УДК 004.056:378(06)

ПОДХОД К ПОСТРОЕНИЮ МОДЕЛИ СИСТЕМ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Доценко Сергей Павлович
д. х. н., профессор
Кубанский государственный аграрный университет, Краснодар, Россия

Пшенецкий Сергей Петрович
к. т. н., доцент
Академия маркетинга и социально-информационных технологий - ИМСИТ, Краснодар, Россия

Изложено перспективное направление обеспечения безопасности бизнеса - создание экономически обоснованных систем менеджмента информационной безопасности. Показано их место в общей структуре менеджмента организации. Приведена обобщенная структура и методология построения системы менеджмента информационной безопасности

Ключевые слова:
БИЗНЕС, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, МЕЖДУНАРОДНЫЕ СТАНДАРТЫ, СИСТЕМА МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

UDC 004.056:378(06)

THE APPROACH TO CONSTRUCTION OF MODEL OF INFORMATION SECURITY MANAGEMENT SYSTEMS

Dotsenko Sergey Pavlovich
Dr. Sci. Chem., professor
Kuban State Agrarian University, Krasnodar, Russia

Pshenetskiy Sergei Petrovich
Cand. Tech. Sci., associate professor
Academy of marketing and social - information technologies - IMSIT, Krasnodar, Russia

The perspective direction of a safety of business - creation of the economically justified systems of management of information safety is stated. Their place in the general structure of management of the organization is shown. The generalized structure and methodology of construction of information security management system is resulted

Keywords:
BUSINESS, INFORMATION SAFETY, THE INTERNATIONAL STANDARDS, INFORMATION SECURITY MANAGEMENT SYSTEM

Информационная безопасность — одна из важнейших, но не очень зримых областей в деятельности почти любой компании. Информационная безопасность – это защита активов организации (например, информации) от неавторизованного раскрытия или неавторизованного или случайного изменения, а также гарантия того, что информация готова к использованию в тот момент, когда она нужна. Высший приоритет она имеет в организациях, в которых информационные и нематериальные активы превалируют над материальными.

Поскольку основной целью бизнеса является формирование положительных финансовых потоков, он обращает внимание на информационную безопасность (ИБ) только тогда, когда появляются реальные угрозы основной деятельности. При этом важно понимать, что

без постоянного учета факторов риска эффективное развитие бизнеса не только сводится к нулю, но может нанести организации непоправимый ущерб – утрату репутации, нарушение непрерывности процессов, финансовые убытки, а в худшем случае – невозможность дальнейшего ведения бизнеса.

Для современного менеджмента характерен проактивный подход, который в отличие от реактивного предполагает решение проблем не «по мере их поступления», когда бывает уже слишком поздно ими заниматься, а предусматривает заблаговременный анализ и упреждение возможных проблем, на основе оценки рисков, руководствуясь при этом соображениями экономической целесообразности.

Оценка рисков нужна руководителям компаний и государства для принятия взвешенных управленческих решений - без этого в современных условиях могут произойти очень большие неприятности на личном, корпоративном, государственном и мировом уровне, не говоря уже просто о неэффективном расходовании средств на защиту. Насколько глобальными могут быть последствия недооценки рисков, видно на примере захлестнувшего весь цивилизованный мир финансового кризиса, основной причиной которого является отсутствие адекватного управления финансовыми рисками, а порой и самого осознания этих рисков [1].

Применительно к ИБ проактивный подход заключается в построении систем менеджмента информационной безопасности (СМИБ), которые призваны минимизировать информационные риски и повысить эффективность защиты информации. Методологической основой такого подхода являются международные стандарты класса *«Good Practice»*, в первую очередь, серии *ISO 27000* [2].

