УДК 621.396

С.Б. Гордиенко, В.В. Алейников, А.В. Литвинов, О.В. Рзаев

АКТУАЛЬНЫЕ ВОПРОСЫ ПОСТРОЕНИЯ И СЕРТИФИКАЦИИ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ КОМПАНИИ

В статье рассмотрены актуальные вопросы построения и сертификации системы управления информационной безопасностью, преимущества внедрения и влияние на общую коммерческую привлекательность организации сертифицированной СУИБ, а также её связь с другими системами управления и процессами организации. Проанализированы механизмы планирования и контроля на этапах подготовки организации к сертификации по ISO 27001. Для подтверждения соответствия существующей в организации СУИБ требованиям стандарта, а также ее адекватности бизнес-рискам определена процедура эффективного функционирования и непрерывного совершенствования в соответствии с моделью ПРПД к процессам СУИБ.

Ключевые слова: оценка информационных рисков, системный подход, информационная безопасность, система управления информационной безопасностью.

Введение

Для многих компаний настало время задуматься об управлении безопасностью. ИТ-инфраструктура многих из них достигла уровня, требующего четко отлаженной координации.

Управление информационной безопасностью — это циклический процесс, включающий:

- осознание степени необходимости защиты информации и постановку задач;
- сбор и анализ данных о состоянии информационной безопасности в организации; оценку информационных рисков; планирование мер по обработке рисков;
- реализацию и внедрение соответствующих механизмов контроля, распределение ролей и ответственности, обучение и мотивацию персонала, оперативную работу по осуществлению защитных мероприятий;
- мониторинг функционирования механизмов контроля, оценку их эффективности и соответствующие корректирующие воздействия.

Руководитель обязан контролировать ситуацию в своей организации, подразделении, проекте и во взаимоотношениях с заказчиками. Это означает быть осведомленным о том, что происходит, своевременно узнавать обо всех нештатных ситуациях и представлять себе, какие действия надо будет предпринять, в том или ином случае. В организации существует несколько уровней управления, начиная с менеджеров высшего звена и заканчивая конкретным исполнителями, и на каждом уровне ситуация должна оставаться под контролем. Другими словами, должна быть выстроена вертикаль управления и процессы управления.

Построение системы управления информационной безопасностью (СУИБ).

При построении системы управления безопасностью эксперты рекомендуют опираться на международные стандарты ISO/IEC 27001/17799.

Согласно ISO 27001, система управления информационной безопасностью (СУИБ) — это «та часть общей системы управления организации, основанной на оценке бизнес рисков, которая создает, реализует, эксплуатирует, осуществляет мониторинг, пересмотр, сопровождение и совершенствование информационной безопасности». Система управления включает в себя организационную структуру, политики, планирование, должностные обязанности, практики, процедуры, процессы и ресурсы.

Создание и эксплуатация СУИБ требует применения такого же подхода, как и любая другая система управления. Используемая в ISO 27001 для описания СУИБ процессная модель предусматривает непрерывный цикл мероприятий: планирование, реализация, проверка, действие (ПРПД).

