Разработка политики безопасности организации в свете новейшей нормативной базы

Статья опубликована в журнале "Защита информации. Конфидент" № 2, 2004.

А. С. Марков, к. т. н., с. н. с.,

С. В. Миронов, В. Л. Цирлов

Введение

Современная лицензионная политика в области безопасности информации определяет наличие у организаций, разрабатывающих средства защиты информации (СЗИ) или оказывающих услуги по защите информации, документа, в котором определены концептуальные и общеорганизационные вопросы информационной безопасности (ИБ). Традиционно в мировой практике такой документ называется политикой безопасности (ПБ) организации, однако в нашей стране до недавнего времени отсутствовали какие-либо четкие требования к документу такого рода. Актуальность разработки ПБ возникла с формированием новейшей нормативной базы в области ИБ, в первую очередь ГОСТ 15408-02 (и соответствующими РД Гостехкомиссии России [7, 8]), ГОСТ 15.002-00, а также ожидаемой отечественной редакцией ISO 17799. Структура и общие вопросы разработки ПБ с учетом новейшей нормативной базы по ИБ и рассматриваются в данной статье.

1. Политика безопасности: основное содержание

1.1. Новые нормативные требования, касающиеся политики безопасности организации

Общепринято понимать под ПБ документ, в котором отражены основные направления, цели и задачи, свои обязательства и важнейшие принципы деятельности предприятия в области защиты информации, официально сформулированные его высшим руководством и принятые к обязательному выполнению на предприятии. До недавнего времени необходимость в разработке ПБ в основном определялась пониманием руководства организации проблемы защиты ресурсов компьютерных систем и сетей организации. Надо сказать, что на российском рынке сложился рынок услуг по разработке документов такого рода, однако весьма различающихся по составу и содержанию [1, 2, 5, 6, 9].

Отношение к ПБ поменялось со становлением новой нормативной базы ИБ, с одной стороны, и совершенствованием требований лицензионных органов и центров к предприятиям, выпускающим продукцию или оказывающих услуги в области ИБ, - с другой.

Наиболее явно требования к документальному определению вопросов ИБ указаны для предприятий, выпускающих оборонную продукцию, - в ГОСТ 15.002-2000, где предусматривается обязательная программа обеспечения безопасности как часть политики качества. Указанный документ должен включать совокупность процедур, мероприятий и процессов обеспечения безопасности разработки (производства) СЗИ (составляющей гостайну), согласуется с представителем заказчика и подлежит обязательному инспекционному контролю. Однако определение и требования к содержанию собственно ПБ

Однако определение и требования к содержанию собственно ПБ даны во вступившем в силу с 2004 года ГОСТ 15408-02 и международном стандарте ISO 17799, российская редакция которого ожидается в самое ближайшее время. Рассмотрим данные стандарты более подробно.

1.2. ГОСТ 15408 - «Критерии оценки безопасности информационных технологий»

Согласно ГОСТ 15408 «Критерии оценки безопасности информационных технологий» (КОБИТ), ПБ организации - это одно или несколько правил, процедур, практических приемов или руководящих принципов в области безопасности, которыми руководствуется организация в своей деятельности [3, 8]. ПБ является одним из компонентов среды безопасности, включающей также законы, опыт, специальные навыки, знания и угрозы безопасности, присутствие которых в этой среде установлено или предполагается. Изложение ПБ организации включается в такие документы, как Профиль защиты и Задание по безопасности. В дальнейшем положения ПБ используются при формулировании Целей безопасности для объекта оценки и его среды. Также подчеркивается необходимость наличия механизмов проверки соответствия объекта оценки ПБ. Тем самым ПБ рассматривается в КОБИТ, прежде всего, как одно из базовых начальных условий

