УДК 004.056.5

В.В. ВЫСОЦКИЙ, докторант МАУП, начальник управления информационной безопасности, ООО "Итер Ком" (г. Киев)

ПРОБЛЕМЫ МИНИМИЗАЦИИ РИСКОВ ПРИ АУТСОРСИНГЕ ИНФОРМАЦИОННЫХ УСЛУГ

Рассмотрены причины, приводящие к передаче управления информационными процессами и функциями на обслуживание другой организации (аутсорсинг), а также угрозы, возникающие при этом. Предложены технические и административные методы и способы уменьшения рисков, связанных с различными видами угроз информационной безопасности, возникающие при аутсорсинге ИТ-услуг. Табл.: 1. Библиогр.: 11 назв.

Ключевые слова: информационные процессы, аутсорсинг, угрозы информационной безопасности, уменьшение рисков.

Постановка проблемы. В настоящее время, в период стремительно изменяющихся технологий, выживают и добиваются успеха те компании, которые ведут свой бизнес наиболее эффективным способом, снижая операционные расходы и сохраняя высокое качество товаров и услуг.

Одной из наиболее современных и успешных бизнес-моделей, позволяющих добиться реальных конкурентных преимуществ, является аутсорсинг, в частности ИТ-аутсорсинг, который предполагает делегирование внешней специализированной компании решение вопросов, связанных с разработкой, внедрением и сопровождением информационных систем как целиком на уровне инфраструктуры предприятия (сопровождение оборудования или ПО), так и объёмов работ, связанных с развитием и/или поддержкой функционирования отдельных участков системы.

При ИТ-аутсорсинге изменяются степени угроз безопасности информации, уменьшаются и исчезают одни виды рисков, а также появляются и увеличиваются другие виды рисков. Особенно остро данный вопрос касается небольших организаций, которые обычно не могут позволить себе содержать отдельного специалиста по информационной безопасности. Таким образом, стоит задача выявления рисков, возникающих и увеличивающихся при аутсорсинге информационных процессов, их оценка, а так же определение способов уменьшения таких рисков для малых и средних организаций.

Анализ литературы. В мировой практике отмечается стремительный прорыв аутсортинговых технологий в менеджменте организаций [1 – 10]. В научных публикациях последнего десятилетия определены основные пути и методы перехода на аутсорсинг [1]; формы аутсорсинга [2]; описаны концепции и техники использования различных моделей оценки рисков [3, 6, 8].

Выделяют следующие основные причины аутсорсинга [4,8]:

1. Отказ от непрофильных видов деятельности.

2. Необходимость повышения качества обслуживания.

3. Финансовая причина, за которой следует желание компании сфокусироваться на основных видах деятельности [8].

В современном менеджменте организаций можно выделить три основные формы ИТ-аутсорсинга [2]:

– Ресурсный аутсорсинг (аутсорсинг персонала).

– Функциональный аутсорсинг.

– Стратегический аутсорсинг – подразумевает полную передачу управления ИТ-службами компании аутсорсеру.

Как и большинство других государств, Украина испытывает дефицит специалистов сферы информационных технологий (ИТ). По данным аналитической компании IDC [5] из года в год увеличивается нехватка специалистов в области сетевых технологий. В связи с этим, содержание полноценного штата квалифицированных сотрудников IT-отдела в данный момент достаточно дорогостояще и не всегда возможно. В этом случае имеет смысл воспользоваться услугами компаний-аутсорсеров. Это позволит наладить работу информационных систем, решить проблему нехватки высококвалифицированных ИТ-специалистов, уменьшить затраты на обеспечение работы ИТ-отдела, сфокусироваться на ведении основного бизнеса. Но при переходе на аутсорсинг возникают новые риски и увеличивается вероятность некоторых существующих рисков. Большинство новых рисков аутсорсинга было рассмотрено в литературе на протяжении последних десяти лет, в то время как вопросу роста рисков информационной безопасности при аутсорсинге уделялось мало внимания.