Применение модели ПРПД к процессам СУИБ

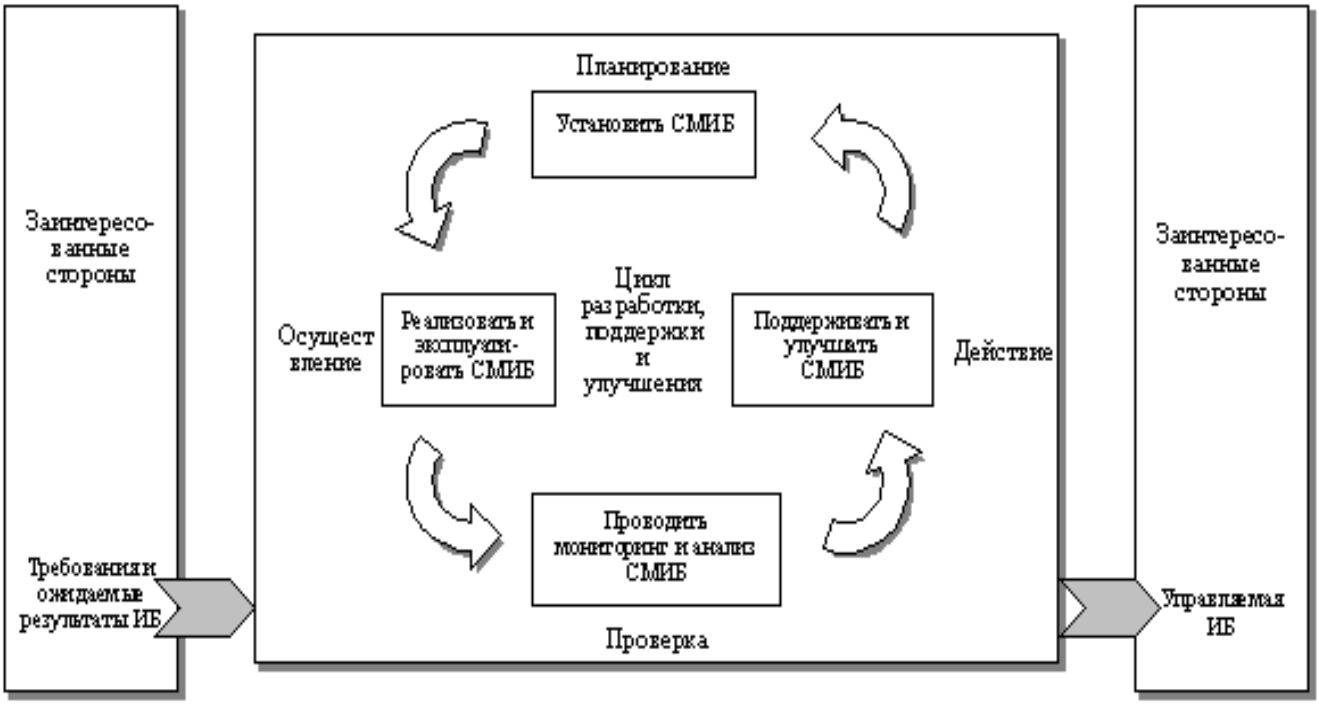

Рис.1. Применение модели ПРПД к процессам СУИБ

Процесс непрерывного совершенствования обычно требует первоначального инвестирования: документирование деятельности, формализация подхода к управлению рисками, определение методов анализа и выделение ресурсов. Эти меры используются для приведения цикла в действие. Они не обязательно должны быть завершены, прежде чем будут активизированы стадии пересмотра [2].

На стадии планирования обеспечивается правильное задание контекста и масштаба СУИБ, оцениваются риски информационной безопасности, предлагается соответствующий план обработки этих рисков.

В свою очередь, на стадии реализации внедряются принятые решения, которые были определены на стадии планирования.

На стадиях проверки и действия усиливают, исправляют и совершенствуют решения по безопасности, которые уже были определены и реализованы.

Проверки могут проводиться в любое время и с любой периодичностью в зависимости от конкретной ситуации. В некоторых системах они должны быть встроены в автоматизированные процессы с целью обеспечения немедленного выполнения и реагирования. Для других процессов реагирование требуется только в случае инцидентов безопасности, когда в защищаемые информационные ресурсы были внесены изменения или дополнения, а также когда произошли изменения угроз и уязвимостей. Необходимы ежегодные или другой периодичности проверки или аудиты, чтобы гарантировать, что система управления в целом достигает своих целей.

Руководство организации выпускает политику безопасности, в которой вводится понятие СУИБ и провозглашаются ее основные цели: управление непрерывностью бизнеса и управление безопасностью. На вершине СУИБ находится директор по ИБ, возглавляющий управляющий комитет по ИБ — коллегиальный орган, предназначенных для решения стратегических вопросов, связанных с обеспечением ИБ.

Директор по ИБ несет ответственность за все процессы управления ИБ, в число которых входят: управление инцидентами и мониторинг безопасности, управление

изменениями и контроль защищенности, инфраструктура безопасности (политики, стандарты, инструкции, процедуры, планы и программы), управление рисками, контроль соответствия требованиям, обучение (программа повышения осведомленности).

Создание подобной структуры управления является целью внедрения ISO 27001/17799 в организации.

Один из основных принципов здесь - «приверженность руководства». Это означает, что такая структура может быть создана только руководством компании, которое распределяет должности, ответственность и контролирует выполнение обязанностей [2]. Другими словами руководство организации строит соответствующую вертикаль власти, а точнее модифицирует существующую модель для удовлетворения потребностей организации в безопасности. СУИБ может создаваться только сверху вниз.

Другим основополагающим принципом является вовлечение в процесс обеспечения ИБ всех сотрудников организации, имеющих дело с информационными ресурсами — «от директора до уборщицы». Неосведомленность конкретных людей, работающих с информацией, отсутствие программы обучения по ИБ — одна из основных причин неработоспособности конкретных систем управления.

