

УДК 658.6

АНАЛИЗ ЭКОНОМИЧЕСКОЙ ВЫГОДЫ АУТСОРСИНГА ДЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Иваев М.И.,

Поволжский государственный университет телекоммуникаций и информатики, Самара,
email: Sihovcovairina14@gmail.com; ivaevmarat@ya.ru

Шиховцова И.А.,

Поволжский государственный университет телекоммуникаций и информатики, Самара,
email: Sihovcovairina14@gmail.com; ivaevmarat@ya.ru

Оникейчук Д.Д.,

Поволжский государственный университет телекоммуникаций и информатики, Самара,
email: Sihovcovairina14@gmail.com; ivaevmarat@ya.ru

Аннотация. Анализ экономической выгоды аутсорсинга для информационной безопасности является важным аспектом принятия решения о внедрении такой стратегии в организации. Аутсорсинг информационной безопасности подразумевает передачу определенных функций и задач, связанных с обеспечением безопасности данных и информационных систем, третьей стороне, специализирующейся в этой области. Первоначальное преимущество аутсорсинга информационной безопасности заключается в снижении затрат на поддержание собственного ИТ-отдела, который специализируется на защите данных и информационных систем. Вместо того, чтобы нанимать сотрудников, обеспечивать их обучение и постоянное обновление знаний, аутсорсинг позволяет воспользоваться услугами уже опытных и квалифицированных специалистов. Это может значительно снизить расходы на заработную плату, обучение, оборудование и программное обеспечение.

Ключевые слова: информационная безопасность, цифровая экономика, угрозы, снижение затрат, экономия времени, гибкость, снижение рисков.

ANALYSIS OF THE ECONOMIC BENEFITS OF OUTSOURCING FOR INFORMATION SECURITY

Ivaev M.I.,

Volga State University of Telecommunications and Informatics, Samara,
email: Sihovcovairina14@gmail.com; ivaevmarat@ya.ru

Shikhovtsova I.A.,

Volga State University of Telecommunications and Informatics, Samara,
email: Sihovcovairina14@gmail.com; ivaevmarat@ya.ru

Onikeychuk D.D.,

Volga State University of Telecommunications and Informatics, Samara,
email: Sihovcovairina14@gmail.com; ivaevmarat@ya.ru

Abstract. Analyzing the economic benefits of outsourcing for information security is an important aspect of deciding whether to implement such a strategy in an organization. Information security outsourcing involves transferring certain functions and tasks related to ensuring the security of data and information systems to a third party specializing in this area.

The initial advantage of information security outsourcing is the reduction in costs of maintaining an in-house IT department that specializes in protecting data and information systems. Instead of hiring employees, providing them with training and constantly updating their knowledge, outsourcing allows you to use the services of already experienced and qualified specialists. This can significantly reduce costs for salaries, training, equipment and software.

Keywords: Information security, digital economy, threats, cost reduction, time saving, flexibility, risk reduction.

Аутсорсинг информационной безопасности — это процесс передачи управления и обеспечения защиты информации компании третьей стороне. Эта модель стала все более популярной среди компаний, так как позволяет экономить ресурсы и получить квалифицированную поддержку в области информационной безопасности. Разработка модели компании, занимающейся аутсорсингом информационной безопасности, является важной задачей для обеспечения надежной защиты информации.

ИБ-аутсорсинг включает в себя:

- внедрение и настройку системы мониторинга передачи информации по сетевым каналам и на внешние устройства (DLP);
- анализ перехвата DLP и выявление нарушений;
- составление подробных отчетов по инцидентам.



Рис. 1. Схема начала работы аутсорсинга в компании

Результаты исследования

Анализ эффективности аутсорсинга включает ряд общих принципов, которые помогают определить, насколько успешно и выгодно предприятие использует аутсорсинг, такие как:

1. Цель и ожидания: необходимо четко определить цель использования аутсорсинга и осознать, какие ожидания относятся к данному процессу. Ожидания могут включать сокращение расходов, повышение качества услуг, концентрацию на основной деятельности и т.д.

2. Расчет экономической эффективности: необходимо провести расчеты, чтобы оценить, будет ли аутсорсинг более выгодным, чем выполнение работ внутри компании. Расчеты могут включать оценку затрат на оборудование, персонал, обучение, а также сравнение цен на рынке аутсорсинговых услуг.

