УДК 65.012.8

# УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ НА ПРОМЫШЛЕННОМ ПРЕДПРИЯТИИ РЕСПУБЛИКИ КАЗАХСТАН

***ИСКАКОВ А.Е.***

**АННОТАЦИЯ**

В статье рассматриваются вопросы управления изменениями в службе безопасности, принципы планирования и развития, мониторинга и повышения уровня защищенности производственного предприятия. Проведенная работа основана на анализе смоделированного предприятия.

**Ключевые слова**: управление безопасностью; управление изменениями; планирование; корпоративное управление; управление рисками.

# SECURITY MANAGEMENT ON INDUSTRIAL ENTERPRISE OF THE KAZAKHSTAN REPUBLIC

***ISKAKOV A.E.***

**ABSTRACT**

The article considerate management of changes in the security service, the principles of planning and development, monitoring and improving the protection level of the industrial enterprise. The work which is carried out is based on the analysis of the models enterprise.

**Key words:** security management; change management; planning; corporate governance; risk management.

Процесс создания и внедрения службы безопасности логически завершается переходом на качественно новый уровень этого бизнес-процесса, а именно переходит в состояние постоянного саморазвития и мониторинга уровня потенциальных рисков и новых угроз для реализации комплексов эффективных превентивных и/или корректирующих мероприятий. Проблематика поднимаемого вопроса состоит в том, что во многих случаях по завершению процесса внедрения эффективной системы управления безопасностью она переходит в состояние стагнации и саморазрушения. Вопросы безопасности являются одними из наиболее критичных в условиях современного рынка, но не смотря на это им не придается должного значения собственниками бизнеса и топ-менеджментом.

Описываемые проблемы поднимались еще в работах Ж. Бержье [2], однако из работ наших современников следует отметить труды А. Доронина [4], А. Гурова [3]. В трудах этих исследователей описываются теоретические основы построения систем управления безопасностью, подкрепленные классическими примерами из практики авторов и смоделированными для наглядного представления о различных аспектах безопасности предприятия и личности.

Все вышеназванные авторы не предоставляют практического руководства, применимого после построения системы безопасности, эффективно противодействующей потенциальным злоумышленникам, в сфере закрепления предпринятых изменений и противодействию перехода управления безопасностью в состояние стагнации.

Общеизвестно, что ведение предпринимательской деятельности сопряжено с определенными категориями рисков, часть которых можно объединить в группу, связанную с вопросами безопасности. К данной группе мы можем отнести риски физической, экономической, информационной и внутренней безопасности.

Рассматривая риски этой группы более предметно, мы можем выделить типовые формулировки, характеризующие их:

– неблагонадежным и/или некомпетентным кадровым обеспечением предпринимательской деятельности;

– внутрикорпоративным мошенничеством и коррумпированностью;

– лоббированием интересов конкурирующих структур или третьих лиц;

– риск физического устранения, нанесения вреда здоровью, ключевым работникам и/или членам их семей;

– риск корпоративного захвата предприятия, недружественного поглощения;

– возможность утечки критичной информации – сведения о корпоративных и/или

личных банковских счетах, приватная информация, как то – бизнес-план, финансовая отчетность, планы мероприятий;

– компрометация руководства и/или работников предприятия, ущерб репутации предприятия.

Приведенные типовые формулировки не могут быть отнесены только к одной подгруппе рисков, ввиду их многофакторного потенциального влияния на деятельность предприятия и возможность комбинирования нескольких рисков в одну цепочку причинно-следственных связей.

К примеру, в случае проникновения злоумышленника в состав работников предприятия и закрепления на определенной позиции, он будет стремиться привести на предприятие своих подельников, для расширения сферы влияния на принятие предприятием тех или иных решений и получения большего спектра информации, в том числе конфиденциальной и даже секретной [5].

Это реализуется посредством внутрикорпоративного мошенничества, а именно: подкуп, угрозы или шантаж, лиц ответственных за предварительную оценку соискателя имеющейся вакантной должности [5]. Это упрощается при наличии устоявшихся неформальных социальных групп внутри работников предприятия. Как правило, они формируются по национальному, территориальному или клановому признакам, и несколько реже, основываясь на принадлежности к одной структуре предприятия, общему кругу интересов, конфессиональной принадлежности, или прохождению учебы, службы или работы в одних и тех же организациях и структурах.

