АНАЛИЗ ПРОБЛЕМ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ПРЕДПРИЯТИЯ

З.В. Родионова, к.т.н., доцент
Новосибирский государственный университет экономики и управления «НИНХ»,
г. Новосибирск
E-mail: rodionova_z@ngs.ru

В связи с растущей сложностью современного бизнеса, предприятия осуществляют непрерывное обновление технологий, устанавливают более мощное и качественное оборудование, вносят изменения в бизнес-процессы и информационные системы. В результате чего, процесс обеспечения безопасности информационных систем является трудоемким, дорогостоящим, а также слабо формализованным [1, 2].

Специалисты в области информационной безопасности отмечают, что инвестиции предприятий в обеспечение информационной безопасности (покупка средств защиты, затраты на оплату труда, затраты на проведения внешнего и внутреннего аудита безопасности и др.), неуклонно увеличиваясь из года в год и как правило не окупаются. Процесс создания системы управления информационной безопасностью предприятия не относится к основным видам деятельности, таким как производство товаров и предоставление услуг и как следствие должен быть экономически обоснован и оправдан.

Эффективная система управления информационной безопасностью предприятия адаптирует и изменяет требования к защите ресурсов в зависимости от изменений бизнес-процессов, которые в свою очередь подвержены влиянию внешней и внутренней среды [3-4]. К внешним изменениям относятся изменения, обусловленные законодательством или организационно-распорядительными документами вышестоящих органов (министерств, ведомств, государственных регуляторов). Внутренние изменения могут быть обусловлены оптимизацией бизнес-процессов, совместным использованием информационных ресурсов с другими предприятиями, изменениями технологий обработки информации и др. Указанные изменения могут касаться всех элементов системы информационной безопасности: от информационных ресурсов, концептуальных документов, инструкций и регламентов до конфигурации программно-технических решений.

Функционирование системы управления информационно безопасностью предприятия основывается на процессе результативного управления рисками. Процесс анализа угроз и оценки рисков информационной безопасности является непрерывным, исходные данные определяются на этапе создания системы информационной безопасности, далее в процессе ее функционирования производится мониторинг изменения угроз и рисков, их повторный анализ и оценка. Как правило, источником данных для проведения подобного вида работ являются результаты интервьюирования и анкетирования работников предприятия и внешних экспертов, которые получены в ходе предпроектного обследования и последующего аудита.

Предприятие, как живой организм, который постоянно подвержен изменениям. Оперативно отслеживать и интерпретировать такие изменения на настройки системы управления информационной безопасность – это трудоемкий процесс, который требует больших временных затрат. Анализ моделей бизнес-процессов даёт возможность отследить влияние происходящих изменений на многие аспекты информационной безопасности. Бизнес-процесс можно рассматривать, как источник знаний для управления рисками информационной безопасности, так как для достижения цели любого бизнес-процесса необходим определенный набор информационных ресурсов [5-6].

Можно сделать вывод о том, что эффективную систему управления информационной безопасностью предприятия можно построить использую процессный подход к управлению, что закреплено в разделе 0.2. «Процессный подход» стандарта ГОСТ Р ИСО МЭК 27001-2006. Процессный или системный подход позволяет анализировать систему в целом, а не отдельные её части. Практическая реализация применения процессного подхода для управления информационной безопасностью наталкивается на существенные сложности, которые прежде всего связаны с отсутствием описания четких механизмов, с другой с неопределенностью источников знаний.

Следующие факторы могут существенно снизить эффективность внедрения процессного подхода или свести все усилия к нулю: разработка моделей бизнес - процессов, не соответствующих действительности; только формальное внедрение управленческих процедур на уровне документации; отсутствие вовлеченности персонала; отсутствие поддержки высшего руководства; непонимание сотрудниками предприятия идеи процессного подхода и нежелание участвовать в ее воплощении.

В заключение следует отметить, что построение эффективной системы управления информационной безопасностью является сложным и непрерывным процессом, от которого зависит жизнеспособность предприятия.

Список литературы

1. Шардаков, Е.А. Совершенствование процесса построения информационных систем в образовательном учреждении с использованием технологий управления бизнес-процессами / Е.А. Шардаков, П.М. Пашков // Вестник НГУЭУ. – 2014. – № 3. – С. 228 – 239.
2. Большаков А.А., Долинина О.Н., Шатохин В.В. Управление образовательным процессом на основе автоматизированных комбинированных обучающих систем / А.А. Большаков, О.Н. Долинина, В.В. Шатохин // Вестник СГТУ, №2(35), 2008, с.54-62.
3. Родионова З.В. Технология управления изменениями прав доступа на основе анализа бизнес-процессов / З.В. Родионова // Вестник НГУЭУ. – 2011. – № 1– С. 16 - 21.
4. Родионова З.В. [и др.] Информационная система управления правами доступа на основе анализа бизнес-процессов / Т.М. Пестунова, З.В. Родионова // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2010. – № 2 (22). – Ч.2. – С. 253 - 256.
5. Родионова, З.В. [и др.] Управление процессом предоставления прав доступа на основе анализа бизнес-процессов / Т.М. Пестунова, З.В. Родионова // Прикладная дискретная математика. – Красноярск: Издательство научно-технической литературы, 2008. – С. 91 - 95.
6. Родионова З.В. Анализ аспектов информационной безопасности на основе формальных моделей бизнес-процессов / Пестунова Т.М., Родионова З.В., Горинова С.Д. // Доклады ТУСУР. – Томск. – 2014. – С. 150-156.