Не менее важно и то, что в основе любого планирования мероприятий по ИБ должна лежать оценка рисков. Отсутствие в организации процессов управления рисками приводит к неадекватности принимаемых решений и неоправданным расходам [3]. Другими словами, оценка рисков является тем фундаментом, на котором держится стройное дерево СУИБ.

Столь же фундаментальным принципом является «внедрение и поддержка СУИБ собственными руками». Привлечение внешних консультантов на всех этапах внедрения, эксплуатации и совершенствования СУИБ во многих случаях вполне оправдано. Более того, это является одним из механизмов контроля, описанных в ISO 17799. Однако создание СУИБ руками внешних консультантов невозможно по определению, т.к. СУИБ — это совокупность организационных структур формируемых руководством организации и процессов, реализуемых ее сотрудниками, которые должным образом осведомлены о своих обязанностях и обучены навыкам обращения с информацией и ее защиты. СУИБ стоит немалых денег, но ни за какие деньги нельзя купить опыт и знания.

Сертификация системы управления информационной безопасностью

Для подтверждения соответствия существующей в организации СУИБ требованиям стандарта, а также ее адекватности существующим бизнес рискам используется процедура добровольной сертификации. Хотя без этого можно и обойтись, в большинстве случаев сертификация полностью оправдывает вложенные средства и время.

Во-первых, официальная регистрация СУИБ организации в реестре авторитетных органов, таких как служба аккредитации Великобритании (UKAS), что укрепляет имидж компании, повышает интерес со стороны потенциальных клиентов, инвесторов, кредиторов и спонсоров.

Во-вторых, в результате успешной сертификации расширяется сфера деятельности компании за счет получения возможности участия в тендерах и развития бизнеса на международном уровне. В наиболее чувствительных к уровню информационной безопасности областях, такой, например, как финансы, наличие сертификата соответствия ISO 27001 начинает выступать как обязательное требование для осуществления деятельности. Некоторые отечественные компании уже сталкиваются с этими ограничениями.

Также очень важно, что процедура сертификации оказывает серьезное мотивирующее и мобилизующее воздействие на персонал компании: повышается уровень осведомленности сотрудников, эффективнее выявляются и устраняются недостатки и несоответствия в системе управления информационной безопасностью, что в перспективе означает сокращение накладных расходов на эксплуатацию информационных систем. Вполне

возможно, наличие сертификата позволит застраховать информационные риски организации на более выгодных условиях [4].

Как свидетельствует текущая практика, расходы на сертификацию по BS7799 в большинстве случаев несопоставимо малы в сравнении с затратами организации на обеспечение информационной безопасности, а получаемые преимущества многократно их компенсируют.

Следует подчеркнуть, что все перечисленные преимущества организация получает только в том случае, если речь идет о системе сертификации, имеющей международное признание, в рамках которой обеспечивается надлежащее качество проведения работ и достоверность результатов.

Подготовка к сертификации

Подготовка организации к сертификации по ISO 27001 — процесс довольно длительный и трудоемкий. В общем случае, он включает в себя шесть последовательных этапов, которые выполняются организацией, как правило, при помощи внешних консультантов.

