Maksimova Elena Aleksandrovna – Volgograd State University; e-mail: Maksimova@volsu.ru; 100, Universitetsky pr. Volgograd, 400062, Russia; phone: +78442460368; the department of informational security; cand. of eng. sc.; associate professor.

Omelchenko Tatyana Aleksandrovna – e-mail: omelchenkotanya@mail.ru; the department of informational security; student.

Alekseenko Valerii Vladimirovich – e-mail: infsec@volsu.ru; the department of informational security; postgraduate student.

УДК 004.056.5, 004.89

А.М. Цыбулин, В.А. Балдаев, А.А. Бешта

АУТСОРСИНГ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Российские компании стали использовать аутсорсинг с целью отказаться от непрофильных активов и сконцентрироваться на основном направлении своего бизнеса. При реализации своих услуг компания аутсорсер получает доступ к ресурсам и компонентам информационной системы, что приводит к изменению уровня угроз безопасности информации, уменьшаются и совсем исчезают одни риски и появляются новые риски. Актуальными проблемами являются своевременная идентификация, оценка и минимизация старых и новых рисков, а также автоматизация этих процессов. Проводится анализ услуг аутсорсинга, строится дерево угроз информационной системе при аутсорсинге и рассчитывается остаточный риск. Для обеспечения безопасности ИС при передаче ее на аутсорсинг проводятся работы по минимизации рисков: подготовка ИС к передаче на аутсорсинг, оценка уровня информационной безопасности в процессе и после аутсорсинга, а в случае снижения уровня, проведение работы по восстановлению уровня информационной безопасности. Предлагаются модель и алгоритмы по оценке и минимизации рисков при аутсорсинге на основе данных мониторинга, аудита, инвентаризации программного и аппаратного обеспечения. Разработан программный комплекс, который позволяет автоматизировать процесс минимизации рисков.

Аутсорсинг; аутсорсер дерево угроз; инсайдерская деятельность; информационная безопасность; инвентаризация; мониторинг; остаточный риск.

A.M. Tsybulin, V.A. Baldaev, A.A. Beshta

OUTSOURCE AND INFORMATION SECURITY

The Russian companies began to use outsourcing in order to abandon non-core assets focus on the general direction of their business. When implementing its services company - outsourcer gets access to resources and components of the information system, which leads to change of a level of information security threats, reduce and completely disappear, some risks and new risks are emerging. The actual problems are timely identification, assessment and minimization of old and new risks, as well as the automation of these processes. Outsourcing services are analyzed, a tree of threats to the information system in outsourcing is built, and residual risk is calculated. To ensure the security of information system when sending it to outsourcing a number of works to reduce the risks is carried out. It is proposed to include in this work: preparation of information system to the outsourcing, assessing the level of information security during and after outsourcing, and in the case of level reduce carrying out repair work. Algorithms are proposed for the assessment and minimizing risks during outsourcing based on monitoring data, inventory of hardware and software. The program complex, which allows to automate the process of minimizing the risks is developed.

Outsourcing; outsourcer; tree of threats; insider activity; information security; inventory; monitoring; the residual risk.

В связи с постоянным усложнением информационных систем компаний и ростом потребности в них, найти квалифицированный ИТ-персонал становится всё сложнее, да и сам персонал постоянно дорожает. Для разрешения этой проблемы всё

больше российских компаний начинают пользоваться услугами ИТ-аутсорсинга, следуя примеру Европейских компаний, где затраты на ИТ-аутсорсинг составляют в среднем более 50 % ИТ-бюджета. Использование ИТ-аутсорсинг позволяет компаниям отказаться от непрофильных активов и сконцентрироваться на основном направлении своего бизнеса [1, 2]. Но при передаче компонентов информационной системы (ИС) на аутсорсинг очень острой становится проблема обеспечения её информационной безопасности [3, 4].

