабочего времени – создавать и просматривать отчеты об их активности за любой промежуток времени. Анализ полученной информации позволяет увеличить эффективность деятельности любой организации и выявить «халявщиков», имитирующих работу.

Служба безопасности способна выявить и пресечь утечки информации через разного рода мессенджеры (ICQ, Miranda, и т.д.) Сможет проверить, не посещает ли сотрудник «подозрительные» веб-сайты и не запущены ли у него «подозрительные» приложения. Списывал или записывал он, какую либо информацию с/на сменные носители. Также для наблюдения пригодятся снимки экрана – можно наблюдать всё, что пользователь компьютера видит на мониторе.

Отделу кадров нужна та же информация, что и руководителю. Используя статистику, собранные программой данные, можно понять, на что реально тратится рабочее время и сделать из этого соответствующие выводы.

Системные администраторы с помощью мониторинга узнают о том, что происходит в локальной сети – какие программы использовал пользователь в определенный промежуток времени и какие сайты он посещал. Снимки экрана помогут в выявлении и решении различных проблем.[122]

• «Кейлоггинг» – или так называемый клавиатурный сниффер: полное протоколирование всех нажатых пользователем клавиш (включая скрытые символы или «реальные» отображаемые «*» – для ввода паролей и даже последовательность нажатий специальных клавиш, таких как CTRL, ALT, Delete) с привязкой к приложению, дате и времени.

• Запись и протоколирование «чатов»(AOL, Google, IRC, Skype и т.д.), систем мгновенных сообщений (AIM (AOL Instant Messenger), MSN, Yahoo, MySpace, ICQ, Trillian и т.д), а так же возможность блокировать любой принятый или инициированный пользователем «чат».

• Возможность прочесть любой email отправленный, либо принятый (включая email специализированных почтовых сайтов).

• Просмотреть любой и каждый веб-сайт посещенный пользователем (и что именно он делал на этих сайтах, каким содержимым интересовался и сколько провел общего времени): социальные сети, поисковые ресурсы, файловые хранилища и т.д.

• Благодаря функциям записи образов экрана, можно видеть не только, что делается за компьютером, но также и точную последовательность

[122] Эффективность работы персонала: программы мониторинга в помощь руководителю // http://itkaliningrad.ru/articles/6/0/3245

этих действий. Программы, которые пользователь запускает, будь-то текстовые процессоры, электронные таблицы, базы данных, презентации, игры и т.п.

• Отслеживание записи/перезаписи, новых/существующих документов копируемых на сменные носители: диски и карты памяти. Плюс запись всех документов распечатанных пользователем на принтере.

• Запись и протоколирование файлов пересылаемых/скачиваемых пользователем с помощью email, файлообменных сетей, и т.д.

• Система оповещения, которая проинформирует в случае, если компьютер используется ненадлежащим образом. Путем использования ключевых слов и фраз, которые определяют системные администраторы, программа отправляет им электронное сообщение, содержащее подробный отчет о том, где, когда и как было использовано ключевое слово, каждый раз, когда это слово набирается на клавиатуре, в чате, в электронном сообщении или в качестве запроса на поисковых сайтах.

• Программа может использоваться в режиме «невидимки», как программа-шпион, или в открытом режиме, когда пользователь видит, что за ним наблюдают, но избавиться от этого не может. Что прямым образом влияет на повышение дисциплины и мотивации сотрудников – очевидно, что когда работодатель наблюдает за сотрудниками, и они знают об этом, то их рабочая мотивация увеличивается. Вряд ли кто-нибудь будет проводить рабочие часы на развлекательных сайтах или за компьютерными играми, зная, что все это не останется без внимания руководства.[123]

Результаты исследования Американской ассоциации менеджмента показали: 82 % руководителей используют те или иные формы электронного контроля или физического наблюдения, в 63 % компаний отслеживают обращение к интернету, около 47 % компаний просматривают электронную почту своих сотрудников. Работодатели считают контроль над персоналом своим естественным правом, поскольку всё, что создает сотрудник на рабочем месте и в рабочее время – собственность компаний, а значит работодатель имеет право знать, что делает персонал и на что тратит время, оплачиваемое компанией.[124]