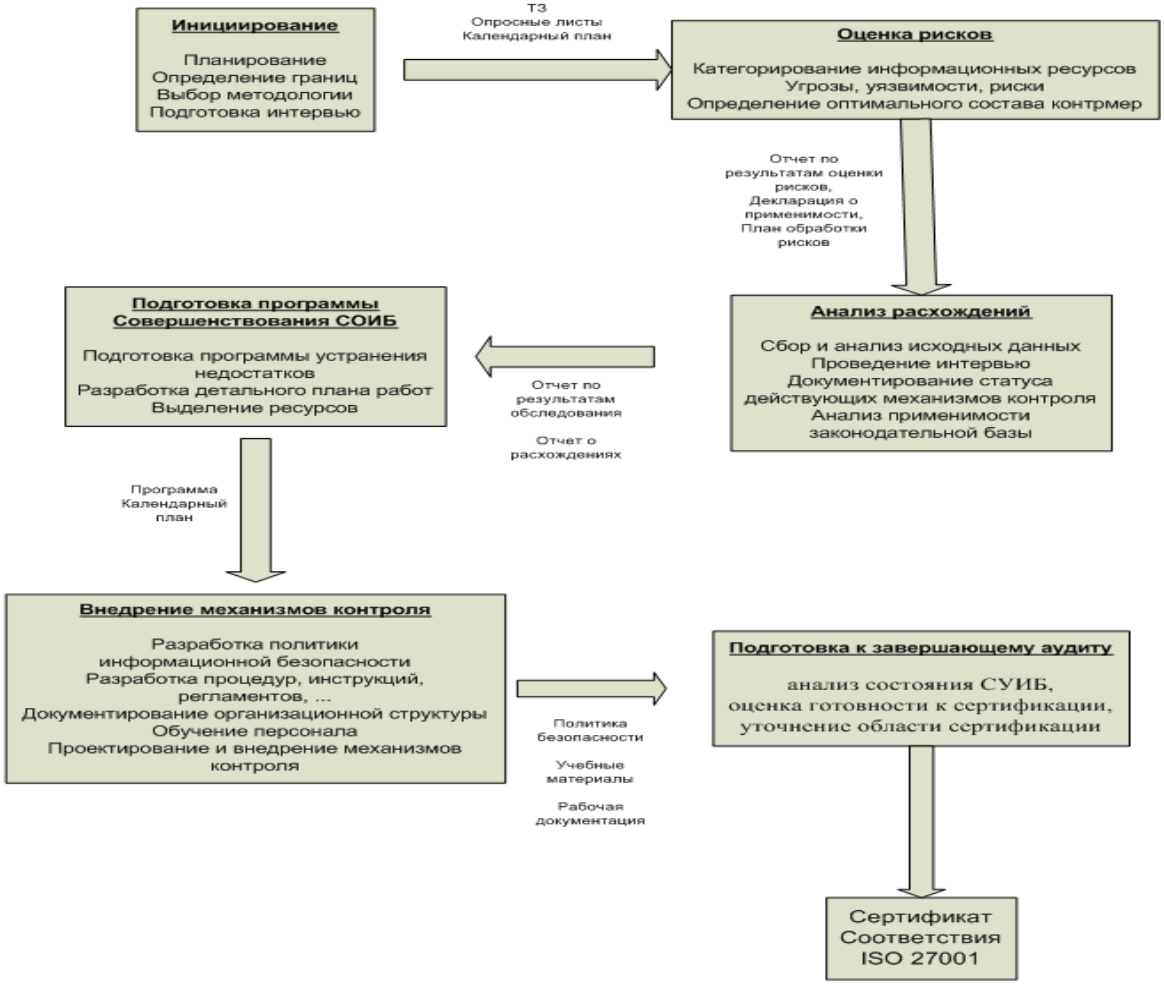

Рис.2 . Этапы подготовки организации к сертификации по ISO 27001

На первом этапе проводится предварительный аудит СУИБ, в ходе которого оценивается текущее состояние, осуществляется инвентаризация и документирование всех основных составляющих СУИБ, определяются область и границы сертификации и выполняется еще целый ряд необходимых подготовительных действий. По результатам аудита разрабатывается детальный план мероприятий по подготовке к сертификации.

На втором этапе выполняется оценка информационных рисков, основной целью которой является определение применимости описанных в стандарте механизмов контроля в данной конкретной организации, подготовка декларации о применимости и плана обработки рисков.

На третьем этапе выполняется анализ расхождений с требованиями стандарта, в результате которого оценивается текущее состояние механизмов контроля в организации и идентифицируются расхождения с декларацией о применимости.

На последующих этапах осуществляется планирование и внедрение недостающих механизмов контроля, по каждому из которых разрабатывается стратегия и план внедрения.

Работы по внедрению механизмов контроля включают в себя три основные составляющие: подготовка сотрудников организации: обучение, тренинги, повышение осведомленности; подготовка документации СУИБ: политики, стандарты, процедуры, регламенты, инструкции, планы; подготовка свидетельств функционирования СУИБ: отчеты, протоколы, приказы, записи, журналы событий и т.п.

На заключительном этапе осуществляется подготовка к сертификационному аудиту: анализируется состояние СУИБ, оценивается степень ее готовности к сертификации, уточняется область и границы сертификации, проводятся соответствующие переговоры с аудиторами органа по сертификации.

В процессе внедрения СУИБ возникает много точек преткновения. Часть из них связаны с нарушением описанных выше фундаментальных принципов управления безопасностью. Серьезные затруднения для отечественных организаций лежат в законодательной области. Неполнота и противоречивость действующего законодательства, его запретительный характер в области использования криптографии и во многих других областях, а также неотрегулированность системы сертификации средств защиты информации серьезно затрудняет выполнение одного из главных требований стандарта — соответствие действующему законодательству.