3. Качество услуг: следует оценить потенциального аутсорсингового партнера и его способность предоставлять качественные услуги. Необходимо проанализировать репутацию компании, ее опыт работы на рынке, наличие сертификатов и т.д.

4. Риск и контроль: оценка рисков и возможности контроля является важным аспектом анализа эффективности аутсорсинга. Необходимо определить, какие риски

могут возникнуть при передаче работы третьей стороне и какие меры предпринимать для их снижения. Также следует определить, какие контрольные механизмы можно использовать для отслеживания работы аутсорсингового партнера.

5. Долгосрочное планирование и стратегия: анализ эффективности аутсорсинга должен учитывать долгосрочную перспективу и стратегические цели компании. Необходимо оценить, какие выгоды может принести аутсорсинг на протяжении длительного периода времени и какой будет его вклад в общую стратегию развития компании.

Эти принципы помогут предприятию осуществить адекватный анализ эффективности аутсорсинга и принять обоснованное решение о его использовании.

Где же понадобится аутсорсинг?

Аутсорсинг информационной безопасности может быть полезен для различных организаций и учреждений. Вот несколько примеров:

1. Крупные предприятия: Крупные компании, имеющие большое количество конфиденциальной информации, могут воспользоваться услугами аутсорсинга информационной безопасности, чтобы эффективно защищать и управлять своей информацией.

2. Малые и средние предприятия: Малые и средние предприятия могут не иметь достаточных ресурсов или экспертизы в области информационной безопасности. Аутсорсинг позволяет им получить доступ к профессиональным услугам безопасности без необходимости создания собственного внутреннего отдела по безопасности.

3. Государственные учреждения: Государственные учреждения, такие как правительство и образовательные учреждения, также могут воспользоваться аутсорсингом информационной безопасности, чтобы защитить свою конфиденциальную информацию и данные граждан.

4. Медицинские учреждения: Медицинские учреждения обрабатывают большое количество конфиденциальных медицинских данных пациентов. Аутсорсинг информационной безопасности может быть важным для обеспечения безопасности этих данных и соблюдения нормативных требований, таких как Закон о порatabельности и учете медицинской информации (HIPAA) в США.

5. Финансовые учреждения: Банки, страховые и инвестиционные компании работают с критически важными финансовыми данными своих клиентов. Аутсорсинг информационной безопасности может помочь им обеспечить безопасность и защиту этих данных от киберугроз и утечек информации.

В целом, аутсорсинг информационной безопасности, может быть полезен для любой организации или учреждения, которое хочет эффективно защитить свою информацию и данные, независимо от их размера или отрасли.

Как начать процесс аутсорсинга информационной безопасности?

Начать процесс аутсорсинга информационной безопасности можно следующим образом:

1. Оценка текущей информационной безопасности: Начните с проведения аудита информационной безопасности вашей компании. Оцените уровень рисков, уязвимостей и потенциальных угроз для систем и данных.

2. Определение потребностей: Определите, какие именно аспекты информационной безопасности вы хотите аутсорсить. Это может быть мониторинг безопасности, оценка уязвимостей, защита от вредоносного ПО и т. д.

3. Поиск подходящего поставщика: Проведите исследование и найдите подходящего поставщика услуг аутсорсинга информационной безопасности. Исследуйте их репутацию, опыт работы и сертификации.

4. Проведение проработки: Составьте необходимые документы, такие как соглашение о конфиденциальности и обязательствах по безопасности, чтобы обеспечить безопасность данных и ответственность сторон.

5. Запуск: Начните процесс аутсорсинга информационной безопасности, предоставив выбранному поставщику доступ к системам и данным. Убедитесь, что приведены четкие инструкции и согласованы показатели безопасности.

6. Контроль и управление: Внедрите механизмы контроля и управления услугами аутсорсинга информационной безопасности. Наблюдайте за эффективностью и соответствием предоставляемых услуг.

7. Периодический анализ и обновление: Регулярно анализируйте свои потребности и оценивайте эффективность услуг аутсорсинга информационной безопасности. Обновляйте соглашения и процессы, чтобы соответствовать новым требованиям и угрозам.

Основные достоинства и недостатки аутсорсинга

Плюсы анализа экономической выгоды аутсорсинга для информационной безопасности:

1. Снижение затрат: аутсорсинг информационной безопасности может быть более экономичным, чем содержание внутреннего отдела по информационной безопасности. Это позволяет снизить расходы на рабочую силу, оборудование, программное обеспечение и обучение.