Как утверждают авторы, базовой категорией процедуры мониторинга и фактически результирующим показателем выступает уровень лояльности персонала. Это достаточно точный показатель социального здоровья организации как эффективно работающего хозяйствующего субъекта.[125]

---

[123] Эффективность работы персонала: программы мониторинга в помощь руководителю // http://itkaliningrad.ru/articles/6/0/3245

[124] Соломанидина Т.О., Соломанидин В.Г. Кадровая безопасность компании. – М.: Изд-во «Альфа-Пресс», 2011. С. 66.

[125] Копейкин Г.К., Потемкин В.К. Менеджмент экономической безопасности. – СПб.: Терция, 2004. С. 79.

2.5. Меры безопасности при увольнении сотрудника

Если уж работник не оправдал надежд и его приходится увольнять, необходимо делать это грамотно, так, чтобы у работника не было чувства унижения, агрессии и делания отомстить. Вопрос расставания с сотрудниками зависит в частности от того, на каком основании сотрудника увольняют (по собственному желанию или по инициативе администрации) и насколько ценен сотрудник для организации. Если нет желания оставить сотрудника в организации, то его заявление на увольнение подписывается руководителем сразу. Если с работником жалко расставаться, то руководителю, прежде чем подписывать заявление, следует предпринять ряд действий, направленных на то, чтобы оставить работника в организации.

Меры системы безопасности, принимаемые при увольнении сотрудника по собственному желанию:

1. Выяснение истинных причин увольнения.
2. Выяснение планируемого места будущей работы.
3. Выявление истинной мотивации сотрудника, его лояльности к покидаемому предприятию.
4. Выяснение объема известной ему информации (особенно конфиденциальной).
5. Установление риска угрозы разглашения конфиденциальной информации и принятие мер к их минимизации.
6. Контроль сдачи увольняющимся всех конфиденциальных материалов.
7. Проведение инструктажа с увольняющимся по неразглашению конфиденциальной информации. Инструктаж проводится лицом, ответственным за сохранение коммерческой тайны на предприятии.[126]

Если работник действительно ценный, следует обсудить с ним условия, на которых он останется, попытаться ликвидировать причину увольнения.

Какие бы ни были причины увольнения сотрудника, он должен покидать организацию без чувства обиды, раздражения и мести. В этом случае фирма может надеяться, что вслед за увольнением не возникнут иные проблемы, связанные с тем, что он предоставит конфиденциальную информацию конкурентам или криминальным структурам[127]. Очень подрывают лояльность персонала организации необъясненные увольнения и

---

[126] Обеспечение безопасности при подготовке к увольнению и после увольнения сотрудника // http://uslugi-po-zaschiteinformacii.ru/obespechenija_bezopasnosti_pri_uvolnenii.html

[127] Соломанидина Т.О., Соломанидин В.Г. Кадровая безопасность компании. – М.: Изд-во «Альфа-Пресс», 2011. С. 116.

практика ругать уволенных, поэтому причина увольнения должна быть объяснена всем официально, с точными и аргументированными фактами плохой работы сотрудника или обстоятельств, связанных с политикой компании, положением дел.[128]

Подготовка к увольнению сотрудника осуществляется по следующим этапам:

