Кокутин С.А. Совершенствование СМИБ – гарантия качества информационной безопасности предприятия [Электронный ресурс] // Информационно-экономические аспекты стандартизации и технического регулирования: Научный интернет-журнал. 2012. – № 6(10). Режим доступа http://iea.gostinfo.ru/files/2012_06/2012_06_17.pdf

УДК 338.49

СОВЕРШЕНСТВОВАНИЕ СМИБ – ГАРАНТИЯ КАЧЕСТВА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Кокутин С.А. ФГУП «Российский научно-технический центр информации по стандартизации, метрологии и оценке соответствия» (ФГУП «СТАНДАРТИНФОРМ»)

В статье рассматривается модель менеджмента информационной безопасности на основе Международного стандарта ISO/IEC 27001:2005. Показана необходимость введения, реализации, эксплуатации, мониторинга, пересмотра, поддержки и совершенствования системы менеджмента информационной безопасности в современных условиях.

Ключевые слова: *информационная безопасность, система менеджмента информационной безопасности, международный стандарт.*

UDC 338.49

IMPROVEMENT OF INFORMATION SECURITY MANAGEMENT SYSTEM – ENTERPRISE INFORMATION SECURITY QUALITY ENSURANCE

Kokutin S.A. FGUP «Russian Research and Development Information Center on Standartization, Metrology and Compliance Check» (FGUP «STANDARTINFORM»)

The article covers the model of information security management based on the International Standard ISO/IEC 27001:2005. Displays *the* necessity *for the* introduction*, implementation, operation, monitoring, revision, maintenance and improvement of the management informational security in* the *presence.*

Keywords: *information security, information security management system, international standard.*

В настоящее время важным рейтинговым показателем надежности и устойчивости предприятия является состояние его информационной безопасности (ИБ). Во всем мире на протяжении длительного времени разрабатываются и успешно внедряются всевозможные средства защиты информации, однако число утечек конфиденциальных данных, преступлений

в сфере компьютерной информации продолжает оставаться на высоком уровне. Причин подобной ситуации достаточно много, прежде всего, это растущие в геометрической прогрессии потребности бизнеса, заключающиеся во всестороннем обновлении информационных технологий и их внедрении в бизнес-процессы, стремительная изменчивость корпоративных сетей, пренебрежительное отношение к правилам информационной безопасности собственных сотрудников предприятий и организаций и др.

Согласно статистическим данным порядка 15 тыс. преступлений в сфере компьютерной информации ежегодно регистрируется на территории Российской Федерации. Анализ данных показывает, что в России, начиная с 2000-х гг., наблюдалось ежегодное удвоение числа зарегистрированных преступлений. Так, например: 2001 г. – 3 тыс., 2002 г. – 6 тыс., 2003 г. – 12 тыс., а с 2004 г. Министерство внутренних дел ежегодно регистрирует порядка 15 тыс., таких преступлений.[1]

Информация, представленная CSI (Computer Security Institute), в ежегодном выпуске о преступлениях и инцидентах в области компьютерной информации и др., также свидетельствует об их росте.[2]

Заслуживают внимания результаты исследования, проведенного Колумбийским университетом, в рамках которого осуществлялось глобальное сканирование IP-адресов. Исследование позволило выявить, что около 21 тыс. роутеров, web-камер и VoIP-устройств полностью открыты для удаленных атак. О последствиях несанкционированного доступа к административному интерфейсу сетевого устройства стоит только догадываться. Роутер может быть использован для сетевых атак на другие электронные вычислительные машины, а VoIP-устройство

[1] См.: Количество регистрируемых киберпреступлений растет // Информационно-методический журнал «Защита информации. Инсайд». 2009. №6.
[2] См.: 2010/2011 Computer Crime and SeCurity Survey // www.gocsi.com/survey.

перепрограммировано таким образом, что будет осуществлять запись всех разговоров и отправлять их злоумышленнику.

