3. Доклад о состоянии окружающей среды Волгоградской области в 2011 году. – Волгоград: Смотри, 2012. – 352 с.
4. Долгосрочная программа по энергосбережению и повышению энергетической эффективности Волгоградской области на 2010 -2020 гг. Утв. Пост. № 347-п Админ. обл. от 26.07.2010 г. // Электронный ресурс «Консультант Плюс» – 2013.

ИТ РИСКИ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Исаев И.В.

Волгоградский государственный аграрный университет, Волгоград, e-mail: isav7779@gmail.com

Проанализированы наиболее значимые информационные риски ИТ. Произведена категоризация ИТ-рисков. Представлен процесс организации процесса минимизации рисков. Охарактеризованы основные правила минимизации ИТ-рисков. Представлен комплекс мер по минимизации ИТ-рисков.

Обеспечение информационной безопасности – одна из главных задач современного предприятия. Угрозу могут представлять не только технические сбои, но и несогласованность данных в различных учетных системах, которая встречается едва ли не у каждой второй компании, а также неограниченный доступ сотрудников к информации.

Кроме этого ещё более серьезную угрозу могут представлять любые форс-мажорные обстоятельства (пожары, затопления), несущие катастрофические последствия для существования бизнеса.

Информационные риски – это опасность возникновения убытков или ущерба в результате применения компанией информационных технологий. Иными словами, ИТ-риски связаны с созданием, передачей, хранением и использованием информации с помощью электронных носителей и иных средств связи.

ИТ-риски можно разделить на две категории:

• риски, вызванные утечкой информации и использованием ее конкурентами или сотрудниками в целях, которые могут повредить бизнесу;

• риски технических сбоев работы аппаратного и программного обеспечения, каналов передачи информации, которые могут привести к убыткам.

Работа по минимизации ИТ-рисков заключается в предупреждении несанкционированного доступа к данным, а также аварий и сбоев оборудования и программного обеспечения.

Процесс минимизации ИТ-рисков:

1. Выявление возможных проблемы, а затем определение способов их решения.

2. Определение сроков интеграции новых технологий при необходимости, по причине преобразования или слияния организации.

3. Оптимизация бизнес-процессов организации.

4. Обеспечение защиты интеллектуальной собственности организации и ее клиентов.

5. Разработка порядка действий при форс-мажорных обстоятельствах.

6. Определение фактических потребностей информационных ресурсов.

Некоторые способы минимизации рисков:

Для обеспечения необходимой защиты от ИТ-рисков и контроля безопасности можно провести следующие мероприятия.

Определить круг лиц, отвечающих за информационную безопасность, создать нормативные документы, в которых будут описаны действия персонала компании, направленные на предотвращение ИТ-рисков, а также обеспечить резервные мощности для работы в критической ситуации.

Разработать единые стандарты информационных систем в рамках организации, то есть перейти к единым отчетным формам, а также единым правилам расчета показателей, которые будут применяться во всех программных продуктах компании, используемых для этой цели.

Классифицировать данные по степени конфиденциальности и разграничить права доступа к ним.

Следить за тем, чтобы любые документы, обращающиеся внутри организации, создавались с помощью систем, централизованно установленных на компьютерах. Установка любых других программ должна быть санкционирована, иначе риск сбоев и вирусных атак резко возрастет.

Внедрить средства контроля, позволяющие отслеживать состояние всех корпоративных систем: в случае несанкционированного доступа система должна или автоматически запрещать вход, или сигнализировать об опасности, чтобы персонал мог принять меры.

Разработать и создать систему, позволяющую оперативно восстановить работоспособность ИТ- инфраструктуры при технических сбоях.

Помимо перечисленных мер необходимо подготовиться к последствиям возможных кризисных ситуаций и описать действия компании по выходу из кризиса.

Обязательным условием успешного риск-менеджмента в области информационных технологий является его непрерывность. Поэтому оценка ИТ-рисков, а также разработка и обновление планов по их минимизации должны производиться с определенной периодичностью, например раз в квартал. Периодический аудит системы работы с информацией (информационный аудит), проводимый независимыми экспертами, будет дополнительно способствовать минимизации рисков.

В заключение отметим, что разработка и реализация политики по минимизации ИТ-рисков не принесет пользы, если рекомендуемые стандарты и правила неверно используются, например, если сотрудники не обучены их применению и не понимают их важности. Поэтому работа по обеспечению ИТ-безопасности должна быть комплексной и продуманной.

АКТУАЛЬНЫЕ ПРОБЛЕМЫ В СФЕРЕ СОГЛАШЕНИЙ ОБ УРОВНЕ ПРЕДОСТАВЛЕНИЯ УСЛУГ

Исаев И.В.

Волгоградский государственный аграрный университет, Волгоград, e-mail: isav7779@gmail.com

Проанализирована необходимость в четкой организации взаимодействия между потребителями и поставщиками информационных услуг. Выявлены и охарактеризованы наиболее актуальные проблемы, сдерживающие применение соглашений об уровне предоставления услуг. Проанализированы примеры использования данного вида соглашений.

На определенном этапе успешного развития любого ИТ-проекта перед теми, кто принимает решения, возникает дилемма, о том как поддерживать работоспособность бизнеса. Необходима четкая схема взаимоотношений между организациями, предоставляющими информационные услуги, и потребителями этих услуг. Таким образом сформировалась необходимость регулирования таких вопросов путем соглашений на предоставление услуг с должным качеством.

Соглашение на предоставление услуг (SLA) – это контракт, регламентирующий отношения между сервис-провайдером и его клиентом. Степень важности этого документа предполагает должные усилия для его грамотной разработки. На данный момент актуальны некоторые заблуждения относительно данного направления:

1. Отсутствует необходимость в SLA.

