УДК 316

СТРУКТУРА СИСТЕМЫ УПРАВЛЕНИЯ КАДРОВОЙ БЕЗОПАСНОСТЬЮ ИНЖИНИРИНГОВОЙ КОМПАНИИ

© 2013 г. ***Л.С. Егорова, П.С. Фролова***

Текстильный институт Ивановского государственного политехнического университета

egorova@igta.ru

Поступила в редакцию 10.03.2013

Выявлено влияние факторов реализации информационной угрозы в инжиниринговой компании и действий сотрудников, которые способствуют реализации данной угрозы. Разработана структура системы управления, основанной на стратегии адекватного ответа на угрозы, и на ее основе схема движения решения вопросов кадровой безопасности инновационно ориентированной организации.

Ключевые слова: система управления кадровой безопасностью, риски и угрозы, стратегия, организационная структура, функции.

Специфические условия рыночной трансформации отечественной экономики значительно увеличивают вероятность негативной реализации рисков и угроз кадровой безопасности инновационно ориентированных организаций, поэтому назрела острая необходимость в проведении исследований и разработке мер в области выявления рисков и устранения угроз системы кадровой безопасности организации. Тем более это актуально для инжиниринговых компаний, где в силу их специфики особое значение имеет человеческий фактор.

Безопасность организации представляет собой динамически устойчивое состояние (динамическое равновесие), при котором ему в данный момент опасность не угрожает.

Целью обеспечения безопасности любой организации является комплексное воздействие на потенциальные и реальные угрозы (риски), мешающие ей успешно функционировать в сложных и нестабильных условиях внешней и внутренней среды. Самое сложное звено в системе безопасности организации – это ее сотрудники, выступающие одновременно как объекты и как субъекты потенциальных угроз.

Поэтому кадровую безопасность целесообразно рассматривать также с двух позиций:

1. С позиции организации безопасной деятельности персонала.

2. С позиции безопасности организации от возможных негативных действий их сотрудников.

Таблица 1

Влияние факторов реализации информационной угрозы в инжиниринговой компании

2009	2010	2011
Естественные факторы (стихийные бедствия – пожар, наводнение, ураган, молния и другие причины)		
2%	2%	2%
Человеческие факторы		
случайные		
– угрозы, носящие случайный, неумышленный характер (связанные с ошибками процесса подготовки, обработки и передачи информации; с нецеленаправленной «утечкой умов», знаний, информации; связанные с ошибками процесса проектирования, разработки и изготовления систем и их компонент; с ошибками процесса подготовки и обработки информации)		
14.5%	19.5%	22%
умышленные		
– угрозы, обусловленные умышленными, преднамеренными действиями людей (связанные с передачей, искажением и уничтожением научных открытий, изобретений секретов производства, новых технологий по корыстным и другим антиобщественным мотивам (документация, чертежи, описания открытий и изобретений и другие материалы); подслушиванием и передачей служебных и других научно-технических и коммерческих разговоров; с целенаправленной «утечкой умов», знаний, информации; связанные с несанкционированным доступом к ресурсам автоматизированной информационной системы (внесение технических изменений в средства вычислительной техники и средства связи, подключение к средствам вычислительной техники и каналам связи, хищение носителей информации: дискет, описаний, распечаток и др.)		
83.5	78.5%	76%
100%	**100%**	**100%**

Рис. 1. Действия сотрудников,
способствующие реализации угроз информационной безопасности

По нашему мнению, для повышения уровня общей безопасности организации необходимо выделить два основных направления в области кадровой безопасности, связанных с функционированием персонала компании. Первое направлено на охрану и улучшение условий труда и сотрудников. Второе – на повышение лояльности персонала к своей организации.

Как показало проведенное нами в инжиниринговой компании исследование, по характеру потерь от реализованных угроз 85% приходится на информационную безопасность, 15% на безопасность имущества организации [1, с. 54].

Наибольший удельный вес среди влияния факторов на реализацию информационных угроз имеет человеческий фактор. На естественные факторы, в 2011 году приходится 2%. На человеческие факторы, носящие неумышленный, случайный характер – 22%, носящие умышленный характер – 76%, всего – 98%. Численное изменение влияния данных факторов в 2009, 2010, 2011 годах показано в таблице 1.

