**Сравнение директив безопасности**

Йоханнес Зауэр

**Управление безопасностью в соответствии с ITIL, ISO и BSI.**

Современным предприятиям адекватный уровень безопасности нужен сегодня больше, чем когда-либо. Деловые и ИТ-процессы переплетаются все теснее: качество первых сильно зависит от готовности служб ИТ, а недоступность последних часто отрицательно сказывается на конкурентоспособности. В связи с этим вот уже в течение многих лет прослеживается тенденция к стандартизации методов и мероприятий в области безопасности информационных технологий.

В последние годы в области безопасности ИТ появилось множество стандартов. Все они нацелены на реализацию адекватной защиты информационных технологий. Соответствующие своды правил и эталонные модели описывают британская ITIL, британский стандарт BS 7799, опирающийся на него стандарт ISO/IEC 17799 и руководство по базовой защите, изданное германским ведомством по безопасности информационной техники (BSI).

**Эталонная модель ITIL**

Библиотека инфраструктуры ИТ (Information Technologies Infrastructure Library, ITIL) своим появлением обязана стремлению британских властей разработать стандартизированный метод для улучшения качества, безопасности и экономичности процессов ИТ. Для этого Управление государственной торговли Великобритании вместе с предприятиями и организациями выработало эталонную модель, в рамках которой возможна универсальная реализация процессов ИТ.

Содержащаяся в своде правил ITIL библиотека процессов предлагает практическую методологическую модель для внедрения стандартизированных процессов в управлении службами ИТ (IT Service Management, ITSM). Главные задачи — улучшение качества услуг ИТ для непрерывных процессов и обеспечение их экономической эффективности. Библиотека процессов делится на несколько разделов. Важнейшие базовые процессы описываются в разделах Service Delivery (доставка услуг) и Service Support (поддержка услуг). Теме безопасности ИТ отводится раздел Security Management (управление безопасностью).

Управление безопасностью в соответствии с ITIL преследует две крайне важные цели:

выполнение требований по безопасности, содержащихся в соглашениях об уровне сервиса (Service Level Agreement, SLA), и других внешних требований, следующих из договоров, законов и правил корпоративной безопасности (политики);

создание определенной (не специфицированной более подробно) базовой защиты.

ITIL, как и BS 7799, уходит корнями в 1980-е гг. С тех пор она утвердилась в качестве стандарта де-факто для моделирования, реализации и управления деловыми процессами ИТ. Возможности сертификации предприятия на соответствие требованиям ITIL в данный момент не существует, вместо этого

ответственные лица могут подтвердить свое знание ITIL и стать обладателями сертификата ITIL Foundation Certificate. Его наличие является необходимым условием для получения базирующегося на нем и значительно более всеобъемлющего сертификата ITIL Service Manager Certificate.

BS 7799 И ISO 17799

British Standard 7799, как и ITIL, содержит практический опыт, которым предприятия и организации могут воспользоваться при реализации мер но обеспечению безопасности ИТ. Уже в конце 80-х гг. у британских властей возникла идея введения стандарта в области безопасности информации. Это привело к разработке «Системы правил управления безопасностью информации» под руководством Министерства торговли и промышленности. Первая часть BS 7799 была опубликована в качестве стандарта в 1995 г. Всего же в BS 7799 Две части:

BS 7799, часть 1 (ISO/IEC 17799) - руководство по управлению информационной безопасностью;

BS 7799- часть 2 - спецификация систем управления информационной безопасностью.

Если в первой части предлагаются лишь рекомендации по принятию необходимых мер, то во второй — определяются методы и требования к системе управления информационной безопасностью (Information Security Management System, ISMS). Поскольку BS 7799 привлек к себе внимание специалистов других стран, в январе 2000 г. первая часть была преобразована в стандарт Международной организации по стандартизации (International Organization for Standardization, ISO). ISO/IEC 17799:2000 в данный момент находится на доработке и предположительно летом текущего года будет опубликована в версии 17799:2005э Главные цели ISO/IEC 17799 включают в себя следующее:

определение практически полезных минимальных требований в области безопасности ИТ;

создание общей базы для предприятий, заинтересованных в разработке, реализации и измерении эффективной системы безопасности;

предоставление контрольного стандарта для управления безопасностью ИТ в пределах организации.

ISO/IEC 17799:2000 состоит из десяти тематических разделов, где содержится 127 рекомендаций, которые не представляют собой обязательных норм. Потому сертификация возможна лишь в рамках BS 7799-2.

**Руководство BSI**

Еще один возможный подход опирается на руководство по базовой защите информационных технологий BSI. Каждые полгода но мере накопления и приобретения новых знаний об информационных опасностях и технологиях BSI обновляет руководство. Оно содержит описание стандартных мер по безопасности, указания по реализации, вспомогательные средства для многочисленных наиболее часто используемых конфигураций ИТ и нацелено на решение регулярно возникающих проблем, поддержание повышенного уровня безопасности и упрощение разработки концепции безопасности ИТ. Предлагаемые здесь стандартные меры ориентируются на среднюю потребность в защите, типичную для большинства систем ИТ.