При передаче компонентов ИС на аутсорсинг возникают следующие новые условия окружения [5]:

- расширяется круг лиц, допущенных к работе с ИС;
- более активное использование внешних каналов связи;
- неизвестная исходная защищенность инфраструктуры аутсорсера;
- неизвестный круг третьих лиц, получающих доступ к инфраструктуре и системе, включая физический уровень;
- отсутствие контроля над регламентами и их исполнением на стороне провайдера;
- инсайдерская деятельность;
- отсутствие оперативной обратной связи и информирования по инцидентам ИБ на стороне аутсорсера.

Аутсорсер получает доступ ко всем компонентам ИС.

Оценки рисков ИС при передаче на аутсорсинг будут ассоциированы с компонентами ИС (табл. 1).

Таблица 1

Компоненты и методы оценки рисков

Компонент ИС	Методы оценки риска
Аппаратное обеспечение	Инвентаризация аппаратного обеспечения до, в процессе и после аутсорсинга с возможностью контроля изменений
Программное обеспечение (в том числе прикладное)	Инвентаризация и мониторинг программного обеспечения до, в процессе и после аутсорсинга с возможностью контроля изменений
Конфигурационные файлы	Резервное копирование конфигурационных файлов на внешний носитель и восстановление с него
Базы данных	Резервное копирование баз данных на внешний носитель и восстановление с него.
Другая информация, не содержащаяся в базах данных (электронные документы, изображения и т.д.)	Резервное копирование другой информации на внешний носитель и восстановление с него

Услуги аутсорсинга, ассоциированные с угрозами для информационной системы представлены в [5], с добавлением компонент ИС, приведены в табл. 2. По данной таблице строится дерево угроз информационной системе при ее аутсорсинге. На рис. 1 приведено дерево угроз для типовой ИС.

Анализ дерева угроз информационной безопасности показывает, что актуальными являются угрозы на все три свойства информации: доступность, целостность и конфиденциальность.

В связи с этим актуальным является вопрос разработки системы оценки информационной безопасности ИС в процессе и после аутсорсинга.

Предлагается модель информационной системы с позиции информационной безопасности, которая фиксирует основные угрозы ресурсам ИС: доступ к конфиденциальной информации на рабочих станциях пользователей, злоумышленное воздействие на вспомогательные активы, нарушение качества сервиса, угрозы природного и техногенного характера, несанкционированное сетевое взаимодействие, доступ к данным об инцидентах ИБ под контролем аутсорсера, а не заказчика, доступ аутсорсера к конфиденциальной информации, содержащейся в бизнес-приложениях, нарушение необходимого качества сервиса в связи с удаленностью инфраструктуры. На основе модели и дерева угроз рассчитывается остаточный риск для ИС [6, 7 ,8].

Таблица 2

Угрозы для информационной системы и ее компонент, связанные с услугами аутсорсинга

Услуга аутсорсинга	Компонент ИС	Угроза
Поддержка пользователей	Аппаратное обеспечение, программное обеспечение, конфигурационные файлы, базы данных, другая информация	Доступ к конфиденциальной информации на рабочих станциях пользователей в результате передачи на аутсорсинг
Управление вспомогательными активами	Аппаратное обеспечение, программное обеспечение	Воздействие на вспомогательные активы в результате передачи на аутсорсинг
		Нарушение качества сервиса в результате передачи на аутсорсинг
Поддержка непрерывности бизнеса	Аппаратное обеспечение, программное обеспечение, базы данных, конфигурационные файлы	Угрозы природного и техногенного характера затрагивающие аутсорсера
Управление сетями	Аппаратное обеспечение, конфигурационные файлы, другая информация	Несанкционированное сетевое взаимодействие в результате передачи на аутсорсинг
Управление безопасностью	Аппаратное обеспечение, программное обеспечение, конфигурационные файлы, другая информация, базы данных	Данные об инцидентах ИБ под контролем Исполнителя, а не Заказчика
Поддержка приложений	Программное обеспечение, конфигурационные файлы, другая информация	Доступ к конфиденциальной информации, содержащейся в бизнес-приложениях в результате передачи на аутсорсинг
Хостинг приложений	Программное обеспечение, конфигурационные файлы, другая информация, базы данных	Нарушение необходимого качества сервиса в связи с удаленностью инфраструктуры в результате передачи на аутсорсинг

Для обеспечения безопасности ИС при передаче ее на аутсорсинг необходимо провести работы по минимизации рисков. Предлагается включить в эти работы: подготовку ИС к передаче на аутсорсинг, оценку уровня информационной безопасности в процессе и после аутсорсинга, а в случае его снижения уровня провести работы по восстановлению.