Несмотря на то, что *ISO 27001:2005* носит необязательный характер, все больше компаний не только рассматривают его внедрение как высокоприоритетную задачу, но и тратят немалые средства на

сертификацию, хотя нигде, кроме Японии, никто их этого делать не заставляет. Ведь, кроме этого стандарта, в мире имеется еще более 500 стандартов и нормативных документов в области ИБ, десятки из которых носят для организаций обязательный характер. Пример тому - Microsoft, безусловно имеющая одну из наиболее сильных систем менеджмента в мире, приняла решение о формализации своих процессов управления ИБ в соответствии с *ISO 27001* вслед за Cisco, HP, IBM, Yahoo и другими гигантами IT - индустрии.

Причина такого успеха *ISO 27001* кроется, прежде всего, в полезных свойствах самого стандарта и универсальности принятого в нем процессного подхода к решению проблем ИБ, а именно:

- простота (небольшой по объему текст, нормально воспринимается даже неспециалистами);
- высокоуровневость, поскольку рассматриваются первичные организационные вопросы, без ответа на которые более низкоуровневые технологические вопросы утрачивают смысл;
- полнота - стандарт охватывает все аспекты обеспечения информационной безопасности, а не только IT;
- здравый смысл - все рекомендации стандарта легко находят обоснование при помощи здравого смысла, доступного практически любому человеку;
- экономическая обоснованность (стандарт рекомендует внедрять только те механизмы контроля, которые необходимы для уменьшения рисков до приемлемой величины и являются экономически обоснованными, при этом определяя основные подходы к оценке и обработки риска);
- универсальность, так как описанный в стандарте подход в равной степени актуален для любой организации.

Немаловажным фактором при этом, является и тот, что построенные на его основе *ISO 27001* СМИБ органически вписываются в общую систему менеджмента организации, имеющую единые базовые понятия, процессный подход и структуру (рис. 1).

Рисунок 1 - Место СМИБ в общей системе менеджмента организации

Структура СМИБ

Структура современной СМИБ представляет собой процессно - ориентированную систему управления, включающую организационный, документальный и программно-аппаратный компоненты. Можно выделить следующие разрезы СМИБ: процессный, документальный и зрелостный.

Процессы СМИБ созданы в соответствии с требованиями стандарта *ISO/IEC 27001:2005*, в основе которого лежит цикл управления Plan-Do-Check-Act. В соответствии с ним жизненный цикл СМИБ состоит из четырех типов деятельности: Создание - Внедрение и эксплуатация - Мониторинг и анализ - Сопровождение и совершенствование. Процессы СМИБ интегрируются в существующую структуру бизнес-процессов организации для выполнения всех требований стандарта (рис. 2).