Исходным пунктом для выбора адекватных мер безопасности является так называемая концепция безопасности, которая вырабатывается на основе имеющихся процессов. Для того же сначала на предприятии проводится анализ структуры с целью определения фактического состояния систем ИТ и приложений, а затем устанавливается степень потребности в защите (планируемое состояние). Базирующееся на этих результатах сравнение желательных показателей с фактическими отражает дефицит безопасности, на основе чего определяются необходимые мероприятия (см. Рисунок 1). Весьма полезным оказывается построение руководства в виде блок-схемы, благодаря которому становится возможным простое применение комплексных мер.

Метод эффективен во многом благодаря тому, что цель создания измеряемой базовой защиты ИТ достигается без дорогостоящего анализа рисков. Дополнительный анализ (к примеру, анализ рисков и угроз) необходим лишь в том случае, если система нуждается в более высоком уровне безопасности. BSI предлагает предприятиям сертификацию: сертификат базовой защиты информационных технологий. Кроме того, существует возможность «самопознания», включающая две ступени: «начальный уровень базовой защиты ИТ» и «стандартный уровень базовой защиты ИТ».

**Сравнение подходов**

Все три подхода преследуют цель долгосрочного обеспечения безопасности ИТ и отличаются лишь лежащими в их основе принципами.

Руководство BSI по базовой защите ИТ предлагает структурированный метод создания концепции безопасности и реализации управления безопасностью ИТ. В нем четко описываются необходимые шаги по разработке концепции безопасности. Во многом благодаря такой процессной структуре его использование оказывается очень эффективным. Комплекс мер очень конкретен, и в некоторых случаях даже приводятся значения параметров, которые непосредственно могут быть реализованы в соответствующей системе ИТ. Это очевидная сильная сторона модели BSI. Степень детализации рекомендаций но предлагаемым мерам позволяет быстро внедрить адекватный уровень безопасности информационных технологий. Однако такая техническая глубина не всегда оправдана при интеграции в области деловых процессов, где требуется более высокая степень абстракции. Так, к примеру, руководство BSI не описывает, как предприятие может интегрировать ISMS в уже существующие процессы.

В противовес этому TSO/TEC 17799 описывает требования к мерам по безопасности ИТ скорее с информационной точки зрения и ориентируется на некий типовой уровень. 127 общепризнанных рекомендаций ISO/IEC 17799 чосят все же примерный характер: они служат в качестве ориентира и не обязательны к исполнению. Так, пользователь не найдет советов по поводу длины пароля и прочих деталей конфигурации систем ИТ, как это свойственно для руководства по базовой безопасности систем ИТ. Такой описательный подход позволяет провести общее определение целей безопасности, не вникая во все технические детали.

Оба названных стандарта концентрируются исключительно на безопасности ИТ, между тем как ITIL появилась вследствие совершенно иной мотивации. Хотя безопасность ИТ — очень важная часть самых разных базовых процессов ITIL, к примеру управления непрерывностью, первичной мотивацией внедрения ITIL являются цели бизнеса: ITIL в первую очередь нацелена на то, чтобы адаптировать ландшафт ИТ к требованиям пользователей и клиентов. В этот иерархический процессный подход включается и управление безопасностью. Поэтому внедрение системы управления безопасностью в соответствии с 1TIL имеет смысл лишь тогда, когда организация ИТ уже отвечает требованиям ITIL или ее планируется привести в соответствие с ними. Тогда станет возможным обращаться к имеющимся процессам ITIL и дополнять их функциями и процессам и безопасности.

Внедрение управления безопасностью в соответствии с ITIL оказывает значительное влияние на организацию служб ИТ: свод правил предусматривает дополнение всех базовых процессов значительным — относящимся к безопасности — содержимым (Service Desk, например, в качестве единой точки обращения за помощью). При этом могут использоваться имеющиеся структуры процессов и инструменты отчетности. ITIL предлагает возможность определения ключевого индикатора производительности (Key Performance Indicator, KPI) для измерения эффективности на основе количественных характеристик. Так, об эффективности принятых мер можно судить по количеству инцидентов в области безопасности за определенный промежуток времени.

Кроме того, база данных управления конфигурацией (Configuration Management Database, CMDB) предоставляет централизованную структуру данных. Она очень хорошо расширяется в соответствии с требованиями трех целей защиты: готовности, надежность и целостность. Таким образом оказывается доступен всеобъемлющий инструмент с широким набором интерфейсов. Что касается ISMS, то IT1L в этом случае ссылается на BS 7799 как на эталон в управлении безопасностью, а в приложении А дастся сравнение ITIL и BS 7799.

В случае всех трех подходов речь идет о признанных на международном уровне стандартах безопасности информационных технологий, причем ITIL, в силу исторических причин, занимает особое место. Каждый отличается своими особенностями. Одним из возможных критериев выбора может быть стремление или потребность сертификации: ITIL предлагает лишь возможность персональной сертификации; сертификация в рамках BS 7799 проводится только для второй части (7799-2), а сертификат базовой защиты ИТ, напротив, включает в себя проверку определенного в нем управления безопасностью ИТ, а также реализацию соответствующих мер. На практике часто предлагается своего рода комбинация в целях наилучшего использования особенностей содержания и методов каждого стандарта.

**Список литературы**

Журнал LAN №8 2005