КОНЦЕПТ
научно-методический электронный журнал
Юнкерова Ю. И. Системное управление информационными рисками // Концепт. – 2013. – № 11 (ноябрь). – ART 13229. – 0,4 п. л. – URL: http://e-koncept.ru/2013/13229.htm. – Гос. рег. Эл № ФС 77-49965. – ISSN 2304-120X.
ART 13229 УДК 004.2

Юнкерова Юлия Игоревна,
аспирант кафедры экономики и управления на предприятии ФГАОУ ВПО «Белгородский государственный национальный исследовательский университет», г. Белгород
yunkerova_yi@mail.ru

Системное управление информационными рисками

Аннотация. *В статье рассматривается концепция системного подхода к анализу сущности информационных рисков, а также к процессу управления указанными рисками. Целостность взгляда на проблему системного управления информационными рисками основана на том, что внешняя и внутренняя системы предприятия представлены в виде комплекса. Чтобы достичь конечных целей бизнеса, необходимо адаптировать архитектуру информационной системы предприятия к данному виду управления информационными рисками, а также обеспечить активное участие менеджмента в системном управлении информационными рисками.*
Ключевые слова: *информационные риски, системное управление, внешняя и внутренняя среда, архитектура информационной системы, информационная безопасность.*

Информационные риски напрямую связаны с возникновением убытков или возникновением ущерба в процессе применения компанией информационных технологий. Однако, необходимо отметить, что термин «информационный риск» до сих пор большинство исследователей связывают только с областью информационной безопасности [1]. При этом аспект снижения важнейших показателей качества информации на предприятии во внимание не берется, хотя ущерб от данного события может в несколько раз превышать подобный от утечки информации или потери информационных данных. Таким образом, термин «информационный риск» имеет широкий экономический смысл и, как любое экономическое явление и категория, требует системного подхода к анализу, а в данном случае – к управлению.

На основании работ ряда исследователей представляется возможным определить сущность системного подхода и рассмотреть его основные свойства и характеристики [2–5]:

– базой возникновения системного подхода является общая теория систем;

– используя системный подход, необходимо иметь в виду, что ключевую роль здесь будут играть конечные цели использования системы и цели применения подсистем;

– системный подход предлагает согласование используемых методов и средств на базе единой методики, чтобы достичь поставленной целей системы или процесса;

– применение системного подхода возможно с целью решения проблемных задач, постановка и решение которых не могут быть осуществлены при помощи методов отдельных разделов математики;

– реализуя системный подход, необходимо использовать не только формальные методы, но и методы качественного анализа и синтеза, основанные на интуиции и опыте специалиста;

– в рамках системного подхода возможно объединение знаний специалистов в различных областях знаний;

– методы системного подхода дают возможность представить систему или процесс как связанные подсистемы (вложенные процессы) и провести их согласо-

ванное исследование, чтобы достичь конечных общих целей исследования системы или процесса;

– с использованием системного подхода в структуре системы или процесса необходимо строго определить границы, а также обозначить входные и выходные связи с внешними процессами и средой;

– при использовании системного подхода определение масштабов системы и внешних связей необходимо выбирать в соответствии с целями исследования.

Системное управление предполагает выделение систем, в соответствии с целями исследования и уровнем рассмотрения проблем. Сущность информационных рисков может быть рассмотрена с учетом двух взаимосвязанных систем – информационной системы предприятия (внутренней среды) и внешней среды.

В рамках системного анализа информационная система предприятия – это открытая система, образуемая множеством взаимосвязанных информационных элементов, позволяющих получать, обрабатывать, хранить и передавать необходимую информацию с целью эффективного функционирования предприятия. Информационные элементы данной системы – субъекты и объекты информационных процессов. К субъектам информационных процессов относят сотрудников предприятия, участвующих в процессах получения, обработки, хранения и передачи информации. Объекты – информационные ресурсы и материальные средства, обеспечивающие информационный процесс предприятия.

Внешняя информационная среда предприятия образуют объекты, субъекты, процессы и явления внешней среды, которые оказывают влияние на элементы информационной системы предприятия и на информацию во внешней среде, которая имеет отношение к предприятию и протекающим на нем бизнес-процессам.