для разработки и оценки информационной системы. Однако определение ее чрезвычайно туманно, и, хотя круг вопросов, подлежащих формализации в рамках ПБ, очерчен, конкретные особенности разработки этого документа не затрагиваются. Более того, КОБИТ оставляют за рамками рассмотрения целый ряд проблем, традиционно включаемых в понятие «политика безопасности»: это и административные меры, и физическая защита, и вопросы управления персоналом. Такой подход, обеспечивающий некоторую дополнительную универсальность, подчеркивается самими разработчиками КОБИТ. Таким образом, сами по себе КОБИТ не содержат практических рекомендаций по разработке ПБ, а являются некоторым метастан-дартом, позволяющим формализовать отдельные аспекты ПБ, что мы покажем ниже.

Следует отметить, что некоторые организационные вопросы ИБ определены в документе «Общая методология оценки безопасности информационных технологий», разработанного в рамках международного проекта «Общих критериев» (Common Criteria for IT Security Evaluation), однако не имеющего пока нормативного аналога в нашей стране.

1.3. ISO 17799-неформальный подход к разработке политики безопасности

Заявления руководства Гостех-комиссии России на ряде заседаний ТК-362 о готовящейся версии (видимо, аутентичной) международного стандарта ISO 17799 позволяет нам рассмотреть известный практический стандарт относительно трактовки ПБ.

Документ ISO 17799 [9, 10] состоит из двух частей. Первая - «Практические рекомендации» - определяет и рассматривает следующие аспекты ИБ:

- политика безопасности;
- организация защиты;
- классификация и управление информационными ресурсами;
- управление персоналом;
- физическая безопасность;
- администрирование компьютерных систем и сетей;
- управление доступом к системам;
- разработка и сопровождение систем;
- планирование бесперебойной работы организации;
- проверка системы на соответствие требованиям ИБ.

Вторая часть - «Спецификации системы» - рассматривает те же аспекты с точки зрения сертификации информационной системы на соответствие требованиям стандарта.

Очевидно, что положения стандарта ISO 17799 как нельзя более удачно дополняют КОБИТ.

Предписываемая документом структура политики информационной безопасности изображена на рис. 1.

Обратим внимание на требования стандарта по инвентаризации информационной инфраструктуры, подлежащей защите. Помимо программно-аппаратных, информационных и коммуникационных ресурсов, сюда следует отнести имеющиеся в организации нормативные документы, которые не должны вступать в противоречие с положениями ПБ. Обработка в рамках защищаемой системы информация подлежит категоризации по уровню секретности или конфиденциальности.

Соответствие законодательству также является одним из важнейших аспектов разработки ПБ, зачастую определяющим значительную часть используемых технологий защиты (классический пример для России - ограничения по легальному использованию криптографических средств). Во избежание возможных осложнений соответствующие вопросы должны быть согласованы с экспертом по правовому обеспечению ИБ.

Подчеркнем также важную роль раздела, определяющего ответственность за обеспечение ИБ. Хотя традиционно персональную ответственность за проведение мер по обеспечению ИБ несет руководитель организации, необходимо четкое распределение должностных обязанностей и ответственности между конкретными должностными лицами. Каждый сотрудник должен четко представлять свои обязанности в области защиты информации и ответственность за их невыполнение.

Обучение персонала в области ИБ должно проводиться непрерывно, как в процессе работы, так и по мере необходимости в специализированных учебных центрах. Соответствующий раздел ПБ должен содержать обязанности должностных лиц по консультированию и инструктированию пользователей информационной системы, а также порядок прохождения профессиональной переподготовки.

Следует отметить, что ПБ не является и не может являться единственным документом, регламентирующим процесс обеспечения ИБ организации. Одновременно с ПБ должны быть разработаны подробные инструкции, относящиеся к конкретным вопросам реализации ПБ. Если сама ПБ является документом статичным, определяется общей инфраструктурой организации и подлежит корректировке только в случае ее коренного изменения, то инструкции должны непрерывно обновляться и совершенствоваться по ходу модернизации информационной системы

предприятия. Общие рекомендации по настройке СЗИ (безотносительно к конкретным продуктам) целесообразно включить в состав ПБ, конкретные же рекомендации по безопасному конфигурированию приложений разрабатываются администратором ИБ в виде одной или нескольких инструкций.