Как следствие усиливается влияние неформальной группы, организованной злоумышленниками, преследующими цель нанести финансово-материальный или репутационный ущерб предприятию-цели или получить реальный (фактический), либо юридический контроль над принимаемыми компанией решениями в ходе ведения хозяйственной деятельности.

Данные риски призвана оценивать, минимизировать и локализовать служба безопасности предприятия. Как правило, кадровый состав этой структуры формируется из числа бывших сотрудников правоохранительных органов, органов госбезопасности и частных сыскных агентств.

В рамках поднятых вопросов, предлагаю рассмотреть смоделированную ситуацию, согласно которой мы имеем вновь открытую или реорганизованную после слияния/поглощения/смены учредителей или топ-менеджмента компанию.

После утверждения штатного расписания, разделения полномочий и ответственности, наряду с решением общехозяйственных вопросов, начинаются первоочередные мероприятия по минимизации рисков и потенциальных угроз в сфере безопасности.

К этим первичным мероприятиям мы отнесем:

– внедрение программно-аппаратных и организационных мер по предотвращению утечек информации (политики, регламенты, сниферы, DLP-пакеты, антивирусная защита, логическое и физическое разделение сетей, межсетевые экраны и т.д.);

– расстановка работников службы безопасности, занятых в сфере физической охраны объекта и ключевых сотрудников (охранники и телохранители);

– монтаж инженерно-технических заграждений, системы охранной и противопожарных сигнализаций, камер видеонаблюдения и биометрических систем идентификации человека (заборы и заграждения, датчики тепла и движения, датчики дыма, купольные и стационарные видеокамеры, сканеры отпечатков пальцев, сетчатки глаза, кровеносной системы кистей рук и т.д.)

– формирование реестра критериев при отборе кандидатов на вакантные должности и их проверка на наличие связей с контрагентами компании или элементов биографии, характеризующих их как неблагонадежных работников;

– создание и внедрение системы проверки контрагентов предприятия на благонадежность и наличие скрытых интересов в деятельности компании;

– создание и внедрение системы проверки и мониторинга деятельности лиц, уполномоченных принимать решения, влияющие на закупки и продажи материально-технических ценностей, работ или услуг;

– ведение и анализ картотеки (базы данных) касательно внутрикорпоративных неформальных групп и взаимоотношениях между ними.

Несмотря на кажущуюся громоздкость данного комплекса мероприятий, он является обязательным для крупного промышленного (и не только) предприятия. Эти меры являются минимальным решением для обеспечения достаточного уровня безопасности компании. Во

временном выражении реализация всех этих мер может занять достаточно длительное время.

На этапе после выполнения предложенных типовых минимальных мероприятий по обеспечению достаточного уровня безопасности наступает момент, когда кардинальная реорганизация службы безопасности может быть произведена лишь в случае сокращений штатного расписания или расширения деятельности компании и появления филиальной сети.

В остальных случаях, не предполагающих критичных последствий для службы безопасности, для поддержания имеющегося уровня безопасности следует прибегать к методике индикативного (или директивного, в зависимости от стиля управления) планирования касательно качественного повышения ее уровня работы.

Это весьма сложный момент для всех категорий работников службы безопасности и он может повлечь за собой как переход к стагнации и постепенному падению уровня защищенности компании, так и крайне медленный рост качественных показателей работы службы безопасности.

Ситуации такого рода в менеджменте рассматриваются такими специальными дисциплинами как «управление изменениями» и «стратегическое планирование» [6].

Исходя из практического опыта автора настоящей статьи, эффективными мерами по сохранению мобилизационного состояния службы безопасности является, прежде всего, принятие нескольких принципов, как теоретического базиса системы управления безопасностью.

Первый принцип – в отличие от технических и программно-аппаратных средств, работники не могут постоянно находиться в мобилизационном (аварийном, критическом) состоянии, так как это непременно приведет к подрыву их здоровья, стрессам, появлению стойкого негативного отношения к работе и коллегам.