Объединение указанных выше систем представляет собой единое явление нового порядка, которое, по мнению исследователей, является информационной сферой предприятия. При этом, исследователи считают, что информационная сфера не будет являться системой по причине иррационального взаимодействия между информационной системой предприятия и внешней средой. Иррациональность вызвана неупорядоченностью, нецелесообразностью, неопознаваемостью, непредсказуемостью и парадоксальностью во взаимодействии систем [6]. Именно указанная иррациональность и лежит в основе возникновения большинства информационных рисков, вызванных функционированием внутренней и внешней сред предприятия, их взаимодействием, имеющем отношение к информации, которая влияет на бизнес-процессы предприятия. Таким образом, наличие двух систем (внешней и внутренней) позволяет говорить о целесообразности использования системного подхода к управлению информационными рисками.

В процессе реализации системного подхода к управлению информационными рисками предполагается рассмотреть их причинно-следственные связи. В процессе изучении природы экономических рисков исследователями используются следующие понятия: причины, факторы риска, и собственно сам риск.

При рассмотрении соотношений причины и фактора риска нужно отметить, что определение внутренних источников активности процессов или объектов, которые порождают риски, происходит посредство выявления их причины. Факторы же являются обстоятельствами, которые способствуют реализации рисков. Так, исследуя причины информационных рисков, которые связаны с таким информационным объектом, как специалист, требуется рассмотрение мотивации поступков этого объекта [7].

Юнкерова Ю. И. Системное управление информационными рисками // Концепт. – 2013. – № 11 (ноябрь). – ART 13229. – 0,4 п. л. – URL: http://e-koncept.ru/2013/13229.htm. – Гос. рег. Эл № ФС 77-49965. – ISSN 2304-120X.

Факторы информационных рисков, в меньшей степени связаны с конкретными источниками риска, чем причины рисков. Они в основном отражают состояние информационной системы предприятия в целом. Понятие «фактор риска» часто является аналогом понятия «уязвимость системы», данное понятие используется в научных работах по защите информации. Непосредственная связь факторов риска с информационной системой предприятия налицо, а руководство предприятия может в полной мере осуществлять влияние на факторы риска путем снижения вероятности наступления рисковых событий в информационной системе предприятия.

Управление информационными рисками определяется политикой управления информационными рисками предприятия, которая разрабатывается руководством предприятия и является на предприятии официальным документом – «Программой управления информационными рисками предприятия», где производится определение и раскрытие следующих понятий:

– целей и задач управления информационными рисками;
– особенностей информационной системы и внешней системы предприятия, оказывающих влияние на условия управления информационными рисками;
– результатов анализа информационных рисков;
– основных научно-методических принципов создания, организации функционирования и развития системы управления информационными рисками;
– функций системы управления информационными рисками;
– порядка управления, мониторинг и аудит системы управления информационными рисками.

Указанная политика управления информационными рисками является руководящим началом при создании системы управления информационными рисками на предприятии.

Система управления информационными рисками является единым комплексом правовых норм, экономических и организационных мер, технических, программных и криптографических средств, а также информационных ресурсов, оказывающих воздействие на информационную сферу предприятия с целью обеспечения минимальных суммарных расходов на предотвращение информационных рисков и компенсацию ущерба от них.

Построение системы управления информационными рисками базируется на следующих принципах:

– принцип системного подхода к построению системы;
– принцип непрерывности функционирования системы;
– принцип равнозащищенности всех звеньев;
– принцип многоуровневой защиты;
– принцип адаптивности системы;
– принцип централизованного иерархического управления;
– принцип дружественного интерфейса;
– принцип открытости системы [8].

Системное управление информационными рисками предполагает обязательный анализ всех возможных для конкретной информационной системы предприятия видов информационных рисков. Полученная информация позволяет сделать выбор адекватных мер и средств, направленных на предотвращение рисков или снижения вероятности их реализации, а также на устранения последствий таких рисков.

Современная информационная система предприятия – многозвенная, многоуровневая система. Информацию получают, хранят, обрабатывают и передают различные звенья системы, при этом также используются различные формы ее представления. Перемещение информации по всему технологическому пути должно происходить без потери качества. Продвигаясь от источников к верхним уровням управления, значимость информации повышается, и это необходимо учитывать при системном управлении информационными рисками.

При системном управлении информационными рисками необходимо всестороннее исследование всех объектов, с которыми взаимодействует информационная система предприятия (внешних и внутренних), при этом желательно структурировать и формализовать связи системы управления информационными рисками с другими объектами.

Системе управления информационными рисками необходимо обеспечить устойчивость информационной системы предприятия к воздействию со стороны информационных рисков, а подобную устойчивость можно обеспечить только при помощи адаптивной системы. Чтобы решить эту задачу, информационная система предприятия должна обладать определенной избыточностью, позволяющей выполнять задачи по:

- постоянному мониторингу системы;
- определению и локализации рисков;
- оценке последствий реализации риска;
- реконфигурации системы, включая и человеческие ресурсы;
- обеспечению функционирования системы в условиях реализованного риска, возможно и с ухудшенными характеристиками;
- восстановлению объектов, поврежденных или утраченных ресурсов;
- обратной реконфигурации системы, для работы в штатном режиме;
- ликвидации последствий воздействия рисков на бизнес-процессы предприятия.