Особняком среди инструкций стоит план обеспечения непрерывности ведения бизнеса. Часто этот вопрос выносится за рамки проблематики ИБ - и совершенно неоправданно, поскольку при разработке такого плана необходимо полагаться, прежде всего, на анализ рисков безопасности, выполняемый в рамках общего аудита безопасности системы. Конкретная методология анализа рисков стандартом не регламентируется и может быть выбрана исходя из сложившихся на предприятии подходов к управлению рисками или же на базе одной из общеизвестных методик. Ручной анализ рисков является трудоемким и для больших компаний вряд ли целесообразен, поэтому рекомендуется применение автоматизированных систем управления рисками. (RiskWatch, BRA и др.). Ключевой момент обеспечения непрерывности деятельности информационной системы - выделение критических компонентов этой системы и четкая отработка мероприятий по их восстановлению в случае поражения. Дополнительным методом обеспечения непрерывности деятельности, хотя и менее результативным, является страхование, позволяющее значительно снизить ущерб в случае реализации выявленных угроз.

1.4. Пример структуры неформальной политики безопасности

Исходя из рассмотренных выше положений стандарта ISO 17799, можно предложить следующую структуру типовой ПБ организации.

1. Общие положения.

- 1.1. Назначение документа.
- 1.2. Основания для разработки документа.
- 1.3. Основные определения.

2. Идентификация системы.

- 2.1. Идентификатор и имя системы.
- 2.2. Ответственные подразделения.
- 2.3. Режим функционирования системы.
- 2.4. Описание и цели системы.
- 2.5. Цели и задачи ПБ.
- 2.6. Системная среда.
  - 2.6.1. Физическая организация системы.
  - 2.6.2. Логическая организация системы.
- 2.7. Реализованные сервисы системы.
- 2.8. Общие правила, принятые в системе.
- 2.9. Общее описание важности информации.

3. Средства управления.

- 3.1. Оценка рисков и управление.
- 3.2. Экспертиза СЗИ.
- 3.3. Правила поведения, должностные обязанности и ответственность.
- 3.4. Планирование безопасности.
- 3.5. Разрешение на ввод компонента в строй.
- 3.6. Порядок подключения подсетей подразделения к сетям общего пользования.

4. Функциональные средства.

- 4.1. Защита персонала.
- 4.2. Управление работой и вводом-выводом.
- 4.3. Планирование непрерывной работы.
- 4.4. Средства поддержки программных приложений.
- 4.5. Средства обеспечения целостности информации.
- 4.6. Документирование.
- 4.7. Осведомленность и обучение специалистов.
- 4.8. Ответные действия в случаях возникновения происшествий.

5. Технические средства.

- 5.1. Требования к процедурам идентификации и аутентификации.
- 5.2. Требования к системам контроля и разграничения доступа.
- 5.3. Требования к системам регистрации сетевых событий.

Примерные инструкции по реализации ПБ могут быть, например, следующими:

1. Требования к защите портов и служб.
2. Порядок проведения экспертизы СЗИ.
3. Порядок проведения анализа рисков.
4. Использование автоматизированных систем анализа защищенности.
5. Порядок восстановления автоматизированных систем после аварийных ситуаций.

Конкретный перечень необходимых инструкций определяется используемой аппаратно-программной платформой. Приведенная структура ПБ, жизнеспособность которой подтверждена неоднократным опытом внедрения, полностью соответствует положениям обоих рассмотренных стандартов.