Главным источником угрозы на предприятиях подобного типа выступают их собственные работники. Объектами рассматриваемой угрозы нередко выступают должностные лица инжиниринговых компаний, имеющие доступ к конфиденциальной информации, часто связанной с научными разработками, к управлению денежными средствами и ликвидными товарно-материальными ценностями, а также к хранению их, к реализации функций управления, регулирования и надзора.

В ходе экспертной оценки нами были выявлены действия сотрудников, которые способствуют реализации информационной безопасности. Данная взаимозависимость между инициатором угрозы и ее исполнителем представлена на рисунке 1, где в скобках указаны процентные значения данных угроз.

Стратегия управления кадровой безопасностью является ключевым элементом системы управления организацией и определяется нами как совокупность приоритетных целей управленческих подходов, реализация которых обеспечивает защиту организации от любых потенциальных угроз, связанных с функционированием кадрового направления ее деятельности [1, с. 54–55].

Стратегия управления кадровой безопасностью может быть реализована на основе одного из трех следующих вариантов [2, с. 8–16]:

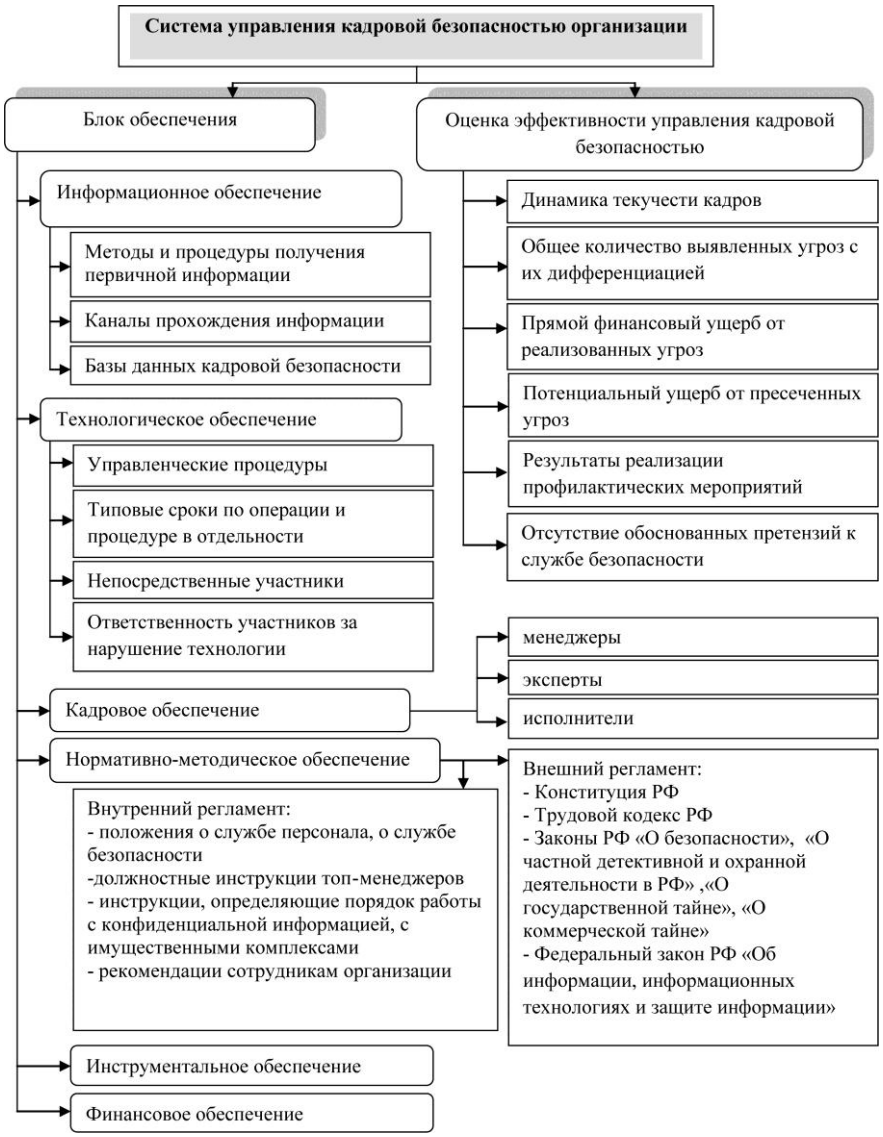


Рис. 2. Структура системы управления кадровой безопасностью инжиниринговой компании, основанная на стратегии адекватного ответа на угрозы

1. Стратегия упреждающего противодействия, включающая профилактические методы противодействия потенциальным угрозам с возможным применением методов на грани легитимности.