SLA – это правообразующий документ. Именно в нем закреплено партнерство продавца и потребителя услуг. Его нельзя игнорировать ни в коем случае. На данный момент не существует стандартных норм и устоявшихся отечественных обычаев делового оборота для регулирования качества предоставляемых информационных сервисов. Поэтому SLA – единственный путь для установления взаимных прав, обязанностей, гарантий и компенсаций.

2. SLA только описывает предоставляемые услуги.

Описание услуг – основной предмет SLA, что вполне естественно. Любая продуктивная совместная работа возможна при наличии общего языка. Именно при составлении SLA компании согласовывают общую терминологию. Помимо указания на то, что и кому предоставляется, четко составленный SLA содержит множество важнейших подразделов: цель сотрудничества, его продолжительность, график предоставления услуг, условия оплаты, условия расторжения, гарантии, размеры компенсаций. SLA – основной и единственный инструмент для регулирования вопросов в сфере предоставления ИТ-услуг.

3. В SLA не должны быть указаны бизнес-цели клиента.

Это не совсем так. Всеобъемлющее понимание основных приоритетов в бизнесе потребителя дает организации, предоставляющей услуги, четкие ориентиры – каким образом нужно действовать при возникновении проблем с обслуживанием клиента.

4. Оплата производится за предоставленные услуги.

В определении цены при составлении SLA важнейший фактор – не сама услуга, а качество ее предоставления. Размер оплаты рассчитывается лишь исходя из определенных качественных критериев, таких, как доступность, время, требуемое для устранения сбоев и т.д. К примеру, американская компания Intira, специализирующаяся на веб-хостинге, указывает в своих SLA, что она компенсирует каждые 15 минут отсутствия доступа к ресурсам клиентов одним днем бесплатного обслуживания и так – вплоть до месяца бесплатного обслуживания в год.

5. Все провайдеры предоставляют стандартные SLA.

Это правда – некоторые даже уделяют место универсальности договорной базы в своей маркетинговой стратегии. Однако подавляющее большинство провайдеров идет навстречу пожеланиям пользователей, особенно корпоративных. Здесь просто не может идти речи о шаблонном SLA. Так, вице-президент аутсорсинговой компании Nuclio Corp. Майк Коффилд (Mike Coffield) отмечает, что каждый SLA его компании строится вокруг бизнес-требований конкретного клиента. На разработку соглашения подчас уходит до трех недель. «Мы не навязываем SLA пользователю, – отмечает Коффилд. – Мы вносим туда все, что ему необходимо».

6. Качество предоставляемых услуг невозможно измерить.

Это главное заблуждение относительно SLA. В зависимости от типа услуги, потребители могут измерить качество ее предоставления по одному из параметров: доступность; среднее количество сбоев за определенный период, их динамика; время, затрачиваемое на их устранение. Вице-президент e-commerce-портала Commerce One Inc. (компания предоставляет услуги хостинга и co-location для сотен известных американских компаний) Сэм Пратер (Sam Prather) отмечает: «На третий день после оформления SLA с компанией Siterock наши технические специалисты не получили ни единого уведомления о сбое. Через месяц услуги Siterock, обходящиеся нашей компании в $15 тыс., сэкономили нам $1,5 млн., избавили нас от головной боли и сохранили нам ценных специалистов». В настоящее время целым рядом экспертных организаций по всему миру разрабатываются унифицированные системы материальной оценки качества услуг в сфере ИТ.

7. Условия SLA распространяются только на того, кто его подписывает.

В случае с пользователем – абсолютно верно. В случае с сервис-провайдером – нет, поскольку он, как правило, является лишь звеном целой инфраструктуры организаций, предоставляющих ИТ-услуги. Качество работы одного провайдера зависит от работы многих других. Часто имеют место SLA внутри подобных структур, они учитывают интересы конечных пользователей. Однако в любом случае SLA должен содержать пункт об ответственности за ущерб, нанесенный третьими лицами.

Секция «Математическое и компьютерное моделирование в экономике», научный руководитель – Магомедгаджиев Ш.М., канд. экон. наук, доцент

ОЦЕНКА ВЗАИМОВЛИЯНИЯ УРОВНЯ ИНФОРМАТИЗАЦИИ И СОЦИАЛЬНО-ЭКОНОМИЧЕСКИХ ПОКАЗАТЕЛЕЙ РЕГИОНОВ: МЕТОДАМИ ЭКОНОМЕТРИЧЕСКОГО МОДЕЛИРОВАНИЯ

Магомедова С.Р.

Дагестанский государственный университет, Махачкала, e-mail: adamadziev@mail.ru

Информационно-коммуникационные технологии (ИКТ) занимают сегодня важное место в инновационном развитии ключевых сфер жизнедеятельности общества: государственного и муниципального управления, бизнеса, образования, здравоохранения, культуры, обеспечения безопасности, общественной жизни. Россия в настоящее время активно включилась в процесс развития информационного общества. Приняты стратегия развития информационного общества в Российской Федерации, государственная программа Российской Федерации «Информационное общество (2011–2020 годы)» и целый ряд других нормативно–правовых актов.

Использование ИКТ отличается неравномерностью в различных регионах, что привело к появлению нового вида пространственной и социальной поляризации – информационного неравенства.

В настоящее время разработаны и применяются различные методы количественной оценки уровня информатизации регионов. Один из методов анализа уровня развития и использования ИКТ в регионах России предполагает расчет Индекса готовности регионов к информационному обществу (ИО-индекс). Методика его расчета разработана Институтом развития информационного общества. В соответствии с это методикой Индекс рассчитывается на основе 77 различных показателей, в т.ч. показателей использования ИКТ в шести сферах (государственном и муниципальном управлении, образовании, здравоохранении, бизнесе, культуре, домохозяйствах) [3].