1. Определение объекта увольнения, т.е. кто конкретно в данной ситуации должен быть уволен.
2. Определение мотивации на увольнение, т.е. поиск ответа на вопрос: почему данный сотрудник должен быть уволен.
3. Подготовка «объекта увольнения». Возможность принятия попыток подведения объекта к принятию решения уволиться по собственному желанию.[129]
4. Изучение причин увольнения и отношение к компании.
5. Перевод на работу без доступа к коммерческой тайны.
6. Выяснение будущего места работы.
7. Подбор сменщика увольняемому лицу, его стажировка.
8. Ограничение должностных полномочий.
9. Ограничение доступа к информационным ресурсам: смена паролей; запрет доступа к информационным массивам локальной сети; запрет пользования внешней электронной почтой; контроль трафика локального почтового ящика; ведение персонифицированного журнала (Log) доступа к информационным ресурсам компании.
10. Ограничение доступа к материальным ресурсам: запрещение получения подотчетных финансовых средств; запрещение визирования документов материального учета; изъятие печатей, ключей и т.п. запрет принимать окончательные решения по проведению финансовых операций с безналичными средствами.
11. Ограничение передвижения по территории (изъятие пропусков, изъятие атрибутики фирмы, запрещение работы в выходные дни).
12. Проверочные мероприятия (проведение инвентаризаций товарно-материальных ценностей (ТМЦ), за которые отвечает сотрудник, возврат затрат на обучение, возмещение нанесенного ущерба).
13. Проверка наличия и состояния документов. При необходимости сдача в архив, уничтожение.
14. Проведение документального оформления отношений. Проверка юридической безупречности оснований, документов и процедуры увольнения.

---

[128] Соломанидина Т.О., Соломанидин В.Г. Указ соч. С. 117.

[129] Обеспечение безопасности при подготовке к увольнению и после увольнения сотрудника // http://uslugi-po-zaschiteinformacii.ru/obespechenija_bezopasnosti_pri_uvolnenii.html

15. Процедурные мероприятия: доведение приказа об увольнении, оформление "обходного" листа, проведение итоговой беседы, выдача трудовой книжки.[130]
16. Проведение окончательного расчета и выдачи денег.

Как выяснил аналитический центр компании «Серчинформ», в борьбе с мстительными работниками российские компании стараются защитить электронную почту (33%), съемные носители (21%), интернет-протоколы передачи данных (19%).[131] Если увольняемый обладал какими-то сведениями, представляющими коммерческую тайну, целесообразно перевести его на другой участок работы, где такие сведения отсутствуют и оставить его в штате до тех пор, пока сведения не потеряют своей актуальности. [132]

Любопытен пример Великобритании, где существует так называемый «садовый отпуск» – оплачиваемый отпуск на долгое время, например, на целый год, который дается после увольнения сотрудника, чтобы сотрудник не смог работать на конкурентов на это время.[133]

В момент увольнения работник наиболее критично и правдиво освещает истинное положение дел. Поэтому после объявление об увольнении руководителю следует внимательно выслушать и проанализировать контрдоводы и аргументы сотрудника в отношении положения дел в организации. Этика предполагает не унижать человека, не наносить ему обиды, не злорадствовать по поводу увольнения, что бы он не сотворил.

2.6. Лояльность персонала

Под лояльностью (от франц. – верность), как правило, понимают преданность сотрудников целям и ценностям организации, другими словами, это такие сотрудники, которые понимают и принимают корпоративную культуру компании.

На практике это проявляется в поведении и установках работников:

- работники связывают свои планы с данной организацией как минимум на три года;

- работники готовы поступиться своими экономическими интересами в пользу среднесрочных экономических целей организации;

---

[130] Соломанидина Т.О., Соломанидин В.Г. Кадровая безопасность компании. – М.: Изд-во «Альфа-Пресс», 2011. С. 118.

[131] Таранин А. Как работодателям мстят обиженные сотрудники // https://www.vedomosti.ru/management/articles/2016/12/08/668700-rabotodatelyam-mstyat-sotrudniki

[132] Соломанидина Т.О., Соломанидин В.Г. Кадровая безопасность компании. – М.: Изд-во «Альфа-Пресс», 2011. С. 118.

[133] Вражнова М.Н., Терновая Л.О. Социология кадровой безопасности: Учебное пособие. – М.: Международный издательский центр "Этносоциум", 2017. С. 227.

- работники доброжелательно относятся к инновационной политике топ-менеджмента организации.