1.5. Формализация положений политики безопасности

Мы показали, что на неформальном описательном уровне ПБ организации может быть успешно разработана на основании стандарта ISO 17799. Однако, хотя в ряде случаев результаты такого подхода оказываются вполне достаточными для координации мероприятий по комплексному обеспечению ИБ организации, зачастую требуется формальное определение требований ПБ. Преимущества формального подхода очевидны:

- формальные положения ПБ допускают исчерпывающий анализ их полноты и непротиворечивости;
- облегчается процесс проверки соответствия объекта оценки положениям ПБ.

В качестве базы для формализации положений ПБ целесообразно выбрать КОБИТ. Указанный мета-стандарт содержит исчерпывающий комплекс требований, которые могут быть успешно использованы для построения разного рода стандартов, а значит, и для формализации неформально изложенных требований ПБ. Структура соответствующего документа ничем не регламентируется, однако целесообразно представлять ПБ организации как Профиль защиты объекта оценки «Информационная инфраструктура организации». Конкретные же инструкции по реализации положений ПБ можно рассматривать как Задание по безопасности этого же объекта оценки [7].

Проиллюстрируем вышесказанное на рассмотренном выше примере структуры ПБ. Выделим те разделы, которые целесообразно формулировать в терминах КОБИТ, и приведем ссылки на соответствующие семейства требования стандарта [3, 8].

2. Идентификация системы.

2.1. Идентификатор и имя системы.

Идентификатор системы целесообразно выбрать в стиле КОБИТ, например S.MAINSYS, где S - идентификатор группы родственных систем, а MAINSYS - идентификатор конкретной (главной) системы.

3. Средства управления.

3.1. Оценка рисков и управление.

- Семейство FMT_MOF - Управление отдельными функциями - требует установление возможности конфигурирования средств безопасности только уполномоченными пользователями.
- Семейство FMT_MSA - Управление атрибутами безопасности - требует наличие контроля безопасности присваиваемых значений.
- Семейство FMT_SAE - Сроки действия атрибутов безопасности - регламентирует использование временных ограничений.
- Семейство FMT_SMR - Роли управления безопасностью - регламентирует порядок назначения порядка соответствующих ролей пользователям.
- Семейство FTA_LSA - Ограничение области выбираемых атрибутов - определяет требования по ограничению области атрибутов безопасности, которые может выбрать пользователь.
- Семейство FTA_SSL - Блокирование сеанса - определяет порядок блокирования или завершения сеанса работы по инициативе пользователя или системы безопасности.

3.2. Экспертиза СЗИ.

- Семейство FPT_TST - Самотестирование функций безопасности - определяет порядок самотестирования и контроля целостности данных и исполняемого кода функций безопасности.

4. Функциональные средства.

4.1. Защита персонала.

- Семейство FDP_UCT - Защита конфиденциальности данных пользователя - требует обеспечить защиту данных от несанкционированного раскрытия.
- Семейство FPT_PHP - Физическая защита - регламентирует меры по обеспечению физической безопасности системы и ее отдельных компонентов. В частности, определяются меры ответного воздействия в случае физического нападения (см. также раздел 4.8).

4.2. Управление работой и вводом-выводом.

- Семейство FDP_RIP - Защита остаточной информации - определяет порядок защиты от повторного использования информации.
- Семейство FTA_TAH - История доступа - определяет требования к отображению истории попыток получить доступ от имени пользователя, осуществившего успешный вход в систему.

4.3. Планирование непрерывной работы.

- Семейство FRU_FLT - Отказоустойчивость - задает требования по обеспечению непрерывного функционирования системы в случае сбоя. Данный раздел является формализацией Плана по непрерывному ведению бизнеса.
- Семейство FPT_ELS - Безопасность при сбое - требует обеспечение выполнения положений ПБ при сбоях заданных типов.

4.5. Средства обеспечения целостности информации.