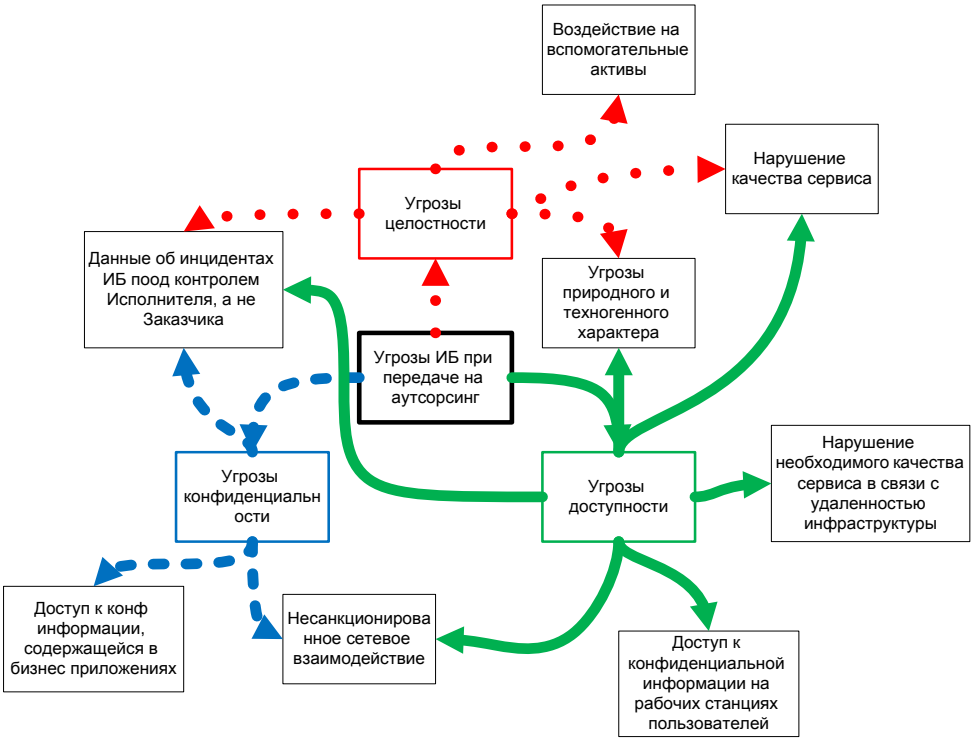


Рис. 1. дерево угроз для типовой информационной системы при передаче ее на аутсорсинг

Подготовка ИС к передаче на аутсорсинг включает работы по защите: баз данных путем их шифрования и резервного копирования; от несанкционированной модификации файлов конфигурации и программного обеспечения ИС путем расчета контрольных сумм и их сохранения на в базе данных на отдельном носителе или рабочем месте; от несанкционированной модификации аппаратных средств ИС путем их инвентаризации и сохранения в базе данных; расчета остаточного риска для ИС и сохранения его значения в базе данных.

Оценка уровня информационной безопасности в процессе аутсорсинга предполагает периодическое представление заказчику возможности проведение мониторинга состояния базы данных и ИС в целом, инвентаризации программного, аппаратного обеспечения ИС и расчет остаточного риска. Оценка уровня информационной безопасности после аутсорсинга аналогична оценке в процессе аутсорсинга.

Для автоматизации процесса минимизации рисков разработаны модель, алгоритмы и программный комплекс на языке C#, который включает следующие модули: пользовательский интерфейс, агентов инвентаризации, мониторинга и аудита программного и аппаратного обеспечения, агент базы данных, агент резервного копирования, агент файлов конфигурации, агент расчета остаточного риска и ряд вспомогательных агентов.