Лояльным может быть назван коллектив, где численность работников, имеющих подобные установки, не менее 80 % общего числа работающих в организации.[134]

Данный принцип включает комплекс мер по установлению позитивных отношений работников к работодателям, от которых зависит острота и глубина проблем организации. От того, кем ощущает себя сотрудник – заменимым «винтиком» или уважаемым передовиком производства – зависят проблемы предприятия.[135]

Более широкое толкование сущности лояльности: это комплекс мер по установлению позитивных отношений работников к работодателям, «терпение» работников в случае невыполнения и/или задержки выполнения обязательств со стороны работодателя, «преданность» сотрудников своему предприятию, вне зависимости от того, удовлетворяет работа на данном предприятии работника или нет и т.д.[136]

Таблица 1

Основные форм реализации и причины нелояльности персонала[137]

Формы проявления нелояльности	Причины, определяющие соответствующую угрозу
1. Согласие на предложение о смене работодателя	Недовольство экономическими условиями найма Недовольство занимаемой должностью или отсутствием перспектив карьерного роста Неудовлетворенность работой в организацией в целом (своими трудовыми функциями, характером труда и т.п.) Неуверенность в будущем организации Недовольство отношением к себе со стороны руководства Недовольство отношениями с коллегами

[134] Копейкин Г.К., Потемкин В.К. Менеджмент экономической безопасности. – СПб.: Терция, 2004. С. 80.

[135] Рыжов Р.О. Кадровая безопасность: опыт социологической концептуализации / Инвестиции, бизнес и право: сборник научных трудов // http://www.ibl.ru/konf/151211/kadrovaja-bezopasnost.html

[136] Царенко Ю. Кадровая безопасность компании // «Кадровик. Кадровое делопроизводство», № 7, июль 2006 г. // http://123-job.ru/content/articles_1132/

[137] Любавская Л.И., Беляйкин Д.В. Кадровая безопасность как фактор конкурентоспособности в сфере банковского предпринимательства: Учебное пособие. – Новосибирск: НФ РГТЭУ, 2010. С. 38-39

Окончание табл. 1

Формы проявления нелояльности	Причины, определяющие соответствующую угрозу
2. Продажа или вынужденная передача конфиденциальной информации конкурентам и иным сторонним структурам	Недовольство экономическими условиями найма Недовольство отношением к себе со стороны руководства Негативные личностные качества Ранее допущенные нарушения, ставшие поводом для шантажа
3. Инициативная передача компрометирующей организацию информации надзорным и налоговым органам	Недовольство отношением к себе со стороны руководства Негативные личностные качества
4. Неумышленное разглашение конфиденциальной информации	Негативные личностные качества Отсутствие должных компетенций из-за неэффективного обучения
5. Прямые хищения денежных средств организации или ее клиентов в любой форме	Недовольство экономическими условиями найма Неуверенность в будущем организации Негативные личностные качества
6. Злоупотребление служебным положением в пользу клиентов или других бизнес-партнеров банка	Недовольство экономическими условиями найма Негативные личностные качества Неуверенность в будущем организации
7. Публичное выражение недовольства работодателем, необоснованная критика политики банка ли своего непосредственного руководства	Недовольство экономическими условиями найма Недовольство занимаемой должностью или отсутствием перспектив карьерного роста Недовольство отношением к себе со стороны руководства Негативные личностные качества
8. Сознательное провоцирование конфликтов в своем трудовом коллективе	Недовольство занимаемой должностью или отсутствием перспектив карьерного роста Недовольство отношениями с коллегами Негативные личностные качества

Указанные в таблице 1 причины нелояльного поведения можно разделить на следующие две группы:

- причины, не связанные с эффективность действующей в организации системы управления персоналом, кадровой политики;

- причины, связанные с кадровой политикой и недостатками в системе управления.