2. Экспертное мнение: аутсорсинг позволяет получить экспертное мнение и опыт специалистов в области информационной безопасности, что может помочь увеличить эффективность и надежность мер по защите информации.

3. Фокус на бизнесе: аутсорсинг информационной безопасности позволяет компании сосредоточиться на своем основном бизнесе и повысить эффективность работы, не отвлекаясь на вопросы безопасности.

Минусы анализа экономической выгоды аутсорсинга для информационной безопасности:

1. Потеря контроля: сотрудничество с внешним поставщиком услуг по информационной безопасности может привести к потере контроля над данными и системами компании. Это может создавать риск утечки данных или несанкционированного доступа.

2. Конфиденциальность данных: передача конфиденциальных данных третьей стороне влечет риск нарушения конфиденциальности. Компания должна быть уверена в безопасности и надежности поставщика услуг перед тем, как передать ему конфиденциальную информацию.

3. Культурные различия: аутсорсинг информационной безопасности за рубежом может создать проблемы из-за культурных различий и различия в подходах к безопасности. Это может привести к непониманию и снижению эффективности сотрудничества.

Почему аутсорсинг выгоден?

Аутсорсинг экономически выгоден по нескольким причинам:

1. Снижение затрат. Передача определенных функций или процессов бизнеса внешнему поставщику услуг позволяет сократить расходы на заработную плату, аренду офисов и инфраструктуру, закупку оборудования и программного обеспечения и т. д.

2. Экономия времени и ресурсов. Заказчику услуг достаточно только описать требования и ожидания, а весь процесс выполнения работ и контроля за ним будет лежать на поставщике услуг. Это позволяет компании сосредоточиться на своих основных задачах и не отвлекаться на дополнительные функции.

3. Лучшие навыки и опыт. Внешний поставщик услуг, специализирующийся в определенной сфере, может обладать большим опытом и компетенциями. Благодаря этому, заказчик получает доступ к передовым знаниям и технологиям, которые можно применить для повышения эффективности своего бизнеса.

4. Гибкость. Аутсорсинг позволяет быстро масштабировать или сокращать объемы работы в зависимости от потребностей компании. Это особенно актуально в случае временных проектов или временного увеличения загрузки.

5. Снижение рисков. Аутсорсинг позволяет снизить риски, связанные с нехваткой специалистов, ограниченными ресурсами или изменяющимися требованиями рынка. В случае обмена внешнего поставщика услуг, компания может легко заменить его на другого поставщика.

Эти факторы помогают компаниям улучшить эффективность и конкурентоспособность, снизить затраты и риски, а также ускорить процессы и повысить качество работы.

Аутсорсинг информационной безопасности стал неотъемлемой частью современных бизнес-моделей. Многие компании вместо того, чтобы содержать внутренние отделы по информационной безопасности, предпочитают передать эту функцию в руки внешних поставщиков услуг. Такой подход может обеспечить значительные экономические преимущества.

Первое и наиболее очевидное преимущество аутсорсинга информационной безопасности — это снижение затрат. Ведение и поддержание собственного отдела по информационной безопасности требует значительных вложений в закупку, установку и обновление необходимого оборудования, программного обеспечения и регулярное обучение персонала. Также не следует забывать о затратах на создание и поддержание инфраструктуры, необходимой для хранения, обработки и передачи информации. При аутсорсинге компания перекладывает большую часть этих затрат на стороннего поставщика.

Первоначальные затраты на аутсорсинг информационной безопасности могут казаться значительными, однако стоит рассмотреть долгосрочные выгоды, которые он предоставляет. Одной из главных причин внедрения аутсорсинга информационной безопасности является снижение затрат на персонал и инфраструктуру.

Кроме того, использование услуг аутсорсинга информационной безопасности позволяет сократить расходы на персонал. Обучение и поддержка высококвалифицированных специалистов в области информационной безопасности требует значительных затрат времени и денег. Когда же компания передает эти функции внешнему поставщику, она получает доступ к команде профессионалов, обладающих необходимыми знаниями и опытом, без необходимости содержать такой отдел внутри компании.

Аутсорсинг информационной безопасности позволяет снизить затраты на обновление и поддержание инфраструктуры. Компании-аутсорсеры обычно имеют современное программное и аппаратное обеспечение, что позволяет снизить затраты на покупку и обновление необходимых технологий.