Проблематика информационной безопасности охватывает широкую сферу, куда входят программные и технические аспекты работы компании, а также организационные особенности функционирования бизнеса. К тому же помимо бизнес-задач, в сферу внимания информационной безопасности попадают и персональные данные сотрудников. Поэтому всплеск угроз в направлении персональных данных сотрудников компаний также заслуживает пристального внимания. О динамике роста утечек персональных данных красноречиво свидетельствует рисунок 1.

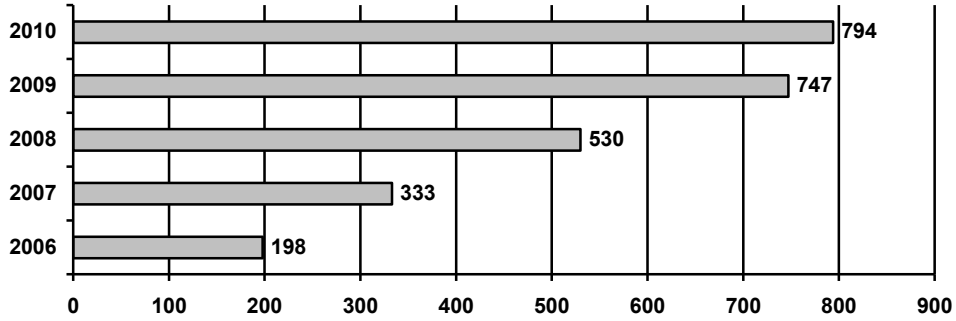


Рис. 1. Динамика роста утечек (2006-2010 гг.)[1]

Согласно, проведенному опросу, компанией Lieberman Software Corporation во время конференции RSA 2011 и Infosecurity Europe 2011, 42 % специалистов ИТ-отделов заявили, что могут беспрепятственно осуществить несанкционированный доступ к конфиденциальным данным компании. При этом 39 % опрошенных высказали мнение о том, что руководство не имеет представления об их возможностях, а 78 % – с полной уверенностью сообщают о способности беспрепятственного выноса корпоративных данных за пределы предприятия. Следует подчеркнуть, что данные исследования проводились среди ИТ-специалистов США и стран Западной Европы[2]. Но, как свидетельствует объективная действительность, отечественные

[1] См.: Ивановский В., Арсентьев А. Новый виток противостояния // CNews. 2011. № 55.
[2] См.: 2011 IT Attitudes and Outlook Survey // www.liebsoft.com/2011_Security_Survey.

работники ИТ-служб обладают не меньшими способностями и возможностями.

Вопросы ИТ-безопасности в настоящее время настолько остры, что руководителям стоит озаботиться их решением, предусматривающим проведение многочисленных организационных, технических, юридических, учебно-консультационных мероприятий. Сюда следует включать и мероприятия социальной инженерии, направленные на предупреждение, обнаружение, отражение, ликвидацию всевозможных видов угроз функционированию информационной инфраструктуры предприятия, минимизацию или поддержание на фиксированном низком уровне рисков, а также минимизацию возможного ущерба, возникшего при реализации этих угроз.

Практика показала, что решение проблем защиты информации, на предприятии, не ограничивается лишь приобретением и внедрением набора программно-аппаратных средств. Такие средства, безусловно, являются одними из важнейших элементов защиты, однако эффективность системы информационной безопасности напрямую связана с тем, насколько она интегрирована в общую информационную систему, и тем, существуют ли в компании стандарты, регламенты, процедуры, политики и руководящие документы по информационной безопасности. Естественно, что наличием в информационной системе разнообразных платформ и приложений определяется ее сложность, а это в свою очередь делает ее достаточно уязвимой. Данная ситуация усугубляется все возрастающей в настоящее время агрессивностью как внешней, так и внутренней среды.