Цель статьи – анализ рисков безопасности информации, возникающих при передаче управления собственными информационными процессами и функциями малых и средних предприятий на обслуживание другой организации, а так же разработка рекомендаций по минимизации как самих рисков, так и вероятности их происхождения для малых и средних предприятий.

Виды угроз, возникающих при использовании информационных технологий, и первичный анализ изменения степени риска при аутсорсинге. По природе возникновения угрозы можно разделить на два класса:

– естественные или объективные – вызванные стихийными природными явлениями, не зависящими от человека. При аутсорсинге данный вид угроз может быть полностью устранен, например, за счет географически разнесенных хранилищ данных, резервных офисов и т.п.

– искусственные или субъективные, которые, в свою очередь, можно разделить на непреднамеренные угрозы, вызванные ошибками при проектировании, во время монтажа оборудования и его эксплуатации – при аутсорсинге уменьшаются; и преднамеренные угрозы, связанные с

определенными устремлениями людей, такими как терроризм, забастовки, хищения, кражи, несанкционированный доступ в компьютерные сети и т.п.

Умышленные угрозы подразделяются на активные и пассивные. Пассивные – направлены на несанкционированное использование информационных ресурсов, не оказывая при этом влияния на ее функционирование. Активные угрозы имеют целью нарушение нормального функционирования информационной системы путем целенаправленного воздействия на ее компоненты.

При аутсорсинге наиболее значимыми угрозами информационной безопасности являются утечка и компрометация информации, несанкционированное использование информационных ресурсов, нарушение информационного обслуживания, незаконное использование привилегий. Это происходит из-за того, что компания-исполнитель получает доступ к конфиденциальным данным и оборудованию предприятия, тем самым увеличивается количество людей, имеющих такой доступ.

Зависимость степени рисков от форм и методов аутсорсинга. Исходя из видов угроз можно определить, что при необходимости повышения качества обслуживания, в случае внедрения аутсорсинга будут уменьшаться риски, связанные с естественными и искусственными причинами, но при этом будет увеличиваться вероятность угроз, источник которых расположен внутри контролируемой зоны, за счет доступа к этой зоне организации, осуществляющей аутсорсинг. При этом, в общем, опасность перебоев в работе сервиса будет уменьшаться, особенно если используется ресурсный аутсорсинг и несколько поставщиков ресурсов.

В случае превалирования финансовой составляющей, изменение степени риска зависит от опыта и знаний, которыми обладали уволенные сотрудники ИТ по сравнению с опытом и знаниями сотрудников, работающих в организации, предоставляющей аутсорсинг. При прочих равных условиях, степень риска будет увеличиваться за счет внутренних угроз.

Аутсорсинг за счет отказа от непрофильных видов деятельности несет в себе те же риски, что и аутсорсинг по финансовым причинам, но при этом финансовая составляющая не имеет такого приоритета, что позволяет использовать больше ресурсов и за счет этого уменьшить внешние риски.

Оценка важности различных сервисов. Была произведена оценка важности различных сервисов до и после передачи на аутсорсинг. Оценка основывалась на качественной модели, опросы проводились среди руководителей малых и средних предприятий, менеджеров по бизнес-направлениям, менеджеров ИТ.

Итоговая оценка указывается в виде удельного веса важности каждого сервиса, т.е. чем больше вес, тем больше влияние данного сервиса на работу организации и тем более важной является задача минимизации как самого риска, так и его вероятности.

Таблица 1

Оценка важности сервисов

Сервис	Вероятность передачи на аутсорттинг, %	Риск перебоев в работе сервиса,%		Риск уничтожения данных,%		Риск утери данных,%	
		До	После	До	После	До	После
Электронная почта	85	70	15	52	0	86	86
Системы мгновенной передачи сообщений (IM)	95	23	30	8	0	35	50
Системы совместного пользования данными	60	82	20	93	0	75	90
Представительские WEB-приложения	95	3	0	40	0	0	0
Бухгалтерские приложения	50	48	20	96	0	78	85
Системы ERP	70	85	37	92	0	64	85
Системные приложения	90	78	10	5	0	0	0
Офисные приложения (календарь, список задач, менеджер проектов и т.п.)	85	24	10	77	0	12	20
Служба печати	70	43	20	0	0	45	50
Локальная вычислительная сеть	70	98	30	0	0	67	85
Интернет	100	56	56	0	0	23	23
Система документооборота	80	23	23	87	0	68	80
Юридическая справочная система	100	48	0	0	0	0	0

Под риском перебоев в работе сервиса понимается временная недоступность сервиса на срок, критичный для данной организации. Риск утери данных означает вероятность того, что данными завладеет конкурирующая фирма. Риск уничтожения данных означает вероятность безвозвратной потери данных без возможности их восстановления.

