УДК 004.056

Шамсутдинов Р. Р.
студент 2-го года обучения магистратуры
Уфимский государственный авиационный технический университет
Российская Федерация, г. Уфа

СТРАТЕГИЧЕСКОЕ УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ НА ОСНОВЕ КОНЦЕПЦИИ КЛАССИЧЕСКОЙ СИСТЕМЫ СТРАТЕГИЧЕСКОГО МЕНЕДЖМЕНТА НА ПРЕДПРИЯТИИ

Аннотация: *в статье проанализированы основные положения стандартов по управлению информационной безопасностью, цикл «планирование – осуществление – проверка – действие» применительно к менеджменту информационной безопасности, концепция стратегического управления предприятием, на основе которых разработана система стратегического управления информационной безопасностью.*

Ключевые слова: *информационная безопасность, стратегический менеджмент, системы менеджмента информационной безопасности.*

Abstract: *the article analyzes the main provisions of the information security management standards, the "plan – do – check – act" cycle for information security, and the enterprise strategic management concept, on the basis of which the information security strategic management system was developed.*

Keywords: *information security, strategic management, information security management systems.*

В настоящее время все актуальнее становится необходимость обеспечения *информационной безопасности* (*ИБ*), что защищает целостность информации, ее доступность и аутентичность, защищает организацию от разглашения информации, деструктивных информационных воздействий.

Информационная безопасность организации должна быть построена в соответствии с действующими правовыми нормами на основе соответствующих организационных документов. Разработка последних осуществляется следующим образом. В первую очередь составляется реестр защищаемых *информационных активов* (*ИА*), затем осуществляется категорирование *ИА* по степени критичности, определяются права доступа субъектов к *ИА*, разрабатывается Политика ИБ, локальные Политики ИБ, такие, как Политика парольной защиты, Политика антивирусной защиты и т.д.

Стандартом ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» рекомендуется управлять *системой менеджмента информационной безопасности* (*СМИБ*) в цикле *Plan-Do-Check-Act* (*PDCA*), представленном на рисунке 1.

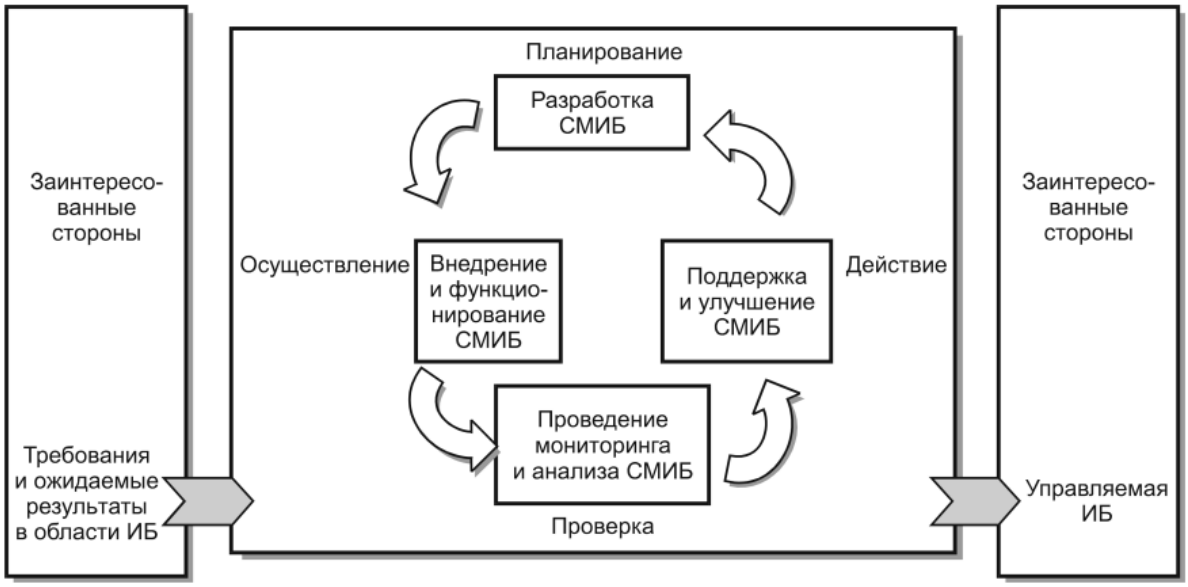

Рисунок 1 – PDCA применительно к СМИБ [1]

Необходимо понимать, что СМИБ – система организационная, и лица, принимающие решения в рамках СМИБ, должны быть не только высоко компетентны по техническим вопросам, средствам и системам защиты, но, что очень важно, владеть знаниями, умениями и навыками в области классического менеджмента. К примеру, руководство ИБ, как и любое

другое, должно выполнять функции менеджмента, среди которых: планирование, организация, мотивация, контроль и координация, что на практике не входит в состав требований к компетенциям инженеров, лучшие из которых нередко становятся руководителями.

Необходимо обратить внимание, что СМИБ, соответствующая стандартам и лучшим практикам обеспечения ИБ – гибкая, оперативно реагирующая на изменение внешней обстановки система. Однако нельзя не учитывать положительного эффекта от добавления в СМИБ элементов стратегического управления.

Рассмотрим понятие стратегического управления применительно к управлению информационной безопасностью. «Стратегическое управление – это комплексная система постановки и реализации стратегических целей предприятия, основанная на прогнозировании среды и выработке способов адаптации к ее изменениям, а также воздействия на нее» [2].