Определить процессы, предоставляющие возможность бизнесу устанавливать, применять, пересматривать, контролировать и поддерживать эффективную систему менеджмента информационной безопасности (СМИБ) позволяет стандарт ИСО/МЭК 27001:2005 «Информационная технология. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования». Данным международным стандартом выбран

процессно-ориентированный подход при ведении, реализации, эксплуатации, мониторинге, пересмотре, поддержке и совершенствовании СМИБ организации. Этот подход, применительно к менеджменту ИБ, направлен на осмысление пользователями следующих сущностных особенностей, в частности:

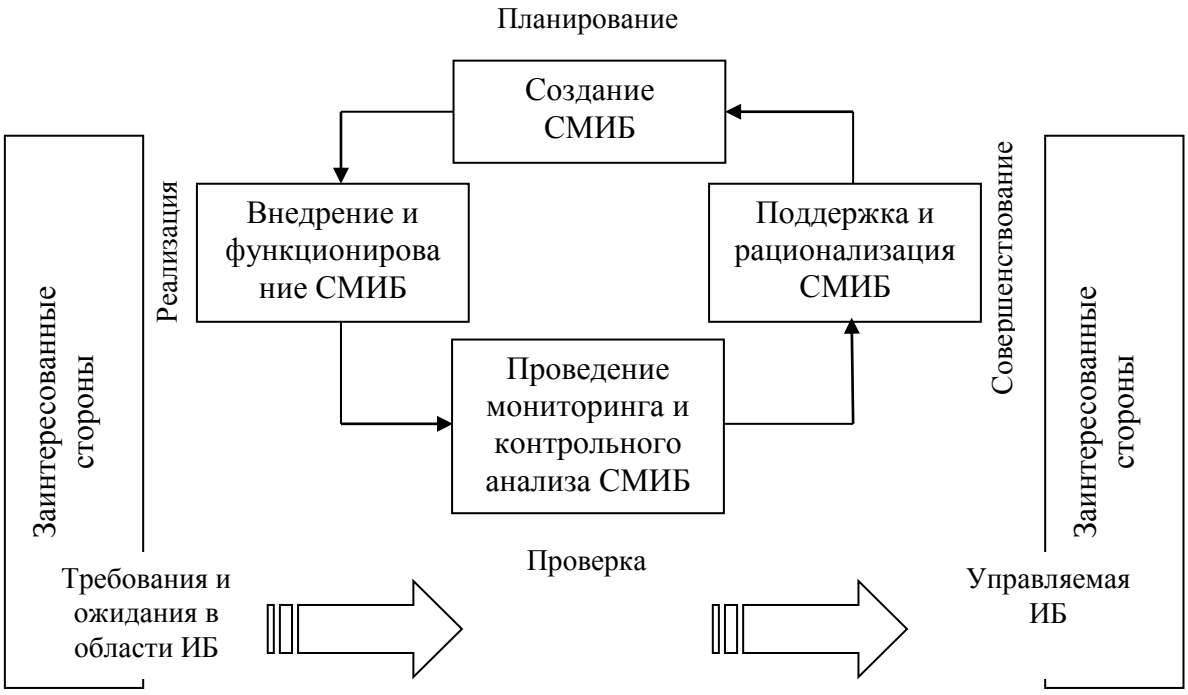
а) понимание требований к информационной безопасности организации и необходимости определения ее политики и целей;

б) внедрение и поддержка мер контроля для менеджмента рисков ИБ в контексте общего управления бизнес-рисками организации;

с) мониторинг и оценка производительности и эффективности СМИБ;

д) непрерывное совершенствование, основанное на объективных измерениях.[1]

Настоящий стандарт реализует модель «Plan-Do-Check-Act» (PDCA) «Планирование – Реализация – Проверка – Совершенствование» (ПРПС). Данная модель направлена на структурирование всех процессов СМИБ (см. рис. 2).



[1] ISO/IEC 27001:2005. Information technology – Security techniques – Information security management systems – Requirements.