Исходя из данных таблицы, можно сделать следующие выводы:

– в небольших организациях уделяется мало внимания утере данных, обычно гораздо меньше, чем уничтожению

– все респонденты отметили отсутствие опасности уничтожения данных при условии наличия у них резервных копий данных, находящихся у

поставщика услуг. Следует учесть, что некоторые сервисы, такие как Интернет, являются переданными на аутсорсинг по-умолчанию.

– респонденты отмечают повышение риска утери данных при передаче сервисов на аутсорсинг, это показывает их боязнь, что данные попадут к конкурентам либо окажутся в открытом доступе, в случае если компания-аутсорсер будет иметь доступ к этим данным. При этом данная величина не имеет обратной корреляции со степенью готовности передать перечисленные сервисы на аутсорсинг, хотя такое соответствие следовало бы ожидать.

Рекомендации по минимизации рисков. Одним из основных технических методов по минимизации рисков от внедрения ИТ-аутсорсинга является разграничение доступа, например, компания-аутсорсер, в первую очередь, может взять под свой контроль средства защиты от внешних угроз, при этом клиент сконцентрируется непосредственно на внутренних критичных ресурсах сети. Такой подход уменьшает риски от внешних угроз, но при этом практически не увеличивает внутренние риски, например, от утечки данных. Также доступ можно ограничить исходя из степени секретности информации, т.е. клиент предварительно проводит анализ собственных данных и на аутсорсинг передаются только те ИТ-ресурсы, которые не содержат критически важной информации.

К административным методам минимизации рисков можно отнести, во-первых, работа компании-аутсорсера по международным стандартам, следствием чего является прозрачность, контролируемость и экономическая обоснованность аутсорсинговых процессов. Во-вторых, четкое разграничение зон ответственности, определение задач поставщика аутсорсинговых услуг и закрепление всего этого в соответствующих соглашениях. Единственный аспект, неподвластный соглашениям и международным стандартам, это "человеческий фактор".

Одним из важнейших требований при аутсорсинге является мониторинг ключевых показателей эффективности, по которым можно отслеживать эффективность построенной системы информационной безопасности и которые могут быть интегрированы в систему управления рисками. Кроме того, должен выполняться мониторинг заранее установленных мероприятий, нацеленных на уменьшение объема убытка или частоты появления рисков.

При оценке влияния поставщика ИТ услуг на степень риска можно исходить из идеализированного представления о таком поставщике, так как степень приближения к идеальности можно определить еще при выборе такого поставщика. В этом случае опасность перебоев и опасность уничтожения данных стремятся к нулю. Для оценки вероятности возникновения таких опасностей у конкретного поставщика услуг достаточно выяснения таких вещей как: наличие процедур резервного копирования и восстановления, дублирование каналов связи, географическое разнесение хранилищ данных. Учитывая это, значимой является только опасность утери данных, что позволяет предложить следующие методы для уменьшения этих рисков:

– первоначально выводить на аутсорсинг только сервисы с низким удельным весом потери данных;

– в случае систем совместного использования данных, а также других систем, где это возможно, осуществлять шифрование данных;

– периодическое предоставление клиенту резервной копии данных, принадлежащих клиенту, но находящихся у поставщика аутсорсинга.