В человеко-машинах, в отличие от технических систем, человек принимает активное участие в компенсаторных механизмах. При этом им используется весь комплекс восстановительных механизмов, а также и организационные и экономические меры.

Системой управления информационными рисками предполагается выполнение сотрудниками определенных обязанностей, требующих регулярности и точности. Излишний уровень обременительности при общении с системой может вызвать у человека тягу к усовершенствованию процесса общения с системой за счет упрощения технологии взаимодействия, отказаться выполнять отдельные обязательные операции. Чтобы решить данную проблему, системе управления информационными рисками необходимо обеспечение дружественного интерфейса системы с сотрудниками предприятия [9].

Дружественный интерфейс – это безопасное и комфортное взаимодействие человека с системой, позволяющее достигать максимальной производительности человеко-машинной системы и обеспечить ее защищенность от информационных рисков. За счет применения дружественного интерфейса возможно сокращение количества неумышленных ошибок персонала, а также неукоснительное выполнение специалистами своих обязанностей по защите от информационных рисков.

Системное управление информационными рисками дает возможность выхода на качественно новый уровень управления. Представление информационной сферы предприятия в виде комплекса позволяет рассмотреть проблему управления информационными рисками целостно.

При системном управлении информационными рисками происходит учет всех негативных событий, которые влияют на безопасность и качество информации: дан-

ные события могут произойти на всех этапах информационного процесса от получения информации до ее использования в бизнес-процессах компании. За счет системного управления возможно согласованное применение всего комплекса механизмов управления, который направлен на достижение конечных целей бизнес-процессов. Повышается доступность экономических механизмов управления, а также усиливается значимость правовых и организационных методов управления.

Данный подход к пониманию сущности информационных рисков дает возможность заключить, что необходимо также в его рамках коренным образом изменить роль и значение менеджмента предприятия в управлении информационными рисками. Системное управление не будет полноценно реализовано без активного участия в процессе управления менеджеров, как среднего, так и высшего звена.

Необходимо адаптировать к управлению информационными рисками на более высоком уровне архитектуру информационной системы предприятия и, прежде всего, архитектуру системы управления информационными рисками. Изменение комплекса взаимосвязанных механизмов и методология их применения – это следствие расширения состава и качественного изменения выполняемых функций системы управления информационными рисками.

Ссылки на источники

1. Симонов С. В. Методология анализа рисков в информационных системах // Защита информации. Конфидент. – 2001. – № 1. – С. 72–76.
2. Там же.
3. Симонов С. В. Технологии аудита информационной безопасности // Защита информации. Конфидент. – № 2. – 2006. – С. 36–41.
4. Шумский А. А., Шелупанов А. А. Системный анализ в защите информации. – М.: Гелиос АРВ, 2008. – 224 с.
5. Щеглов А. Ю. Защита информации он несанкционированного доступа. – М.: Гелиос АРВ, 2005. – 384 с.
6. Там же.
7. Петренко С. А., Симонов С. В. Управление информационными рисками. Экономически оправданная безопасность. − М.: АйТи-Пресс, 2004. − 384 с.
8. Симонов С. В. Технологии ... Указ. соч.
9. Староверов Д. Оценка угроз воздействия конкурента на ресурсы организации // Защита информации. Конфидент. – № 2. – 2005. – С. 58–62.

***Yunkerova Yulia**,*
PhD student at the chair of economics and management of enterprise Scientific and Research Institute Belgorod State University, department of Belgorod State National Research University, Belgorod

System management of information risks

Abstract. The author examines the concept of systematic approach to the analysis of the essence of informational risk as well as the process of managing these risks. A holistic view of the problem of information risk management system is based on the fact that the external and internal enterprise systems are presented in complex. In order to achieve the ultimate goals of the business it is necessary to adapt the architecture of enterprise information system for this type of information risk management and also to provide an active a participation in the management of information risk management system.

Keywords: information risk, system management, external and internal environment, an architecture of the informational system, information safety.

ISSN 2304-120X
11
9 772304 120135

Рекомендовано к публикации:
Горевым П. М., кандидатом педагогических наук, главным редактором журнала «Концепт»;
Утёмовым В. В., кандидатом педагогических наук