Рис. 2. Процессы СМИБ

Так, процесс планирования (создания СМИБ) – направлен на разработку политики, целей и процедур СМИБ, относящихся к менеджменту риска и совершенствованию информационной безопасности, для достижения результатов, соответствующих общей политике и целям организации. Процесс реализации (внедрения и функционирование СМИБ) – требует внедрения и применения политики, мер (средства) контроля и процедур СМИБ. В свою очередь при проведении мониторинга и контрольного анализа СМИБ следует оценивать и измерять эффективность процессов относительно требований политики, целей безопасности и практического опыта СМИБ, а также информировать высшее руководство о результатах деятельности для последующего анализа. Процесс совершенствования, как завершающий в этом цикле, способствует проведению корректирующих и превентивных действий, основывающихся на результатах внутреннего аудита и анализа, осуществляемого высшим руководством, с целью достижения непрерывного совершенствования СМИБ.

Следует акцентировать внимание на трактовке понятия «безопасность информации» отраженном в настоящем стандарте. Так, под безопасностью информации (information security) понимается – сохранение ее конфиденциальности, целостности и доступности, а также охватываются другие свойства, такие как аутентичность, учетность, неотказуемость и надежность.

Принято считать, что информационная безопасность, связана, прежде всего, с проблемой ограничения доступа третьих лиц к информации. Но практика говорит об ином, это всего лишь одна из составляющих общего комплекса вопросов безопасности информации. Именно поэтому, передовые корпорации применяют лучшие мировые практики в области управления информационной безопасностью, к коим следует относить вышеупомянутый международный стандарт.

В связи с этим, важно подчеркнуть, что СМИБ требует от организации непреклонного выполнения ряда процедур по разработке, внедрению, эксплуатации, мониторингу, анализу, поддержке и непрерывному совершенствованию документально оформленной СМИБ с учетом особенностей ведения бизнеса и всех рисков организации (см. табл. 1).

Следует заметить, что целью построения СМИБ на предприятии, либо организации, является обеспечение выбора адекватных и соответствующих мер (средств) контроля безопасности, с помощью которых обеспечивается адекватная защита информационных активов и создается доверие заинтересованных сторон, а ее применение служит для покупателей и поставщиков гарантом высокого уровня защиты информации.

Таблица 1

Система менеджмента информационной безопасности

Создание СМИБ	
1.	Определить область применения СМИБ на основе характеристик бизнеса, организации, ее расположения, активов и технологий, включая детали и обоснование любых исключений из области
2.	Определить политику СМИБ на основе характеристик бизнеса, организации, ее расположения, активов и технологий
3.	Определить подход к оценке риска в организации
4.	Идентифицировать риски
5.	Проанализировать и оценить риски
6.	Определить и оценить различные варианты обработки рисков
7.	Выбрать цели и меры (средства) контроля для обработки рисков
8.	Получить одобрение руководства в отношении предлагаемых остаточных рисков
9.	Получить разрешение руководства на внедрение и эксплуатацию СМИБ
10.	Подготовить «Положение о применимости»
Внедрение и эксплуатация СМИБ	
1.	Разработать план обработки риска, определяющий соответствующие действия руководства, ресурсы, обязанности и приоритеты в отношении менеджмента рисков информационной безопасности
2.	Реализовать план обработки риска для достижения намеченных целей контроля, включающий вопросы финансирования, а также распределение ролей и обязанностей
3.	Реализовать меры (средства) контроля, выбранные для достижения целей контроля
4.	Определить, как измерять эффективность выбранных мер (средств) контроля или их групп и как использовать эти измерения для оценки эффективности контроля, чтобы получить сравнимые и воспроизводимые результаты
5.	Реализовать программы по обучению и повышению компетентности сотрудников
6.	Управлять работой СМИБ

