Иван БАБЕНКО,
Республика Молдова

ИСПОЛЬЗОВАНИЕ ITIL ДЛЯ УВЕЛИЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В МАЛЫХ И СРЕДНИХ ПРЕДПРИЯТИЯХ

This article will provide a general overview of ITIL and discuss how ITIL can improve how small and medium organizations implement and manage information security.

ITIL (Библиотека Инфраструктуры ИТ) – это наиболее распространенный подход к управлению ИТ как поставщика услуг. ITIL представляет собой взаимосвязанный набор методов или лучших практик (“best practice”), взятых как из опыта общественных и государственных организаций, так и предприятий частного сектора. Основой подхода являются книги Библиотеки ITIL.

В настоящее время подходом ITIL руководствуются основные государственные организации и отрасли в таких странах, как США, Великобритания, Германия, Франция и др. Причем прослеживается зависимость между доходностью отраслей и применением в них опыта ITIL.

Дополнением ко всем преимуществам ITIL, как показывает западная практика, методология может служить балансом между IT и потребностями бизнеса, улучшая качество обслуживания и уменьшая затраты на содержание и поддержку IT-службы. Такой подход может помочь улучшению обстановки, связанной с информационной безопасностью.

Библиотека ITIL была разработана в 1980-х британскими учеными, как попытка максимизировать эффективность и рентабельность использования многих ресурсов. Опыт ITIL совершенно оправданно применяется не только в государственной сфере и в крупных компаниях и целых отраслях. Необходимо перенести этот опыт управления в сектор среднего и малого бизнеса. Особенно это становится необходимым сейчас, когда проблемы информационной безопасности начали все чаще затрагивать не только интересы государства и крупных коммерческих структур, но и интересы более мелких структур и субъектов общества, которые не могут себе позволить содержание IT-отдела и обилие защитных средств, представленных на рынке.

ITIL использует подход, в основе которого, заложено эффективное управление и обеспечение предоставлением услуг. В соответствии с ITIL – все действия в бизнесе разделены на процессы, каждый из которых имеет три уровня:

Стратегический: цели организации определены посредством намеченного плана и методологии достижения целей.

Тактический: стратегия переведена в соответствующую организационную структуру и финансовую зависимость для достижения определенных результатов. На данном уровне описывается, какие процессы должны быть выполнены, какие активы должны быть развернуты и каков должен быть результат завершения процесса.

Эксплуатационный: Данный уровень предполагает, что тактические планы выполнены, а стратегические цели достигнуты в пределах указанного времени. На этом уровне проходит анализ выполненных процессов. С возможным переходом в следующую фазу к стратегическому уровню.

Приведем краткие общие описания некоторых процессов ITIL. Особое внимание уделим процессам, обеспечивающим поддержку и предоставление ИТ-сервисов (IT Service Management или ITSM), которые, наряду с процессом Управления информационной безопасностью, существенно влияют на поддержание информационной безопасности. Дадим их расшифровку для сектора малого и среднего бизнеса.

- *Управление Конфигурациями*: Методология для управления конфигурациями производства (например, стандартизацией, контролем состояний, выявление активов). Эти методы составляют логическую модель инфраструктуры, что само по себе является организационной функцией, которая всегда предшествует и предопределяет формирование политики Информационной Безопасности.
- *Управление Инцидентами*: Методы для решения инцидентов (любые события, вызывающие простои, сокращение объемов или ухудшение качества производимых товаров и услуг), и быстрого восстановления функционирования системы. Данная методология указывает на необходимость ее восстановления в кратчайшие сроки после возникновения инцидента. Этот метод полностью отвечает требованиям стандарта ISO 17799 и может находить свое применение в любых масштабах без существенных препятствий.
- *Управление Проблемами*: Свод методов для идентификации причины инцидентов и

предотвращения их повторного возникновения. Основная идея – проактивное предотвращение инцидентов и проблем. Это также частично является административной задачей, кроме этого, подразумевает и некоторый технико-технологический аппарат для защиты и противодействия, который могут себе позволить далеко не все предприятия.

- *Управление Изменениями*: Методы для стандартизации и разрешения вопросов, связанных с изменением в организационной структуре. Эти методы реализуют переход системы через внесение изменений с минимальным неблагоприятным воздействием на функционирование системы, и главным образом на качество вырабатываемого продукта, что также входит в состав ISO стандартов.
- *Управление Релизами*: Методы применяются для выпуска аппаратных средств и программного обеспечения. Они регламентируют проверку и исправление версий программного обеспечения, и аппаратных средств. Также это может быть применено к выпуску нового вида продукции и услуги. Данная методика может помочь в решении проблемы взаимоотношений с клиентами и предусмотреть все риски, связанные с выпуском продукта.
- *Управление Доступностью*: Данная методика регламентирует предоставление продуктов и услуг клиенту (например, оптимизация обслуживания и минимизация числа инцидентов при этом). Эти методы обеспечивают надежность, эластичность, и восстанавливаемость инфраструктуры, что также пересекается со стандартами в области Информационной Безопасности.
- *Финансовое Управление*: Методология служит для понимания и управления стоимостью обеспечения услуг (например, составления бюджета, бухгалтерского учета и т.д.). Происходит регламентация эффективного, экономного (в экономическом отношении) и рентабельного бизнеса. Что, в свою очередь, можно понимать и как финансовую сферу информационной безопасности в экономических системах.
- *Управление Уровнем услуг*: Методология должна применяться в системах для гарантии взаимного удовлетворения клиентов и владельцев системы. Эта методика обеспечивает контроль качества, утверждение и обратную связь для клиента системы и персонала системы. А сама по себе обратная связь с клиентом и своевременная реакция на предпосылки к инциденту могут послужить хорошей базой для предотвращения инцидентов и противодействия угрозам информационной безопасности.

Как видно из вышеописанных процессов, использование ITSM является хорошим средством для поддержания информационной безопасности. Возникает вопрос – каким образом можно справиться с управлением этими процессами малому и среднему бизнесу?

Ответ очевиден – с развитием экономики, все большая часть работ переходит на сторону аутсорсинга. Таким образом, управление этими процессами должно быть возложено на аутсорсинговые организации, занимающиеся предоставлением такого рода услуг и сопровождением. В таком случае для внедрения ISO 17799 и сводных стандартов с применением ITIL достаточно только построить соответствующим образом внутреннюю структуру, внедрить автоматизированную систему и передать е под управление соответствующей организации предоставляющей пакет услуг по допустимой цене за счет сопровождения большого количества предприятий и опыта работы в данной сфере.

Другим преимуществом использования ITIL является применимость современных HelpDesk- и ServiceDesk-решений в масштабах малого и среднего бизнеса, которые могут быть сопряжены с CRM/ERP решениями, а также систем планирования и учета с большой степенью интеграции. Ведь потеря информации и отсутствие инструментов для анализа ситуации в случае инцидентов для современных предприятий являются критическими проблемами. В настоящее время это зачастую решается на уровне организации и структуры предприятия, но упускается аспект информационной безопасности.

Заключение

Информационные меры безопасности стабильно расширяют свои возможности, увеличивают свою сложность и тем самым обретают исключительную важность. Для малых организаций содержать свою собственную подсистему информационной безопасности опасно, дорого, и неэффективно. ITIL позволяет заменять эти процессы стандартизированными, интегрированными процессами, основанными на “best practice” методах. Причем эффективность повышается при использовании аутсорсинга, участия “третьих лиц” и программных средств нового поколения, основанных на ITIL. Некоторые усилия здесь требуются, но все же решение проблемы информационной безопасности становится реальным для любых масштабов деятельности.