- Семейство FDP_SDI - Целостность хранимых данных - определяет меры по мониторингу целостности защищаемых объектов и действия в случае обнаружения нарушения целостности.
- Семейство FDP_ROL - Откат - регламентирует возможность восстановления последнего стабильного состояния системы, то есть отмены последней операции с целью сохранения целостности данных пользователя.
- Семейство FDP_UIT - Защита целостности данных пользователя - регламентирует меры противодействия модификации, удаления, вставки и повторного использования данных. Из всей совокупности требований целесообразно выбрать только наиболее общие, оставив частные вопросы для задания по безопасности конкретных систем.
- Семейство FPT_RCV - Надежное восстановление - регламентирует возможность автоматического восстановления безопасного состояния в случае определенного вида сбоев.

5. Технические средства.

5.1. Требования к процедурам идентификации и аутентификации.

- Семейство FIA_UID - Идентификация пользователя - определяет набор действий, выполнение которых возможно до идентификации. В большинстве случаев целесообразно использовать компонент FIA_UID.2, запрещающий такие действия.
- Семейство FIA_UAU - Аутентификация пользователя - специфицирует применяемые технологии аутентификации и режимы их работы.
- Семейство FIA_ATD - Определение атрибутов пользователя - позволяет связать неформально определенные атрибуты безопасности с субъектом пользователя, который, в свою очередь, определяется семейством FIA_USB - Связывание пользователь-субъект.
- Семейство FPR_ANO - Анонимность - определяет услуги, предоставляемые системой без идентификатора пользователя. В соответствующий перечень необходимо включить, в частности, все общедоступные услуги, предоставляемые компанией.

5.2. Требования к системам контроля и разграничения доступа.

- Семейство FDP_ACC - Политика управления доступом - определяет режим и порядок разграничения доступа.
- Семейство FDP_ACF - Функции управления доступом - описывает правила для конкретных функций, которые могут реализовать политики управления доступом, и определяет область действия этих политик.
- Класс FCS - Криптографическая поддержка - определяет порядок работы с криптографическими ключами, а также криптографические операции.

5.3. Требования к системам регистрации сетевых событий.

- Семейство FAU_GEN - Генерация данных аудита безопасности - определяет подвергаемые протоколированию и аудиту события, уровень протоколирования, перечень регистрационных данных о событии, а также предписывает ассоциировать потенциально регистрируемые события с идентификаторами пользователей системы.
- Семейство FAU_SEL - Выбор со бытий аудита безопасности - определяет атрибуты, на основании которых производится выбор протоколируемых событий безопасности.
- Семейство FAU_STG - Хранение событий аудита безопасности - определяет порядок хранения и защиты регистрируемой информации.
- Семейство FAU_SAA - Анализ аудита безопасности - регламентирует требования к механизмам аудита безопасности.
- Семейство FAU_ARP - Автоматическая реакция аудита безопасности - определяет требования к применяемым методам активного аудита.

Разумеется, предложенный подход к формализации ПБ не является единственно возможным и допускает дальнейшее развитие. При практической разработке формальной ПБ могут быть успешно применены стандартные средства автоматизации применения КОБИТ, порядок использования которых заслуживает отдельного рассмотрения.

2. Разработка политики безопасности организации: средства автоматизации

2.1. Особенности разработки политики безопасности

Разработка ПБ организации, как формальной, так и неформальной, - безусловно, нетривиальная задача. Эксперт должен не только владеть соответствующими стандартами и хорошо разбираться в комплексных подходах к обеспечению ИБ организации, но и, например, проявлять недюжинные детективные способности при выявлении особенностей построения информационной системы и существующих мер по организации защиты информации. Сходная проблема возникает в дальнейшем при необходимости анализа соответствия рекомендаций ПБ реальному положению вещей: необходимо по некоторому критерию отобрать своего рода «контрольные точки» и сравнить их практическую реализацию с эталоном, задаваемым ПБ.