7.	Управлять ресурсами СМИБ
8.	Реализовать процедуры и другие меры контроля, обеспечивающие оперативное обнаружение и реагирование на инциденты, связанные с безопасностью
Проведение мониторинга и анализа СМИБ	
1.	Выполнять процедуры мониторинга и контрольного анализа, а также использовать другие меры контроля
2.	Проводить регулярный анализ эффективности СМИБ (включая проверку ее соответствия политике и целям СМИБ и анализ мер контроля безопасности) с учетом результатов аудиторских проверок безопасности, инцидентов, измерении эффективности, а также предложений и пожеланий всех заинтересованных сторон
3.	Измерять эффективность средств контроля для проверки удовлетворения требований безопасности
4.	Пересматривать оценки рисков через запланированные промежутки времени и анализировать уровень остаточного и приемлемого риска
5.	Проводить внутренние аудиторские проверки СМИБ через запланированные интервалы времени
6.	Проводить на регулярной основе анализ СМИБ со стороны руководства для подтверждения адекватности области применения СМИБ и для выявления направлений совершенствования СМИБ
7.	Обновлять планы безопасности с учетом результатов анализа и мониторинга
8.	Регистрировать действия и события, которые могли бы оказать воздействие на эффективность или работу СМИБ
Поддержка и совершенствование СМИБ	
1.	Реализовывать выявленные возможности совершенствования СМИБ
2.	Предпринимать необходимые корректирующие и превентивные действия. Применять на практике опыт в области безопасности, полученный как в собственной организации, так и в других организациях
3.	Обмениваться информацией о результатах и проведенных мероприятиях со всеми заинтересованными сторонами со степенью детализации, подходящей для создавшихся обстоятельств, и, если нужно, согласовать дальнейшие действия
4.	Обеспечивать, чтобы внедряемые усовершенствования достигали ожидаемых целей

Исходя из этого, стандартизация в области информационной безопасности формирует единый подход при решении задач по обеспечению защиты информации, тем самым способствует повсеместному осознанию в организациях, на предприятиях, необходимости создания систем защиты информации с установлением адекватного порядка управления.

На наш взгляд, вступление Российской Федерации во Всемирную торговую организацию будет способствовать признанию и широкому внедрению, в повседневную деятельность отечественных компаний, международных стандартов, регулирующих подходы к оценке состояния информационной безопасности хозяйствующих субъектов. Именно на этот аспект заострял внимание Правительства РФ, президент страны, после

заседания Международного консультативного совета по созданию и развитию международного финансового центра в России.[1]

Таким образом, выполнение строгих правил и требований по информационной безопасности, непременно качественным образом скажется на состоянии дел в данной сфере, исходя из того, что сертификация на соответствие данным стандартам позволит наглядно показать партнерам, инвесторам, клиентам эффективную корпоративную систему защиты информации. Помимо всего прочего – это один из признаков соответствия хозяйствующего субъекта мировым стандартам.

Список использованных источников и литературы

1. В России признают международные стандарты в области защиты информации // www.securitylab.ru.
2. Ивановский В., Арсентьев А. Новый виток противостояния // CNews. 2011. № 55.
3. Количество регистрируемых киберпреступлений растет // Информационно-методический журнал «Защита информации. Инсайд». 2009. №6.
4. 2010/2011 Computer Crime and SeCurity Survey // www.gocsi.com.
5. 2011 IT Attitudes and Outlook Survey // www.liebsoft.com.
6. ISO/IEC 27001:2005. Information technology – Security techniques – Information security management systems – Requirements.
7. Докукин А.В., Ломакин М.И. Интеграция российских инновационных предприятий в мировую экономику на основе развития информационного обеспечения стандартизации // Российское предпринимательство, 2012, № 2.

[1] См.: В России признают международные стандарты в области защиты информации // www.securitylab.ru.; См.: Докукин А.В., Ломакин М.И. Интеграция российских инновационных предприятий в мировую экономику на основе развития информационного обеспечения стандартизации // Российское предпринимательство, 2012, № 2.