Стратегическое управление отличается от оперативного и тактического не только сроком планирования в несколько лет, не только тем, что оперативные решения должны являться элементами принятой стратегии, но и необходимостью на ранних этапах планирования выдвигать и рассматривать максимально возможное количество альтернатив, что снижает риск ошибки планирования. Это требует бóльших усилий и времени для их оценки [3].

В рамках же оперативного управления менеджерам приходится решать задачи либо жестко структурированные, алгоритм грамотного решения которых хорошо известен, либо с «гибкими» вариациями решений, но с невысоким риском серьезного ущерба при ошибке. Отсутствие же стратегической цели, в том числе в управлении ИБ, можно охарактеризовать фразой «не знающий куда идти не известно куда и придет».

Стратегический менеджмент реализуется системой стратегического управления (ССУ), с ее центральной частью при руководстве, периферийными группами в основных структурных единицах. Назначение

ССУ состоит в своевременном формулировании цели развития, постановке проблем и задач, поиске способов и организации достижения целей. ССУ предусматривает выделение ресурсов корпорации под стратегические цели независимо от фактической структуры управления производственно-хозяйственной деятельностью; создание центров руководства каждой стратегической целью; оценку и стимулирование производственных подразделений и их руководителей по степени достижения стратегических целей. Материальный продукт стратегического управления – система планов организации, включающая представленный документально стратегический план.

Адаптируем классическую ССУ к стратегическому управлению информационной безопасностью, отметим, что она должна быть реализована как подсистема СМИБ. Задачи системы стратегического управления информационной безопасностью (ССУИБ):

– разработка стратегических целей ИБ;

– оценка возможностей и ресурсов компании;

– анализ тенденций в области ИБ;

– оценка альтернативных путей выполнения задач обеспечения безопасности, включая анализ возможных смен и дополнений видов деятельности организации;

– распределение имеющихся ресурсов в стратегически обоснованные и высокоэффективные проекты ИБ;

– подготовка детальных оперативных планов, программ и бюджетов;

– оценка деятельности по обеспечению ИБ на основе определенных критериев с учетом намеченных целей и планов;

– формирование внутренней среды, благоприятствующей инициативному реагированию руководства ИБ на изменение ситуации;

– оценка влияния внешней среды, определение новых возможностей развития угроз ИБ;

– обеспечение целевой направленности всей деятельности системы менеджмента информационной безопасности;

– выработка стратегии обеспечения ИБ;

Разработка стратегии включает следующие обязательные шаги:

– четкое формулирование *видения* образа системы обеспечения ИБ в перспективе и главного направления ее развития (главную стратегическую цель ИБ);

– установка цели и контрольных параметров обеспечения ИБ;

– определение типа предприятия и способов управления ИБ, выявление основных проблем управления ИБ

– анализ сильных и слабых сторон ИБ, выявление возможных угроз, ключевых факторов успеха

– разработка требований и критериев оценки основных видов деятельности по ИБ

– установка цели, а также общих требований к использованию объектов.

Общая стратегическая цель системы ИБ или видение – желаемый идеальный образ будущего состояния ИБ, отражающий наиболее благоприятную ситуацию в наиболее благоприятных условиях внешней среды, оно не зависит от текущей обстановки, существующих в данный момент тенденций развития фирмы и сферы ИБ.

Видение – концепция долгосрочной цели, являющаяся основой для деятельности фирмы. Оно фиксирует общую стратегическую цель компании и главное направление развития, приводящее к ее достижению, а также определяет границы деятельности, что дает возможность свести разработку стратегии к оптимизационной задаче. Видение становится эффективным инструментом ССУИБ при:

– существовании точной системы целеполагания

– доведении желаемого образа будущей системы обеспечения ИБ в письменном виде до каждого сотрудника, участвующего в управлении ИБ;

– соответствующем поощрении инициативы работников;

– существовании четкого распределения полномочий и ответственности

Утвердившись в своем видении, руководство ИБ должно стараться не подстраиваться под внешнюю обстановку, а стремиться формировать внешнюю и внутреннюю среды под созданный образ состояния ИБ, выстраивая их в соответствии с выработанным взглядом.

В целом, стратегическое поле менеджмента ИБ крупных предприятий может дробиться на стратегические единицы менеджмента ИБ – внутрифирменные организационные единицы, отвечающие за выработку стратегии фирмы в одном или нескольким направлениях обеспечения ИБ. Идентификация стратегических единиц – во многом предмет субъективного выбора.

Таким образом, стратегическое управление информационной безопасностью на основе концепции классической системы стратегического менеджмента на предприятии снижает ошибки планирования, позволяет на основе анализа множества альтернатив строить наиболее рациональную стратегию развития системы обеспечения ИБ, направленную на достижение выработанного видения, при стремлении формировать внутреннюю и внешню среды под созданный идеальный образ системы обеспечения ИБ.

Библиографический список:

1. ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».

2. Стратегическое управление крупным промышленным предприятием // Корпоративный менеджмент [Электронный ресурс]. URL:

http://www.cfin.ru/management/strategy/plan/big_manufacture.shtml (Дата обращения: 02.02.2018).

3. Чем отличается стратегический менеджмент от оперативного управления // Radio-angusht [Электронный ресурс]. URL: http://radio-angusht.ru/ chem-otlichaetsya-strategicheskij-menedzhment-ot-operativnogo-upravleniya (Дата обращения: 30.01.2018).