2. Стратегия пассивной защиты от угроз, ориентированная на защиту со стороны государства (через правоохранительные и судебные органы), минимизацию затрат (обеспечение минимального уровня безопасности).

3. Стратегия адекватного ответа на угрозы, включающая создание и развитие блоков обеспечения, формирующих условия для эффективного управления, с дальнейшей оценкой эффективности управления кадровой безопасностью.

Каждый вариант имеет свои достоинства и недостатки.

На наш взгляд, наиболее приемлемой для инжиниринговой компании является стратегия адекватного ответа на угрозы. Ориентация на данный вид стратегии предполагает возможность использования службой безопасности всего комплекса легитимных методов профилактики и отражения потенциальных угроз. В порядке исключения допускается использование и не полностью легитимных методов, но лишь в отношении тех конкурентов или иных источников угроз, которые первыми применили подобные методы.

Предлагаемая нами структура системы управления, основанная на стратегии адекватного ответа на угрозы, представлена на рисунке 2.

В организационной системе управления инжиниринговой компании служба безопасности

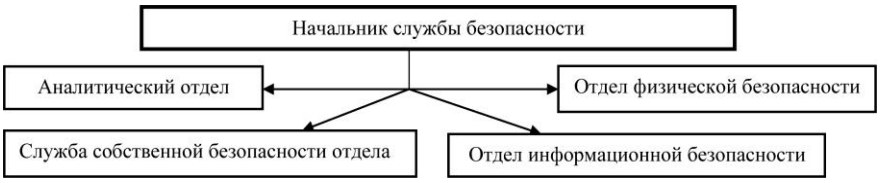


Рис. 3. Структура службы безопасности организации

должна выступать в качестве одного из штабных, то есть наделенных распорядительными-полномочиями подразделений. Она несет основную ответственность за защиту имущественных и неимущественных интересов организации от возможных угроз.

В научной литературе и практической деятельности не сформированы единые требования к структуре данной службы, и в каждой организации она формируется в зависимости от специфики и ресурсных возможностей.

На рисунке 3 представлена наиболее приемлемая, на наш взгляд, организационная структура службы безопасности инжиниринговой компании [3, с. 50–51].

Эффективное выявление рисков и противодействие угрозам кадровой безопасности организации не может быть реализовано силами исключительно службы безопасности. К решению этой задачи должны быть подключены все должностные лица организации и некоторые штабные инстанции. С целью предотвращения возможности пересечения сфер компетенций должно выполняться требование четкой дифференциации функций, полномочий и ответственности основных участников (табл. 2).

На основе выделенных для каждого подразделения компетенций в системе кадровой безопасности нами предлагается схема движения решения вопросов кадровой безопасности, представленная на рисунке 4.

Важным этапом системы обеспечения кадровой безопасности безусловно является контроль над деятельностью сотрудников организации – он должен быть комплексным и непрерывным.

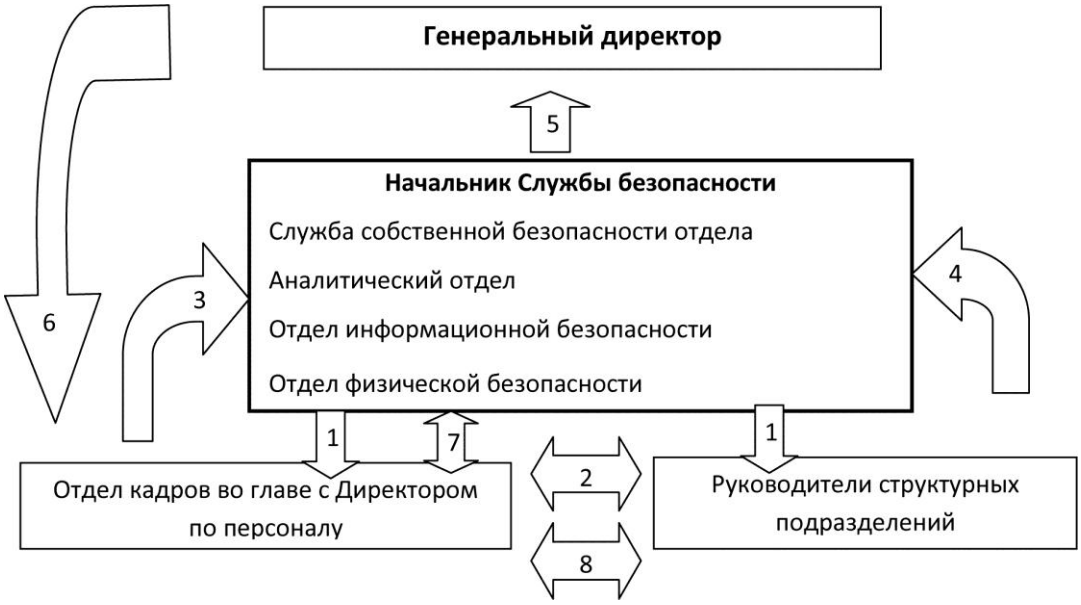
Данные меры в случае их применения в инжиниринговой компании смогут снизить риски, связанные с возможностью утечки конфиденциальной информации, повысить ответственность работников за свои действия, их мотивацию к обеспечению кадровой безопасности в целом и, следовательно, повысить уровень защищенности и лояльности работников в данной организации.