Результаты опытной эксплуатации показали, что программный комплекс обеспечивает решение возложенных на него задач. На рис. 2 показан результат выявления агентом инвентаризации после аутсорсинга ИС новой программы Proxifier version 3.21, которая привела к повышению остаточного риска.

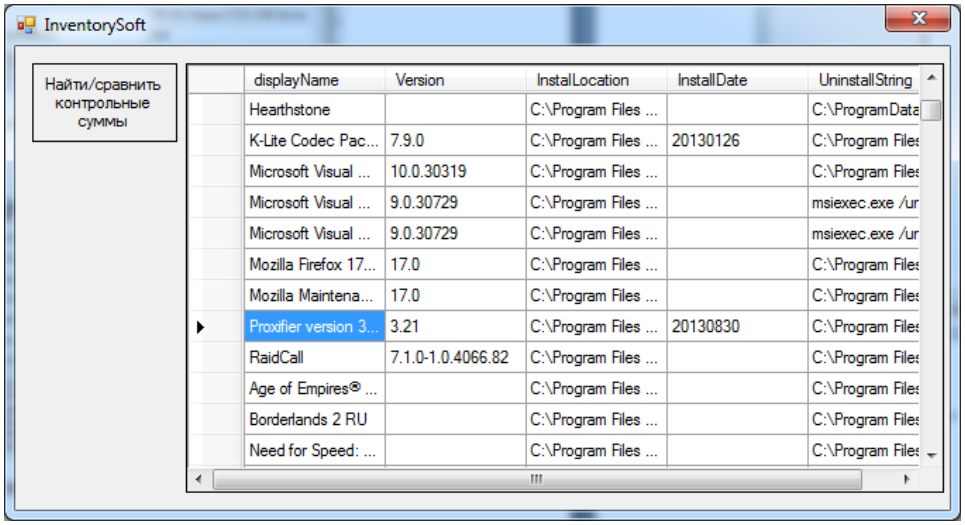


Рис. 2. Сообщение о появление новой программы Proxifier version 3.21

Результаты расчета общего уровня угроз по компоненту, риска по компонентам и риска по информационной системе после проведения аутсорсинга приведены на рис. 3.