К первой группе относятся в первую очередь негативные личностные качества нелояльного работника. В первой главе уже были рассмотрены некоторые примеры характерологического поведения работников, типы трудных людей и потенциально опасные качества. Можно к негативным качествам добавить еще примеры. Такие качества как завышенная самооценка, неадекватная амбициозность, повышенное стремление к власти, чрезмерное честолюбие могут толкать работника на попытки занять место руководителя путем провоцирования конфликтов, «подстав», или приводить к предательству работодателя в качестве мести за нереализованные амбиции. Меркантилизм толкает человека к любым способам личного обогащения, вне зависимости от уровня установленной ему зарплаты и бонусов. Единственный путь нейтрализации угроз кадровой безопасности в случае наличия сотрудников с такими качествами – отказ от работы с ними, поскольку возможность воздействовать на такого работника с целью повышения лояльности обречены на провал.[138] Негативные качества личности носят либо врожденный характер либо формируются в детстве в процессе воспитания и корректировке в дальнейшем поддаются с трудом или вообще не поддаются.

Вторая группа причин нелояльности зависит от самого работодателя, поскольку связано с ошибками в разработке кадровой политики и в функционировании системы управления персоналом. Основные ошибки тут следующие: неэффективная система стимулирования; отсутствие действенной системы обучения; противоречия между позиционируемой и реально существующей культурой; – отсутствие возможностей карьерного роста; неспособность оценить компетентность работников; ошибки при увольнении, сокращении персонала; несправедливость в отношении работников в любой форме. Ниже систематизированы факторы, повышающие и понижающие лояльность персонала (таблица 2):

---

[138] Любавская Л.И., Беляйкин Д.В. Кадровая безопасность как фактор конкурентоспособности в сфере банковского предпринимательства: Учебное пособие. – Новосибирск: НФ РГТЭУ, 2010. С. 40

Таблица 2

Факторы, влияющие на лояльность

Факторы, повышающие лояльность	Факторы, снижающие лояльность
Возможность продвижения по службе как результат личных усилий	Отсутствие перспектив роста; Продвижение по службе только «своих».
Гарантия занятости при добросовестной работе.	Неуверенность в занятости вне зависимости от результатов труда.
Оплата труда по результатам	Несправедливая оценка труда. Качественная работа не вознаграждается.
Четкие правила для всех вне зависимости от статуса.	«Двойные стандарты» для руководства и рядовых сотрудников, для «своих» и «чужих».
Поощрение хорошо выполненной работы.	Обезличивание результатов труда. Администрация приписывает успех себе, а неудачи – подчиненным. Безразличное отношение к оценке работ.
Работник может проявить инициативу, зная, что это не приведет к увеличению объема работ, что он будет услышан	«Инициатива наказуема», приводит лишь к тому, что сотрудника нагружают больше или инициативу отвергают, даже не вникая.
Работа позволяет развивать способности	Способности игнорируются. Профессионалов загружают рутиной.
Справедливое распределение работы.	Сотрудники загружены работой в разной степени при одинаковой зарплате.
Работнику дают возможность самостоятельно принимать решения (в рамках его полномочий).	Мелочный, тотальный контроль. Отсутствие контроля со стороны руководителя, порождающее у работника ощущение «ненужности».
Работнику дают почувствовать значимость его работы и его самого для организации.	Сотрудник считает свою работу бессмысленной или ненужной. Ощущение сотрудников, что они работают «на дядю».
Нет стрессовых ситуаций или они сведены к минимуму.	Частые стрессовые ситуации из-за недостатков в управлении.
Партнерские отношения с коллегами и начальником	Постоянные межличностные конфликты. Ограничена возможность общения на работе.
Хорошая информированность о работе.	Работники плохо информированы о том, что делается на фирме; испытывают ощущение, что от них что-то скрывают.
Гибкий график работы, позволяющий учитывать индивидуальные особенности работников.	Жесткий график, не всегда оправданная жесткая дисциплина.

Формирование лояльности не сводится к разработке специальной программы, а должно быть целенаправленное построение кадровой политики компании, формирование сильной организационной культуры.