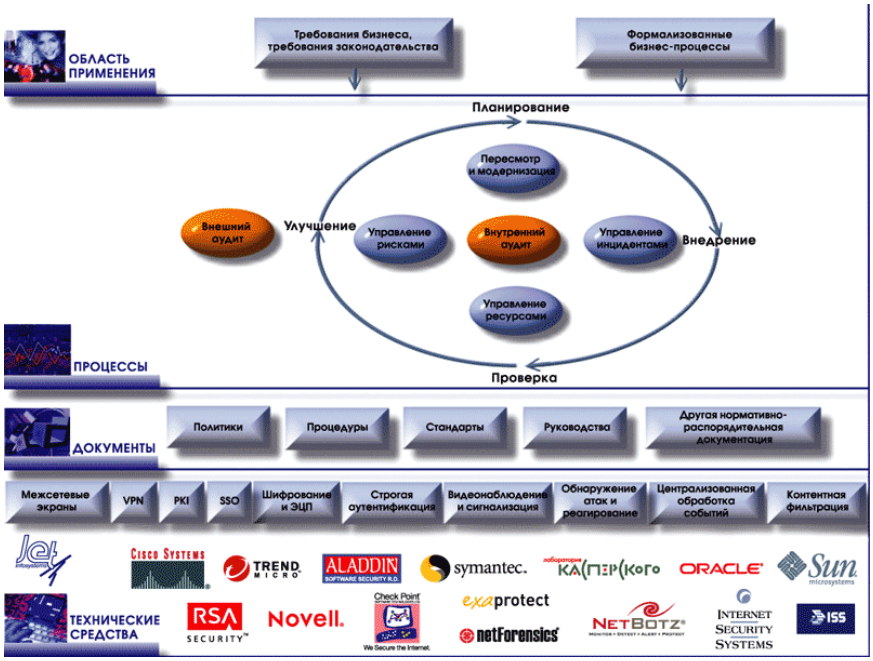

Рисунок 2 - Структура современной СМИБ

Для их автоматизации применяется специализированное программное обеспечение, использование которого позволяет существенно уменьшить трудоемкость эксплуатации СМИБ, повысить уровень зрелости процессов менеджмента и упростить процедуры внутреннего и внешнего сертификационного аудита.

Документация СМИБ состоит из политик, документированных процедур, стандартов и записей и делится на две части: документация менеджмента СМИБ и эксплуатационная документация СМИБ.

Документация менеджмента ИБ представлена Политиками ИБ и СМИБ, основной процедурой – "Менеджмент ИБ" и сопутствующими формами записей, процедурами "Внутренний аудит", "Управление документацией" и "Управление Записями".

Зрелостная модель СМИБ определяет состав и детализацию разрабатываемой документации, последовательность построения СМИБ, детальность разрабатываемой документации и степень автоматизации процессов менеджмента и эксплуатации СМИБ. При оценке и планировании используется модель зрелости CobiT [3]. В Программе

повышения зрелости СМИБ приводятся состав и сроки мероприятий по совершенствованию процессов менеджмента ИБ и управления эксплуатацией средств ИБ.

Построение СМИБ

Корректное построение СМИБ в организации — основа для дальнейшей деятельности организации. Специалисты организации могут разработать и внедрить СМИБ самостоятельно, выполняя требования стандарта и учитывая мировую практику, либо прибегнуть к помощи компетентных организаций, имеющих опыт в данной области. В любом случае построение СМИБ организации подразумевает прохождение следующих основных этапов.

- Предварительный аудит.
- Определение области действия и границ СМИБ.
- Назначение сотрудников, ответственных за СМИБ (создание структуры, которая будет внедрять и обеспечивать работоспособность СМИБ организации, к примеру, отдел внутренней безопасности).
- Инвентаризация активов организации и определение их важности.
- Оценка защищённости активов организации (анализ существующих угроз и уязвимостей, а также вероятностей их реализации).
- Определение подхода организации к оценке рисков (стандарт не устанавливает обязательного метода к определенному методу оценки рисков – наоборот, организация может предложить свой метод оценки рисков, и чем проще будет этот метод, тем лучше).
- Подсчёт рисков в организации как в качественных, так и в количественных показателях.

- Анализ рисков и принятие решений по обработке рисков (принять риск, уменьшить риск до допустимого уровня, передать третьей стороне, избежать риска).
- Выбор целей управления и средств для обработки рисков.
- Анализ существующих контрмер (организационные мероприятия и программно-технические средства, направленные на защиту определённого актива организации).
- Анализ процессной документации организации (создаётся список организационных документов, требующих внедрения).

Создание политики информационной безопасности (пересматриваемый документ, который должен быть одобрен руководством и представлен для изучения всем сотрудникам организации; описывает функциональные обязанности руководства и подход к управлению информационной безопасностью).

Создание Заявления о применимости (обязательный документ, который содержит все рекомендации Приложения А стандарта ISO/IEC 27001:2005 с описанием, выполняется ли данное требование в организации).

- Разработка документации СМИБ (инструкции, процедуры, методики, записи, корпоративные стандарты и т. д.).
- Внедрение СМИБ (внедрение необходимых технических средств, подготовка к аудиту и т. д.).
- Обучение персонала (проводится при принятии на работу, при внедрении СМИБ и при внесении изменений в СМИБ).
- Проведение внутреннего аудита СМИБ организации.

Если в организации уже существует своя система информационной безопасности, и строить с нуля СМИБ представляется нецелесообразным, то оптимальным решением является проведение внутреннего аудита. На

основе результатов такого анализа можно откорректировать действующую систему, разработать недостающие процессные документы, улучшить подход к оценке рисков в организации и т. д.