Другим важным аспектом экономической выгоды аутсорсинга информационной безопасности является гибкость и масштабируемость. Стандартные услуги аутсорсинга предлагают возможность выбора пакета услуг, оптимально соответствующего потребностям компании. При необходимости компания может легко масштабировать или уменьшить объем услуг, а также внести изменения в работу отдела в зависимости от текущих потребностей. Возможность гибко регулировать затраты на информационную безопасность позволяет компании оптимизировать использование своих ресурсов и сфокусироваться на основных бизнес-процессах.

Помимо этого, аутсорсеры часто имеют доступ к передовым технологиям и инструментам, которые позволяют эффективнее контролировать и защищать информацию. Это может включать в себя использование современных механизмов анализа данных и идентификации угроз, мониторинга сетевой активности и анализа уязвимостей системы.

Кроме того, аутсорсинг информационной безопасности может способствовать повышению эффективности работы компании. Профессиональные поставщики услуг в этой области обладают глубокими знаниями и экспертизой, что позволяет им эффективно анализировать угрозы и риски, разрабатывать стратегии предотвращения инцидентов и реагировать на них с большей оперативностью. Благодаря этому компания может сохранить свою репутацию, избежав серьезных инцидентов, которые могут негативно сказаться на бизнесе.

В целом, аутсорсинг информационной безопасности предоставляет компаниям множество экономических преимуществ. Благодаря снижению затрат, улучшению эффективности работы, гибкости и доступу к опыту, аутсорсинг становится все более привлекательным для организаций, стремящихся обеспечить надежную информационную безопасность и оптимизировать использование своих ресурсов.

В конечном счете, аутсорсинг информационной безопасности может принести значительные экономические выгоды компании. Это включает в себя снижение затрат на персонал и инфраструктуру, сокращение рисков и улучшение эффективности в области информационной безопасности.

Однако, при принятии решения об аутсорсинге информационной безопасности необходимо учесть ряд факторов. Например, важно выбрать надежного и квалифицированного партнера, проверить его репутацию и опыт работы в данной области. Также стоит учесть юридические и комплаенс-аспекты, чтобы убедиться, что передача информации и данных будет осуществляться в соответствии с требованиями законодательства.

Выводы

В завершение, аутсорсинг информационной безопасности может стать ценным инструментом для компаний, которые стремятся добиться оптимальной защиты своей информации и минимизировать экономические риски. Важно тщательно взвесить все плюсы и минусы данного подхода и принять решение, которое будет наиболее соответствовать потребностям и целям компании в области информационной безопасности.

Литература

1. Организация ИТ-аутсорсинга. [Электронный ресурс]. URL: <https://intuit.ru/studies/courses/4820/1072/lecture/16431?page=1> (дата обращения 25.03.2024).
2. Аутсорсинг ИТ и ИБ — оценка экономической эффективности и рисков использования. [Электронный ресурс]. URL: <https://www.elvis.ru/upload/iblock/ab7/ab7274f899135a156e660dcacsb2d33b.pdf> (дата обращения 25.03.2024).
3. Анализ эффективности аутсорсинга. [Электронный ресурс]. URL: <https://businessprocess.narod.ru/index28.htm> (дата обращения 25.03.2024).
4. Щеглов В.Ю., Скворцов А.О. Использование ИТ-аутсорсинга для обеспечения экономической безопасности предприятия // Известия высших учебных заведений. 2018. № 2 (8). С. 29-34.
5. Названы плюсы ИБ-аутсорсинга для малого и среднего бизнеса. [Электронный ресурс]. URL: <https://telesputnik.ru/materials/trends/news/nazvany-plyusy-ib-autsorsinga-dlya-malogo-i-srednego-biznesa> (дата обращения 25.03.2024).
6. Аутсорсинг информационной безопасности. [Электронный ресурс]. URL: <https://safe-surf.ru/specialists/article/5253/642419/> (дата обращения 25.03.2024).
7. Тихонова А.С., Ермашкевич Н.С. Методы оценки эффективности аутсорсинга как инструмента организации и оптимизации затрат труда в компаниях // Креативная экономика. 2020. Т. 14. № 7. С. 1369-1388. DOI: 10.18334/ce.14.7.110532.
8. Аутсорсинг и аутстаффинг услуг ИБ: мнение экспертов. [Электронный ресурс]. URL: <https://lib.itsec.ru/articles2/control/autsorsing-i-autstaffing-uslug-ib-mnenie-ekspertov> (дата обращения 25.03.2024).