Согласно проведенным в США исследованиям, процветающие и быстрорастущие фирмы имеют высокую культуру и особый стиль, способствующий достижению. Признаки сильной организационной культуры:

- работники имеют четкие представления о ценностях и твердые убеждения о способах достижения целей;
- существуют партнерские отношения на всех уровнях;
- высоко ценятся профессиональная компетентность и верность делу;
- продвижение по службе зависит от результатов труда;
- поощряется гордость за собственные достижения и успехи фирмы.

Для таких фирм характерна система ценностей, принятых и одобренная всеми сотрудниками. Важно при этом, чтобы ценности и поведение совпадали. Система ценностей, правила и реальное поведение должны быть согласованы. Так, если пропагандируются партнерские отношения, а должности получают те работники, которые имеют родственные или дружеские связи, это действует разрушительно для организационной культуры.[139] Важно честное соблюдение принятых миссии и принципов. Если компания на словах декларирует демократические принципы управления, а по факту реализует авторитарный стиль руководства, то все попытки сформировать лояльность будут сводиться на «нет».

Одной из причин низкой лояльности и одной из угроз кадровой безопасности, является низкая удовлетворенность работой. Именно высокая удовлетворенность работой во многом обеспечиваются высокую лояльность сотрудников работодателю. Руководителю организации важно отслеживать уровень удовлетворенности персонала, поэтому одним из видов мониторинга является мониторинг удовлетворенности. Особенно это важно в случае гражданской службы – Российской федерации или субъекту федерации, что является, в конечном счета, важным фактором национальной безопасности страны.[140]

Для обеспечения лояльности должны быть заложены искренние уважение и забота о нуждах людей:

- Гордость за свою работу, возможность развиваться лично и профессионально.
- Искреннее уважение со стороны руководителя и дружеские отношения с коллегами.

---

[139] Потемкин В.К., Спивак В.А., Покровская Н.Н. Организационная культура: для студентов экономических вузов и факультетов экономики и менеджмента / под. ред. С.Б. Мурашова. – СПб.: СПбАУП, 2006. – С. 112.

[140] Кадровая политика и кадровая безопасность в современной России: Сборник научных трудов / Под ред. Турчинова А.И. – М.: МАКС Пресс, 2011. С. 42.

- Доверие, которое особенно ценят квалифицированные специалисты. Это может выражаться, например, в самоменеджменте, возможности выбирать график работы, в самостоятельности при принятии решений, личной ответственности за результаты проекта и пр.
- Достойное вознаграждение. Если сотрудник получает заработную плату ниже рыночной, то он всегда будет считать себя недооцененным. Расширенный компенсационный пакет требует немалых затрат, но они, по оценкам специалистов, практикующих такую мотивацию, окупаются именно лояльностью и высокой эффективностью труда.[141]

Таким образом, формирование лояльности – результат продуманной кадровой политики компании, отражение отношения руководства организации к персоналу.

[141] Как повысить лояльность персонала // http://www.hr-portal.ru/blog/kak-povysit-loyalnost-personala

Заключение

Таким образом, можно утверждать, что вся деятельность службы персонала – это обеспечение безопасности своего предприятия, поскольку нацелена на такую работу с персоналом, на установление таких трудовых отношений, которые предопределяют высокую степень удовлетворенности трудом.

С точки зрения безопасности каждый кандидат на вакансию, каждый сотрудник предприятия и даже бывшие работники должны рассматриваться как источник потенциальной угрозы как в части умышленного нанесения ущерба, но и в отношении опасности причинения убытков, связанных с низкой квалификацией, с невозможностью применить высокий профессионализм; с недовольством своей работой и условиями труда; с неадекватной оценкой результатов труда; со слабым прогнозированием и контролем благонадежности и т.д.