Сертификация СМИБ

В настоящее время создана система сертификации СМИБ организации по требованиям *ISO/IEC 27001:2005*. Сертификация проводится органами сертификации, имеющими аккредитацию UKAS (United Kingdom Accreditation Service). Органы сертификации осуществляют выдачу сертификатов соответствия установленного образца организациям, успешно прошедшим процедуру сертификации, и регистрацию этих организаций в специальном реестре. Успешное прохождение сертификации подтверждает, что СМИБ организации построена в четком соответствии с практическими правилами, описанными в международном стандарте *ISO/IEC 27002:2007*.

Проверка СМИБ аудиторами сертифицирующего органа включает стадию проверки наличия документации — политик, процедур, методик и других документов, описывающих действия в рамках СМИБ. Проверяется наличие базы рисков информационной безопасности, методики оценки рисков, прогнозирования и управления рисками для уменьшения вероятности их возникновения и реализации. Проводится опрос персонала организации и проверка выполнения требований процессных документов СМИБ. После окончания аудита выполняются корректирующие действия по недостаткам, обнаруженным во время проверки.

Согласно сведениям международного реестра сертификатов СМИБ [4], на сентябрь 2009 года в реестре имеются данные по 5822 действующим сертификатам на СМИБ организаций из более чем 70 стран мира, в числе которых (по нисходящей):

Япония – 3273 сертифицированная СМИБ;

Индия – 477 сертифицированные СМИБ;

Великобритания – 401 сертифицированных СМИБ;

Китай – 205 сертифицированные СМИБ;

США – 95 сертифицированных СМИБ.

И только 10 российских компаний прошли сертификацию по требованиям стандартов на СМИБ (*ISO/IEC 27001:2005*) на тот же период.

Выводы

1. Без управления рисками все еще, как и раньше, можно достигать определенных положительных результатов, однако стабильных результатов достигнуть уже сложнее. Поэтому компании, систематически управляющие рисками, по крайней мере, обладают важнейшим конкурентным преимуществом. Для бизнеса, в целом, можно выделить следующие преимущества, от внедрения СМИБ:

- повышение управляемости и надежности;
- повышение защищенности ключевых бизнес-процессов;
- повышение доверия к организации со стороны контрагентов;
- подтверждение прозрачности;
- упрощение процедуры выхода на внешние рынки (при наличии сертификата);
- повышение авторитета организации, как на внутреннем, так и на внешних рынках;
- повышение доходности и капитализации.

2. Только те компании, в которых существует сбалансированная СМИБ, построенная по Демингу, где управление ИБ на основе риск-ориентированного подхода это рутинная работа менеджмента, где решения по ИБ принимаются на основе оценки рисков, таким образом, чтобы максимизировать возврат инвестиций, где фундаментом СМИБ служат, формализованные процессы, документооборот, грамотно выстроенная

организационная структура, могут рассчитывать на успех в борьбе за внешние рынки.

3. Специалистам в области ИБ понадобится переориентироваться на бизнес и научиться осуществлять декомпозицию бизнес целей и процессов до поддерживающих их информационных активов и связанных с ними угроз и уязвимостей, а уже от них переходить к механизмам безопасности, которыми они привыкли заниматься. Здесь, скорее, потребуются не новые знания, а перенастройка мышления с технически ориентированного на бизнес - ориентированное и риск - ориентированное.

Литература

1. *Тысячникова, Н.А.* Организация внутреннего контроля за операционными рисками/ Н.А. Тысячникова. – (http://www.bankir.ru/technology/article/2194936).

2. Международные стандарты ISO/IEC: 27001:2005, 27002:2005, 27005:2008.

3. Control Objectives for Information and Related Technology (COBIT), доступен на сайте: www.isaca.org.

4. Международный реестр сертификатов СМИБ: (http://www.ISO27001certificates.com)