В общем случае можно выделить следующие процессы, связанные с разработкой и реализацией ПБ и поддающиеся автоматизации. 1. Комплекс мероприятий, связанных с проведением анализа рисков. К этой группе можно отнести:

- учет материальных или информационных ценностей;
  - моделирование угроз ИБ системы;
  - собственно анализ рисков с использованием того или иного подхода - например, стоимостный анализ рисков.
2. Мероприятия по оценке соответствия мер по обеспечению ИБ системы некоторому эталонному образцу: стандарту, формальной политике безопасности, профилю защиты и т. п.
3. Действия, связанные с разработкой разного рода документов, в частности отчетов, диаграмм, профилей защиты, заданий по безопасности.
4. Действия, связанные со сбором, хранением и обработкой статистики по событиям безопасности для организации.

В настоящее время на рынке отсутствуют системы, которые предоставляли бы исчерпывающие средства для автоматизации всех перечисленных аспектов разработки ПБ. Наиболее широко представлены средства для автоматизации анализа рисков, а также для проверки соответствия информационной системы компании положениям того или иного стандарта. Именно на последних системах в силу их относительной новизны, а также с учетом роли, которую они потенциально могут сыграть для популяризации соответствующих стандартов, стоит остановиться подробнее.

2.2. COBRA: неформальные советы мудрой змеи

Наиболее известный программный продукт, предназначенный для проверки выполнения требований стандарта ISO 17799, - это система COBRA производства компании C & A Systems Security Ltd. Помимо анализа соответствия информационной системы компании положениям стандарта, система обеспечивает также автоматизацию проведения анализа рисков. Оценка соответствия системы положениям стандарта ISO 17799 производится следующим образом. Пользователю предлагается ответить на ряд вопросов из следующих групп (рис. 2):

1. Классификация активов и управление ими. Под активами в данном случае понимаются материальные и информационные ценности, рассматриваются вопросы их учета и классификации.
2. Планирование непрерывности ведения бизнеса. Рассматриваются вопросы разработки планов непрерывного ведения бизнеса, их тестирования и распределения ответственности.
3. Управление компьютерными операциями. Выделяется широкий перечень вопросов, связанных с управлением процессами и сервисами безопасности.
4. Соответствие. Рассматриваются вопросы соответствия информационной инфраструктуры различного рода требованиям, инструкциям и рекомендациям.
5. Безопасность персонала. Рассматриваются вопросы распределения ответственности по реализации положений ПБ между сотрудниками, а также порядок приема сотрудников.
6. Физическая безопасность и безопасность среды. Рассматриваются вопросы организации физической защиты на территории предприятия, охраны, контроля физического доступа, энергетической и противопожарной безопасности.
7. Организация безопасности. Рассматриваются вопросы организации службы ИБ на предприятии - в частности, создания форумов по безопасности, а также порядок взаимодействия со сторонними экспертами по безопасности и распределение ролей в ходе реализации мероприятий по защите информации между сотрудниками.
8. Политика безопасности. Вопросы данного раздела преследуют цель определить положение ПБ в системе мер по обеспечению ИБ организации, а также позволяют оценить структуру этого документа и его применимость на практике.
9. Управление доступом к системе. Рассматриваются вопросы контроля и разграничения доступа, а также категорирования защищаемой информации.
10. Разработка и поддержка системы. Рассматриваются вопросы обеспечения ИБ системы на протяжении всего жизненного цикла. В частности, оцениваются применяемые технологии анализа рисков.

Для ответа на очередной вопрос предлагается выбрать либо один, либо несколько возможных вариантов (рис. 3).

Для значительной части вопросов имеются комментарии, поясняющие используемые понятия. На основании сведений, полученных в ходе выполнения всех вопросников или некоторой их части, COBRA автоматически генерирует отчет (рис. 4):

Структура отчета.