Деятельность по обеспечению безопасности не является отдельным направлением в должностных обязанностях менеджера по персоналу, но органично вписывается в него при условии, что в компании присутствуют и грамотно реализуются все этапы управления персоналом. Четкая, прозрачная, справедливая кадровая политика создает предпосылки для формирования чувства гордости работника за предприятие, высокой степени лояльности, желание в нем трудиться во что бы то ни стало даже во времена кризисов.

Если служба по работе с персоналом работает непрофессионально, то можно ожидать убытки в результате предумышленных или непредумышленных действий персонала.

Библиографический список

1. Акцентированные черты характера // http://psyznaiyka.net/view-xarakter.html?id=akcentirovannye-cherty-haraktera
2. Асадов А.Н., Покровская Н.Н., Саядян Н.М., Спивак В.А. Этика деловых отношений: учебное пособие. – СПб: Изд-во СПбГУЭФ, 2006. – 271 с.
3. Асадов М.Н., Прозоровская К.А. Социальная криминология: учебное пособие. – СПб: Изд-во СПбГУЭФ, 2004.
4. Бодров В.А. Информационный стресс: учебное пособие. – М.: ПЕР СЭ, 2000.
5. Виды контроля персонала // http://uslugi-po-zaschiteinformacii.ru/vidy_kontrolja_personala.html
6. Вражнова М.Н., Терновая Л.О. Социология кадровой безопасности: учебное пособие. – М.: Международный издательский центр "Этносоциум", 2017. – 276 с.
7. Глебовский А.Ю**.** Кадровая безопасность: фильтры грубой и тонкой очистки // http://www.hr-journal.ru/articles/hrs/filtry-kadrovoj-bezopasnosti-Glebovskij.html
8. Демонстративный тип // http://psylist.net/praktikum/demotip.htm
9. Кадровая безопасность на предприятии // http://uslugi-po-zaschiteinformacii.ru/voprosy_bezopasnosti_pri_kadrovom_deloproizvodstve.html (дата запроса 04.06.2018)
10. Кадровая безопасность на предприятии // http://mir-diplom.ru/Kadrovya-bezopasnostj-na-predpriyatii.html
11. Кадровая политика и кадровая безопасность в современной России: Сборник научных трудов / под ред. Турчинова А.И. – М.: МАКС Пресс, 2011. – 224 с.
12. Как повысить лояльность персонала // http://www.hr-portal.ru/blog/kak-povysit-loyalnost-personala
13. Кибанов А. Я., Дуракова И. Б. Управление персоналом организации: отбор и оценка при найме, аттестация: учеб. пособие по специальностям "Менеджмент орг." и "Упр. персоналом". – Изд. 2-е, перераб. и доп. – М.: Экзамен, 2005. – 415 с.
14. Копейкин Г.К., Потемкин В.К. Менеджмент экономической безопасности. – СПб.: Терция, 2004. – 112 с.
15. Костусенко И.И., Куракина Л.Ю. Кадровая безопасность организации: учеб. пособие. – Великий Новгород: НовГУ им. Я. Мудрого, 2015. – 86 с.
16. Кузнецова Н.В. Кадровая безопасность организации: сущность и механизм обеспечения. – Иркутск: Изд-во БГУЭП, 2013. – 288 с.