Второй принцип – для того, чтобы отдельно взятый элемент структуры управления (департамент, отдел, бюро) или отдельный работник не переходили в застойное состояние, следует проводить периодическую ротацию кадров между структурами [6]. Это способствует расширению спектра компетенций и практических навыков работников и препятствует формированию «рутинного» отношения к работе.

Третий принцип – наряду с ротацией кадров, следует регулярно обновлять личный состав подразделения безопасности, организовывать курсы повышения квалификации и различные системы поощрений для работников.

Основываясь на предложенных принципах, следует разрабатывать планы мероприятий по развитию службы безопасности с различными горизонтами планирования. Проводя анализ текущей ситуации, следует оценивать как отношение проделанной работы к запланированному объему работы, так и соотношение имеющихся результатов к «генеральным» планам развития. Для получения непредвзятой оценки состояния уровня защищенности и безопасности компании следует проводить периодические аудиты посредством сторонних организаций.

Отдельным пунктом, следует отметить, что на территории Республики Казахстан и СНГ в целом очень слабо развито профессионально-направленное образование в сфере безопасности. Основными игроками этого рынка выступают военные и ведомственные учебные учреждения, которые не готовят работников частных компаний. Выпускник такого заведения обязан отработать на государственной службе определенный промежуток времени для «восполнения» понесенных государством затрат в ходе его обучения. Альтернативой служит возможность выплатить все затраченные на подготовку средства в пользу государства, по прохождению полного курса обучения, однако для абсолютного большинства выпускников обучение в Академии было сопряжено с желанием поступления на службу в органы государственной безопасности и акселерации темпов карьерного роста в перспективе [7].

В связи с этим, крупные предприятия вынуждены обращаться к зарубежным – европейским, американским и азиатским поставщикам (вендорам) образования в этой сфере. Как правило, это программы MBA, рассчитанные на руководителей и главных специалистов служб безопасности и курсы, организованные военными и полицейскими учебными заведениями в качестве (чаще всего закрытых) мероприятий по обмену практическим опытом.

С проблематикой поставленного вопроса сталкивается абсолютное большинство компаний, вне зависимости от того в какой сфере они ведут свою хозяйственную деятельность. Проведенная аналитическая работа привела нас к однозначным выводам о необходимости централизации и систематизации знаний об управлении безопасностью в частном секторе силами третьей стороны, являющейся лицом, созданным в рамках государственно-частного партнерства, так как на настоящий момент

в Республике Казахстан такой работы не ведется. Также стоит острая проблема в сфере образования – отсутствуют отечественные учебные программы, предлагаемые в высших учебных заведениях, подходящие для специалистов и руководителей служб безопасности.

Я, как молодой специалист, считаю, что основой для трансферта столь необходимого практического опыта и методологии принятия управленческих (стратегических и оперативных) решений, могут и должны стать организации ветеранов органов государственной безопасности. А также требуется разработать при полной поддержке государства и бизнеса, академические учебные программы для магистрантов и докторантов в направлении обеспечения безопасности в гражданских высших учебных заведениях.

## Список литературы

1. Абдуллаев С.Ж. Криминалистическая экспертиза в расследовании преступлений: логико-концептуальные и организационные вопросы. – Карагандинский юридический институт, 2003. – 32 с.

2. Бержье Ж. Промышленный шпионаж. / перевод М.Д. Тертерова. – М.: Международные отношения, 1972. – 322 с.

3. Гуров А. Профессиональная преступность: прошлое и современность. – М., 1990.

4. Доронин А. Бизнес-разведка. – М.: Издательство «Ось-89», 2003. –384 с.

5. Кенжетаев Ч.Д. Методика расследования посредничества во взяточничестве на первоначальном этапе. – Карагандинский юридический институт, 2006. – 24 с.

6. Прохоров А.П. Русская модель управления // Журнал "Эксперт". – 2011. – 376 с.

7. Правила приема на обучение в специальные (военные) учебные заведения Комитета национальной безопасности Республики Казахстан, реализующие профессиональные учебные программы высшего образования в сокращенные сроки, (утверждены приказом Председателя комитета национальной безопасности Республики Казахстан № 182 от 12.04.13 г.)