1. Введение. Содержит общую информацию о сгенерированном отчете.
2. Обзор проверки соответствия. В разделе детализируется информация об использованном вопроснике, выделяются использованные модули и категории вопросов.
3. Анализ несоответствий. Раздел содержит исчерпывающий анализ выявленных несоответствий с указанием ссылок на соответствующие разделы стандарта ISO 17799.
4. Требования по улучшению. Приводятся рекомендации по устранению обнаруженных несоответствий.
5. Перечень вопросов и ответов. Раздел содержит перечень вопросов, которые были использованы при построении отчета, и соответствующих ответов.

Проведенный анализ показывает, что система COBRA действительно позволяет реализовать исчерпывающую проверку соответствия информационной системы положениям стандарта ISO 17799. Однако необходимо подчеркнуть, что COBRA ни в коей мере не претендует на то, чтобы заменить собой эксперта в области ИБ. Действительно, достоверность результатов анализа, проведенного с помощью COBRA, полностью определяется адекватностью ответов на вопросники, которые, в свою очередь, требуют глубокого понимания механизмов обеспечения ИБ, а также архитектуры и особенностей реализации подлежащей оценке информационной системы. Тем не менее в руках специалиста COBRA может стать удобным инструментом, позволяющим значительно ускорить процесс разработки и реализации неформальной ПБ.

Спартанский интерфейс программы не отличается особой изысканностью, однако навигация в большинстве случаев достаточно удобна и интуитивно понятна. Наиболее серьезным препятствием для распространения системы в России является ее англоязычность, которая во многих случаях исключает возможность непосредственного использования сгенерированных отчетов.

2.3. КОНДОР: ISO 17799 с высоты птичьего полета

Программный комплекс КОНДОР (разработчик - компания Digital Security) является русскоязычным аналогом COBRA-подобной системы, также предназначенной для оценки

соответствия информационной системы положениям стандарта ISO 17799 [4]. Концепции этих двух пакетов совершенно аналогичны: на основании ответов на вопросы генерируется отчет. Вопросы структурированы в следующие разделы:

- политика безопасности;
- организационные меры;
- управление ресурсами;
- безопасность персонала;
- физическая безопасность;
- управление процессами;
- контроль доступа;
- непрерывность бизнеса;
- соответствие системы;
- разработка систем.

По глубине анализа (числу вопросов) КОНДОР несколько проще, чем COBRA. Кроме того, возможности по анализу рисков у текущей версии системы отсутствуют. В текущей версии есть определенные некорректности, впрочем, принципиально не снижающие ценность продукта. Так, в блоке «Политика безопасности» можно на первый же вопрос ответить, что ПБ в организации отсутствует - но разговор на этом не будет закончен, придется описывать подробные характеристики этой (несуществующей) ПБ. Соответственно, при построении диаграммы в отчете полученные данные анализируются исключительно с количественной точки зрения - в приведенном на рис. 6 примере требования к несуществующей ПБ скорее выполнены, чем не выполнены.

Наименее проработанным, на наш взгляд, компонентом системы КОНДОР является генератор отчетов. Собственно отчет (см. рис. 5) представляет собой перечень разделов стандарта с указанием тех из них, с которыми выявлено соответствие. К некоторым из положений стандарта доступны краткие комментарии. Также имеется возможность построения диаграмм, показывающих степень соответствия системы требованиям стандарта. Какие либо рекомендации или выводы частично отсутствуют, что несколько снижает эффективность использования подобного рода отчетов.

Отдельной критики заслуживает интерфейс программы. Просмотр отчета достаточно неудобен и требует навигации в четырех направлениях, то же самое можно сказать о справочной системе. При всем при этом, к очевидному достоинству системы КОНДОР по сравнению с COBRA является русскоязычный интерфейс. Остается надеяться, что дальнейшие версии продукта будут следовать по пути более развитого конкурента.