Выводы. Сделанный анализ и методы уменьшения рисков относятся к малым и средним предприятиям, так как крупные предприятия имеют больше возможностей для административного и технического управления рисками, вплоть до выделения отдельных сотрудников или даже отделов для этого. При этом в малых предприятиях существует тенденция к переносу своих ИТ-сервисов на аутсорсинг, но практически отсутствуют ресурсы для контроля предоставляемых услуг. В результате проделанной работы были проанализированы и оценены основные риски, возникающие при передаче управления информационными процессами малых и средних предприятий сторонней организации, а также определены методы уменьшения рисков, что имеет важное значение в современных условиях, т. к. все больше предприятий используют аутсорсинг ИТ-услуг.

Список литературы: 1. *Sparrow E*. Successful IT Outsourcing / *Elizabeth Sparrow*. – Springer, 2003 – 288 p. **2**. ИТ-аутсорсинг гайд [Електронний ресурс] : (портал Outsourcing). – 2010 – Режим доступу: http://www.outsourcing.ru/content/rus/rubr58/rubr-583.asp – Назва з екрана. **3**. *Embrechts P*. Quantitative Risk Management: Concepts, Techniques, and Tools / *Alexander J. McNeil, Rüdiger Frey, Paul Embrechts*. – Princeton University Press, 2005. – 608 p. **4**. *Хейвуд Дж. Б*. Аутсорсинг. В поисках конкурентных преимуществ / *Хейвуд Дж. Б*. – Вильямс, 2002 – 176 с. **5**. Дефицит специалистов по сетевым и телекоммуникационным технологиям к 2008 году может стать критическим [Електронний ресурс] (Cisco Systems, Inc.) – 2005 – Режим доступу: http://www.cisco.com/web/RU/news/releases/txt/0443.html – Назва з екрана. **6**. *Miora M***.** Quantifying the Business Impact Analysis: A New Model / *M. Miora* [Електронний ресурс] – Режим доступу http://www.miora.com/articles/gcc.htm. **7**. *Беркович В.* Вопросы информационной безопасности при аутсорсинге IT-процессов компании / *В. Беркович, А. Коптелов* [Електронний ресурс] – 15.05.2007 – Режим доступу http://citcity.ru/15815/ **8**. *Wilson K*. Deep Dive: Emerging Challenge: Risk Management in an Outsourced World / *K. Wilson* [Електроний ресурс] – 2009 – Режим доступу: http://www.corporatecomplianceinsights.com/wp-content/uploads/pdf/risk-management-in-outsourced-world-karen-wilson.pdf. **9.** Информационные технологии управления: Учеб. пособие для вузов / Под ред. проф. Г.А. Титоренко. – 2-е изд., доп. – М.: ЮНИТИ-ДАНА, 2003. – 439 с.

Статья представлена д.т.н., ведущим научным сотрудником физико-механического института им. Г.В. Карпенка НАНУ А.Я.Тетерко.

УДК 004.056.5

Проблеми мінімізації ризиків при аутсортингі інформаційних послуг / Висоцкій В.В. // Вісник НТУ "ХПІ". Тематичний випуск: Інформатика і моделювання. – Харків: НТУ "ХПІ". – 2010. – № 31. – С. 58 – 64.

Розглянуті причини, що призводять до передачі управління інформаційними процесами та функціями на обслуговування сторонньому підприємству (аутсорсинг), а також загрози, які виникають при цьому. Запропоновані технічні й адміністративні методи та способи зменшення ризиків, що пов'язані з різними видами загроз інформаційній безпеці, які виникають при

аутсорсингу IT-послуг. Табл.: 1. Бібліогр.: 9 назв.

Ключові слова: інформаційні процеси, аутсорсинг, загрози інформаційній безпеці, зменшення ризиків**.**

UDC 004.056.5

Problems of minimization of risks at autsorsinge of informative services / Visotsky V.V. // Herald of the National Technical University "KhPI". Subject issue: Information Science and Modelling. – Kharkov: NTU "KhPI". – 2010. – №. 31. – P. 58 – 64.

The reasons leading to the transfer of information management processes and functions in the service of another organization (outsourcing), as well as the threats arising in this case. The technical and administrative methods and ways to mitigate the risks associated with various types of information security threats arising from the outsourcing of IT services. Tabl.: 1. Refs.: 9 titles.

Keywords: information processes, outsourcing, information security threats, reducing risks.

Поступила в редакцию 01.04.2010