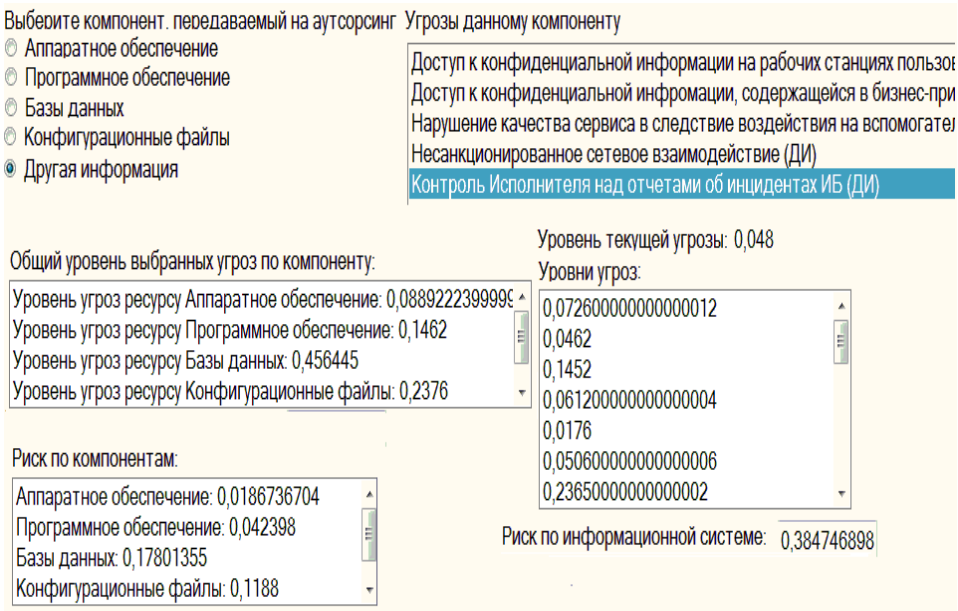
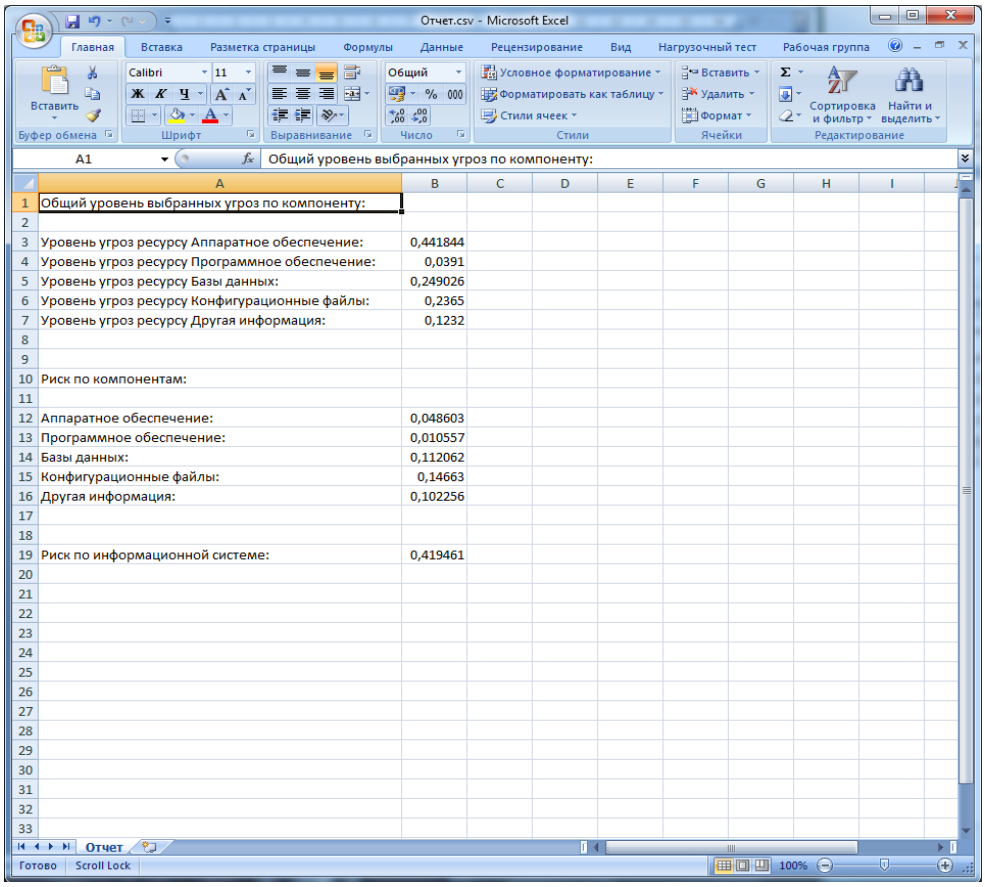


Рис. 3. результаты расчета общего уровня угроз по компоненту, риска по компонентам и риска по информационной системе после проведения аутсорсинга

Общий вид отчета по уровню рисков после аутсорсинга приведен на рис. 4.



	A	B
1	Общий уровень выбранных угроз по компоненту:	
2		
3	Уровень угроз ресурсу Аппаратное обеспечение:	0,441844
4	Уровень угроз ресурсу Программное обеспечение:	0,0391
5	Уровень угроз ресурсу Базы данных:	0,249026
6	Уровень угроз ресурсу Конфигурационные файлы:	0,2365
7	Уровень угроз ресурсу Другая информация:	0,1232
8		
9		
10	Риск по компонентам:	
11		
12	Аппаратное обеспечение:	0,048603
13	Программное обеспечение:	0,010557
14	Базы данных:	0,112062
15	Конфигурационные файлы:	0,14663
16	Другая информация:	0,102256
17		
18		
19	Риск по информационной системе:	0,419461