2.4. CC Toolbox: автоматизация разработки формальной политики безопасности

Рассмотренные нами системы ориентированы исключительно на проверку соответствия требованиям стандарта ISO 17799, что соответствует неформальному уровню разработки ПБ. Формальный уровень, в свою очередь, предполагает использование инструментария КОБИТ, и наиболее известным средством автоматизации в данном случае является пакет CC Toolbox. Общий вид интерфейса пакета CC Toolbox представлен на рис. 7.

Система обеспечивает автоматизацию разработки двух типов документов:

- профилей защиты;
- заданий по безопасности.

Порядок работы с CC Toolbox во многом аналогичен продуктам COBRA и КОНДОР. Пользователю предлагается ответить на ряд вопросов, полностью специфицирующих все разделы профиля защиты или задания по безопасности. На основании информации, полученной из анализа ответов на вопросы, генерируется соответствующий документ, который может быть экспортирован в html-формат или распечатан.

Поскольку требования КОБИТ в отличие от ISO 17799 являются формальными, проблемы полноты вопросников не возникает. Выбор компонентов КОБИТ осуществляется интуитивно понятным образом и в естественном порядке. Принятая концепция позволяет учитывать логические связи между разделами документа, что позволяет эффективным образом вносить изменения в процессе разработки профиля защиты или задания по безопасности. Итак, пакет CC Toolbox может быть с успехом использован при формализации ПБ. Единственным ограничением является опять-таки англоязычность пакета. Однако с учетом аутентичности перевода отечественной версии КОБИТ можно предположить, что разработка русскоязычной версии не составит особого труда. Разработка такой версии продукта могла бы самым благоприятным образом повлиять на ход внедрения ГОСТ Р ИСО/МЭК 15408-2002 в нашей стране.

Заключение

Со становлением новейшей нормативной базы ИБ сформировались основные требования к ПБ как концептуальному и общеорганизационному документу по ИБ организации. Детальные требования к содержанию ПБ будут определены с выходом в свет отечественного прототипа стандарта ISO 17799, а также «Общей методологии оценки безопасности информационных технологий», однако вступивший в силу в текущем году ГОСТ 15408 предоставляет средства формализации основных положения ПБ.

Кроме того, в распоряжении экспертов уже имеется линейка инструментальных средств, позволяющих автоматизировать ряд формальных операций по разработке ПБ. Дальнейшее развитие подобных продуктов должно стать одним из факторов, способствующих успешному применению новейшей нормативно-правовой базы в области обеспечения ИБ.

ЛИТЕРАТУРА

1. Галатенко В. А. Основы информационной безопасности: Курс лекций. — М.: ИНТУИТ.ру, 2003.- 280 с.
2. Законодательно-правовое и организационно-техническое обеспечение информационной безопасности АС и ИВС / Котенко И. В., Котухов М. М., Марков А. С. и др. Под ред. И. В. Котенко. - СПб: ВУС, 2000. - 190 с.
3. Комментарии к Российскому стандарту ГОСТ Р ИСО/МЭК 15408-2002 «Критерии оценки безопасности информационных технологий» / Долинин М. Ю., Кобзарь М. Т., Лыков В. А. и др. - М.: ФГУП «ЦНИИАТОМИН-ФОРМ», 2003. - 38 с.
4. Медведовский И. Д. Программные средства проверки и создания политики безопасности. — SecurityLab, 2004. — <http://www.security-hb.ru/42546.html>
5. Политика безопасности при работе в Интернет: Техническое руководство / Б. Гутман, Р. Бэгвилл; Пер. с англ. Казенова В. Н. — NIST Special Publication 800-12 - 42 с.
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. Руководящий документ. Безопасность информационных технологий — Руководство по разработке профилей защиты и заданий по безопасности. — М.: Гостехкомиссия России, 2003.
8. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. — М.: Гостехкомиссия России, 2002. — Части 1, 2, 3.
9. Симонов С. Аудит безопасности ИС. — Info Jet, 1999. - № 9- 24 с.
10. Управление информационной безопасностью: Практические правила — Info Jet, приложение, 1999.