Управление конфигурациями представляет собой контроль изменяющейся IT-инфраструктуры, ее стандартизацию, инвентаризацию, отслеживание ее состояния, верификацию ее составных частей (представляющих собой обычно набор программного и аппаратного обеспечения и иногда называемых конфигурационными единицами), управление документацией по IT-инфраструктуре, а также предоставление информации об IT-инфраструктуре для всех других процессов управления IT-услугами.

Управление изменениями заключается в определении необходимых изменений в IT-инфраструктуре и способов их проведения с минимальным негативным воздействием на оказание IT-услуг. Изменения могут возникать в результате управления проблемами или выполнения некоторых других процессов управления IT-услугами либо производиться по запросам заказчика. Внесение изменений производится согласно определенным правилам, включающим описание, планирование, создание, тестирование, принятие окончательного решения о проведении изменения, внедрение и оценку результата.

В контексте информационной безопасности наибольшее значение имеет процесс управления конфигурациями, поскольку в его рамках осуществляется классификация конфигурационных единиц и определяются связи между конфигурационными единицами и предпринимаемыми мерами или процедурами безопасности для каждого из уровней их классификации (такие меры или процедуры могут, к примеру, быть описаны во внутрикорпоративных регламентах).

Управление изменениями является одним из наиболее важных процессов, связанных с управлением безопасностью, — именно в процессе управления изменениями в IT-инфраструктуре вводятся и новые меры безопасности. Так, предложения по решению вопросов безопасности обычно включаются в запросы на внесение изменений, и любые меры безопасности, связанные с внесением изменений, должны реализовываться одновременно с проведением самих изменений, а также совместно тестироваться. Тесты проверки безопасности отличаются от обычных функциональных тестов: при обычных тестах проверяется доступность определенных функций, тогда как при тестировании безопасности дополнительно проверяется отсутствие функций, которые могут снизить безопасность системы.

**Управление Конфигурациями**

В контексте информационной безопасности процесс Управления конфигурациями имеет наибольшее значение, так как он позволяет классифицировать Конфигурационные Единицы (CI). Эта классификация определяет связи между Конфигурационными Единицами и предпринимаемыми мерами или процедурами безопасности.

Классификация Конфигурационных Единиц определяет их конфиденциальность, целостность и доступность. Эта классификация основана на требованиях безопасности соглашений SLA. Заказчик ИТ-организации определяет классификацию, так как только заказчик может решить, насколько важны информация или информационные системы для бизнес-процессов. При создании классификации Конфигурационных Единиц заказчик учитывает степень зависимости бизнес-процессов от информационных систем и информации. Затем ИТ-организация увязывает классификацию с соответствующими Конфигурационными Единицами. ИТ-организация должна также реализовать комплекс мер безопасности для каждого Уровня Классификации. Эти комплексы мер могут быть описаны как процедуры, например, «Процедура обращения с носителями данных с личной информацией». В соглашении SLA могут определяться комплексы мер безопасности для каждого Уровня Классификации. Система классификации должна всегда быть совместима со структурой организации заказчика. Однако для упрощения управления рекомендуется использовать одну общую систему классификации, даже если ИТ-организация имеет несколько заказчиков.

Из вышесказанного можно сделать вывод, что классификация является ключевым моментом. Каждая Конфигурационная Единица в Конфигурационной Базе Данных (CMDB) должна быть классифицирована. Эта классификация связывает Конфигурационную Единицу с соответствующим комплексом мер безопасности или процедурой.

**Управление Изменениями**

Виды работ, выполняемых в рамках Процесса Управления Изменениями, часто бывают тесно связаны с безопасностью, так как Управление Изменениями и Управление Информационной Безопасностью взаимозависимы. Если достигнут приемлемый Уровень Безопасности, который находится под контролем Процесса Управления Изменениями, то можно гарантировать, что этот Уровень Безопасности будет обеспечиваться и после проведения изменении. Для поддержки этого Уровня Безопасности существует ряд стандартных операций. Каждый Запрос на изменения (RFC) связан с рядом параметров, которые определяют процедуру приемки. Параметры срочности и степени воздействия могут быть дополнены параметром, связанным с безопасностью. Если Запрос на изменения (RFC) может оказать значительное воздействие на информационную безопасность, потребуются расширенные приемочные испытания и процедуры.

В Запрос на изменения (RFC) также должны быть включены предложения по решению вопросов безопасности. Они опять же должны основываться на требованиях SLA и базовом Уровне Внутренней Безопасности, необходимом для ИТ-организации. Следовательно, эти предложения будут включать комплекс мер по обеспечению безопасности, основанный на Практических нормах по Управлению Информационной Безопасностью.

Желательно, чтобы руководитель Процесса Управления Информационной Безопасностью (а также, возможно, инспектор по безопасности от заказчика) был членом Консультативного комитета по изменениям (Change Advisory Board – CAB).

Однако это не значит, что по всем изменениям необходимо консультироваться с Руководителем Процесса Управления Информационной Безопасностью. В нормальной ситуации безопасность должна быть интегрирована в обычный рабочий режим. Руководитель Процесса Управления Изменениями должен иметь возможность решать, требуется ли ему или комитету CAB входная информация от Руководителя Процесса Управления Информационной Безопасностью. Точно так же руководитель Процесса Управления Информационной Безопасностью не обязательно должен участвовать в выборе мер для конкретных Конфигурационных Единиц затронутых Запросом на Изменения (RFC), так как для соответствующих мер уже должен существовать структурированный подход. Вопросы могут возникнуть только со способом реализации указанных мер.

Любые меры безопасности, связанные со внесением изменений, должны реализовываться одновременно с проведением самих изменений, и они должны тестироваться совместно. Тесты безопасности отличаются от обычных функциональных тестов. Задачей обычных тестов является определение доступности определенных функций. При тестировании безопасности проверяют не только доступность функций безопасности, но также отсутствие других, нежелательных функций, которые могут снизить безопасность системы.

С точки зрения безопасности Управление Изменениями является одним из наиболее важных процессов. Это объясняется тем, что Управление Изменениями вводит новые меры безопасности в ИТ-инфраструктуру вместе с изменениями этой инфраструктуры