Рис. 4. Общий вид отчета в файле Excel (экранная копия)

Выводы. Проанализированы и оценены основные риски, возникающие при передаче управления информационными процессами компании аутсорсеру, а также разработаны модель, алгоритмы минимизации рисков и программный комплекс, позволяющий автоматизировать оценку остаточных рисков.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Готтшальк П.* ИТ-аутсорсинг. Построение взаимовыгодного сотрудничества. Ханс Солли-Сетер. Изд-во: Альпина Паблишер, 2007. – 394 с.
2. *Аникин Б.А., Рудая И.Л.* Аутсорсинг и аутстаффинг, Высокие технологии менеджмента. – 2-е изд., перераб. и доп. – М.: Инфра-М, 2009. – 320 с.
3. Сетевые решения: Вопросы информационной безопасности при аутсорсинге IT-процессов компании. http://www.nestor.minsk.by/sr/2007 /08/sr70812.html.
4. Информационная безопасность при аутсорсинге IT-процессов компании. http://dchel.ru/service/?ID=49472.
5. *Мелехин И.* Риски информационной безопасности при передаче систем на аутсорсинг. [Доклад в виде презентации]. Системный интегратор Информзащита. – 2012. URL: http://www.myshared.ru/slide/93059/.
6. *Бешта А.А.* Архитектура программного комплекса контроля над внутренним злоумышленником // Известия ЮФУ. Технические науки. – 2013. – № 12 (149). – С. 157-163.

7. *Цыбулин А.М.* Архитектура автоматизированной системы управления информационной безопасностью предприятия // Известия ЮФУ. Технические науки. – 2011. – № 12 (125). – С. 58-64.
8. *Кавчук Д.А., Тумоян Е.П., Астафьев Г.А.* Интеллектуальный подход к анализу рисков и уязвимостей информационных систем // Известия ЮФУ. Технические науки. – 2013. – № 12 (149). – С. 79- 86.

Статью рекомендовал к опубликованию д.т.н., профессор О.Б. Макаревич.

Цыбулин Анатолий Михайлович – Волгоградский государственный университет; e-mail: anatsybulin@yandex.ru; 400062, г. Волгоград, пр. Университетский, 100; тел.: 88442460368; кафедра информационной безопасности; зав. кафедрой; к.т.н.; доцент.

Балдаев Вадим Андреевич – e-mail: infsec@volsu.ru; кафедра информационной безопасности; студент.

Бешта Александр Александрович – кафедра информационной безопасности; старший преподаватель.

Tsybulin Anatoly Mihaylovich – Volgograd State University; e-mail: anatsybulin@yandex.ru; 100, pr. Universitetsky,Volgograd, 400062, Russia; phone: +78442460368; the department of informational security; head of department.

Baldaev Vadim Andreevich – e-mail: infsec@volsu.ru; the department of informational security; student.

Beshta Aleksandr Aleksandrovich – the department of informational security; lecturer.

УДК 658.14

Е.П. Соколовский, О.А. Финько

ИНФОРМАЦИОННАЯ ПОДДЕРЖКА УПРАВЛЕНИЯ ЗАПАСАМИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В УСЛОВИЯХ НЕОПРЕДЕЛЕННОСТИ

Воздействие угроз информационной безопасности на объект информатизации и систему защиты информации порождает слабо прогнозируемый спрос на израсходованные (утраченные) элементы средств защиты информации. Для обеспечения функционирования системы защиты информации с требуемым качеством необходимо иметь запас наиболее востребованных элементов средств защиты информации. Рассматриваются такие системы защиты информации, для которых создается запас элементов средств защиты информации. В известных моделях управления запасами учитывается вероятностный характер спроса на предметы снабжения, однако возможность управления информационными потоками, циркулирующими в логистических системах, как правило, не используется. В целях обеспечения информационной поддержки процесса управления запасами элементов средств защиты информации в условиях неопределенности предлагается подход, основанный на управлении информационными потоками в интегрированных логистических системах и известном методе АВС-анализа.

Система защиты информации; информационная безопасность; запасы средств защиты информации.