17. Любавская Л.И., Беляйкин Д.В. Кадровая безопасность как фактор конкурентоспособности в сфере банковского предпринимательства: учебное пособие. – Новосибирск: НФ РГТЭУ, 2010. – 108 с.
18. Мак-Мак В.П. Служба безопасности предприятия // http://www.opvodopad.ru/docs/security_school/busin/16__luzhba_bezopasnosti_predpriyatiya.pdf (дата обращения 04.06.2018)
19. Месть бывшему работодателю стала мотивом убийства в офисном центре в США // https://ria.ru/incidents/20091107/192329743.html
20. Мониторинг персонала // https://www.mipko.ru/monitoring-personala
21. Нелояльность персонала как угроза безопасности организации Л.А. Агатова, Г.Л. Смолян, Г.Н. Солнцева // Труды ИСА РАН 2007. Т. 31// http://www.isa.ru/proceedings/images/documents/2007-31/216-230.pdf
22. Обеспечение безопасности при подготовке к увольнению и после увольнения сотрудника // http://uslugi-po-zaschiteinformacii.ru/obespechenija_bezopasnosti_pri_uvolnenii.html
23. Оленев Р.Г. Мошенничество как вид девиантного экономического поведения: автореф. дис. … канд. экон. наук / спец. 22.00.03. – СПб.: СПбГУЭФ, 2000. – 14 с.
24. Потемкин В. К., Спивак В. А., Покровская Н. Н. Организационная культура: для студентов экономических вузов и факультетов экономики и менеджмента / В.К. Потемкин, В.А. Спивак, Н.Н. Покровская; под. ред. С.Б. Мурашова. – СПб.: СПбАУП, 2006. – 274 с.
25. Причины возникновения предпосылок нелояльности персонала. Принципы организации системы безопасности на предприятии. Методы повышения лояльности персонала // http://poznayka.org/s52913t1.html (дата обращения 19.04.2018)
26. Прозоровская К.А. Управление персоналом. Поведение людей и групп в организации. – СПб.: Изд-во МИПКИ, 2013. – 321 с.
27. Психология менеджмента: Учебник для вузов / Под ред. Г.С. Никифорова. – 2-е изд. – СПб.: Питер, 2004.
28. Рыжов Р.О. Кадровая безопасность: опыт социологической концептуализации / Инвестиции, бизнес и право: сборник научных трудов // http://www.ibl.ru/konf/151211/kadrovaja-bezopasnost.html
29. Слободской А.Л. Управление рисками «человеческого фактора»: учебное пособие / А.Л. Слободской. – СПб.: Типография ПГУПС, 2008. – 142 с.
30. Смирнов А.В. Аддикции и кадровая безопасность / Учебное пособие.- Екатеринбург: Изд-во Урал. гос. пед. ун-та, 2009. – 102 с.
31. Соломанидина Т.О., Соломанидин В.Г. Кадровая безопасность компании. – М.: Альфа-Пресс, 2011. – 688 с.
32. Староверов Д. Лояльность персонала как фактор безопасности бизнеса // http://www.amulet-group.ru/page.htm?id=

33. Структура системы безопасности предприятия // http://uslugi-po-zaschiteinformacii.ru/sostav_i_struktura_sistemy_bezopasnosti.html (дата обращения 19.04.2018)
34. Таранин А. Как работодателям мстят обиженные сотрудники // https://www.vedomosti.ru/management/articles/2016/12/08/668700-rabotodatelyam-mstyat-sotrudniki
35. Турчинов А.И. Кадровая безопасность и глобализация // http://www.nbuv.gov.ua/old_jrn/Soc_Gum/Vcndtu/2012_58/47.htm
36. Царенко Ю. Кадровая безопасность компании // Кадровик. Кадровое делопроизводство. – 2006. – № 7 // http://123-job.ru/content/articles_1132/
37. Шегельман И.Р., Рудаков М.Н. Кадровая безопасность: учебно-методическое пособие. – Петрозаводск: Изд-во ПетрГУ, 2006. – 96 с.
38. Чумарин И.Г. Кадровая безопасность – представители групп риска в организации // Персонал-Микс. – 2001. – № 6.
39. Эффективность работы персонала: программы мониторинга в помощь руководителю // http://itkaliningrad.ru/articles/6/0/32450

Научное издание

Прозоровская Камилла Александровна

КАДРОВАЯ БЕЗОПАСНОСТЬ ОРГАНИЗАЦИИ

Под редакцией доктора экономических наук,
профессора В.К. Потемкина

Подписано в печать 01.10.18. Формат 60×84 1/16.
Усл. печ. л. 4,75. Тираж 500 экз. Заказ 417.

Издательство СПбГЭУ. 191023, Санкт-Петербург, Садовая ул., д. 21.

Отпечатано на полиграфической базе СПбГЭУ