Источником затруднений нередко служит неправильное определение области действия и границ СУИБ. Слишком широкая трактовка области действия СУИБ, например, включение в эту область всех бизнес-процессов организации, значительно снижает вероятность успешного завершения проекта по внедрению и сертификации СУИБ.

Столь же важно правильно представлять, где проходят границы СУИБ и каким образом она связана с другими системами управления и процессами организации. Например, система управления ИБ и система управления непрерывностью бизнеса (BCM) организации тесно пересекаются. Последняя является одной из 11 определяемых стандартом областей контроля информационной безопасности. Однако СУИБ включает в себя только ту часть BCM, которая связана с ИБ — это защита критичных бизнес процессов организации от крупных сбоев и аварий информационных систем. Другие аспекты BCM выходят за рамки СУИБ.

Преимущества сертификации СУИБ

Сертификация независимым авторитетным органом по сертификации продемонстрирует рынку, партнёрам, клиентам, конкурентам, инвесторам и самой компании, что в неё налажено эффективное управление информационной безопасностью. В свою очередь это обеспечивает компании конкурентное преимущество, демонстрируя способность управлять информационными рисками. Это означает, что в компании:

- Выявляются основные угрозы безопасности для бизнес-процессов;
- Вырабатываются рекомендации по повышению текущего уровня защищенности для защиты от обнаруженных угроз и недостатков в системе безопасности и управления;
- Снижаются риски прямых потерь, связанных с нарушением конфиденциальности, неконтролируемыми изменениями данных, простоями информационной системы;
- Информация и компания более защищены;
- Обеспечивается эффективное управление системой в критичных ситуациях.

Кроме того:

- Информационная система компании становится «прозрачнее» для менеджмента;
- Внедрение СУИБ оказывает благотворное влияние на общую организацию работы и профессиональный уровень сотрудников;
- Сертифицированная СУИБ является положительным фактором при слиянии компаний, а также при получении кредитов и правительственных заказов;
- Более безопасное взаимодействие с партнерскими организациями ми клиентами;
- Более высокий уровень доверия со стороны партнёров и клиентов, поскольку они видят, что благодаря соблюдению требований к информационной безопасности, компания демонстрирует стремление уменьшить их риски;
- Признание Вашей компании на международном уровне.

И главное – в критических ситуациях обеспечивается бесперебойность работы организации.

Выводы

Сегодня организация работы серьезной и эффективной компании, претендующей на успешное развитие, обязательно базируется на современных информационных технологиях. Поэтому обратить внимание на стандарты управления информационной безопасностью стоит компаниям любого масштаба. Как правило, вопросы управления информационной безопасностью тем актуальнее, чем крупнее компания, чем шире масштаб ее деятельности и претензии на развитие, и, как следствие, выше ее зависимость от информационных технологий.

Использование международных стандартов управления информационной безопасностью ISO 27001/17799 позволяет существенно упростить создание, эксплуатацию и развитие СУИБ. Требования нормативной базы и рыночные условия вынуждают организации применять международные стандарты при разработке планов и политик обеспечения ИБ и демонстрировать свою приверженность путем проведения аудитов и сертификаций ИБ. Соответствие требованиям стандарта представляет определенные гарантии наличия в организации базового уровня информационной безопасности, что оказывает положительное влияние на имидж компании.

ЛИТЕРАТУРА

1.Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Гостехкомиссия России. - М.: Военное издательство, 1992.

2.Астахов А. Аттестация автоматизированных систем // Jet Info, 2000 - № 11. - 20 с.

3.Марков А.С., Миронов С.В., Цирлов В.Л. Разработка политики безопасности организации в свете новейшей нормативной базы // Защита информации. Конфидент, 2004. - №2. – С. 20-28.

4.Марков А.С., Цибин В.В. К вопросу о сертификации программных ресурсов автоматизированных систем по требованиям безопасности информации // АДЭ, 2004.

5.Марков А.С., Щербина С.А. Испытания и контроль программных ресурсов // InformationSecurity, 2003. – № 6 – С. 25.

6.Разработка систем информационно-компьютерной безопасности / Зима В.М., Котухов М.М., Ломако А.Г., Марков А.С., Молдовян А.А. – СПб: ВКА им. А.Ф.Можайского, 2003. – 327 с.

7.Цибин В.В. Теория и практика аттестации объектов информатизации по требованиям безопасности информации – ЗАО «НПП «БИТ», 2000.

Надійшла: 03.02.2014р Рецензент: д.т.н., проф. Богданович В.Ю.