Таким образом, точно скоординированные, слаженные действия всех подразделений в структуре системы обеспечения кадровой без-

Таблица 2

Распределение функций, полномочий и ответственности между инстанциями в системе управления кадровой безопасностью инжиниринговой компании [3, с. 50–51]

Наименование инстанции	Функции, полномочия, ответственность
Топ-менеджмент	- Выбор базовой концепции организации внутрифирменных трудовых отношений; - утверждение общей стратегии управления безопасностью; - выделение необходимых ресурсов; - контроль над общей эффективностью системы
Служба безопасности	- Разработка и практическая реализация стратегии управления кадровой безопасностью; - методическое руководство деятельностью других подразделений инжиниринговой компании; - специальное обучение персонала организации; - общий мониторинг соответствующего направления деятельности других подразделений организации; - организация служебных расследований; - выполнение соответствующих заявок со стороны других подразделений, включая службу персонала; - общая ответственность за эффективность системы управления
Служба персонала	- Реализация установленных функций по обеспечению должной ответственности и лояльности персонала; - общая ответственность за эффективное противодействие угрозе переманивания сотрудников; - оперативное взаимодействие со службой безопасности
Руководители структурных подразделений	- Текущая работа по специальному обучению подчиненных; - текущий контроль над соблюдением подчиненными правил обеспечения безопасности; - оперативное взаимодействие со службой безопасности



1 – Инициирование проверки сотрудника;
2 – Сбор необходимых данных;
3 – Передача данных из личного дела, личностные характеристики проверяемого сотрудника
4 – Компетентностная оценка сотрудника
5 – Информация о благонадежности сотрудника
6 – Принятие решения и распоряжение относительно неблагонадежного сотрудника
7 – Совместная разработка плана действий относительно неблагонадежного сотрудника
8 – Реализация мероприятий по противодействию угрозам со стороны неблагонадежного сотрудника

Рис. 4. Предлагаемая схема движения решения вопросов кадровой безопасности в инжиниринговой компании

опасности и правильно выбранная и своевременно реализованная стратегия выявления рисков и устранения угроз кадровой безопасности в инновационно ориентированных организациях позволит им успешно функционировать, обеспечивая позитивное развитие отечественной экономики.

Список литературы

1. Фролова П.С., Егорова Л.С., Фролова О.Н. Стратегия управления кадровой безопасностью организации / Генезис экономических и социальных проблем субъектов рыночного хозяйства в России: Научное издание. Выпуск VII / ИГТА. Иваново, 2013. 308 с. С. 53–61.

2. Алавердов А.Р. Кадровая безопасность современного банка: стратегия и тактика управления // Управление в кредитной организации. № 2, март-апрель 2008. С. 3–41.

3. Алавердов А.Р. Управление кадровой безопасностью организации: Учеб. / А.Р. Алавердов. М.: Маркет ДС, 2010. 176 с. (Университетская серия).

THE STRUCTURE OF THE PERSONNEL SAFETY MANAGEMENT SYSTEM OF THE ENGINEERING COMPANY

L.S. Egorova, P.S. Frolova

This article deals withassessment of the influence of factors of information threats implementation of in the engineering company and employees' actions, which contribute to the realization of this threat. Development of management systemstructure, based on the strategy of an adequate response to the threat and on its basis the scheme of movement of the decision of questions of personnel security innovation oriented organization.

Keywords: the control system of the personnel security, risks and threats, strategy, organizational structure, functions.