

Лабораторная работа 5. Управление конфигурациями, изменениями и обновлениями

Цель лабораторной работы: определить основные цели и функции процессов управления конфигурациями, изменениями и обновлениями; рассмотреть, что между ними общего и в чем их различия; изучить жизненный цикл процесса управления обновлениями ИБ.

Задачи лабораторной работы:

1. Управление конфигурациями
 2. Управление изменениями
 3. Управление обновлениями ИБ
- Контрольные вопросы

Содержание лабораторной работы:

1. Управление конфигурациями

Для того чтобы информационные активы случайно не подвергались ненужному риску ИБ и имели меньше уязвимостей, необходимо управлять изменениями в конфигурациях ПО и АО. Все изменения сначала надлежащим образом проверяются, утверждаются, документируются и только после этого внедряются. Так, неверные конфигурации или ненадлежащее функционирование веб-сервера организации могут привести к раскрытию информации ограниченного доступа, информации о пользователях или администрировании веб-сервера, включая пароли, настройки веб-сервера и сети, что может быть использовано для последующих атак.

Управление конфигурациями (англ. configuration management) является жизненно важным для достижения целей организации - оно позволяет контролировать текущее состояние и выбирать будущее¹. Но подход к этому виду управления только с технической и процедурной точек зрения может вызвать бездействие важных процессов, которые могли бы повысить уровень ИБ организации и достигнуть успеха в бизнесе. Управление конфигурациями обеспечивает непротиворечивость, полноту и точность ОИБ. Оно также содержит механизм определения текущего состояния ИБ в организации для всех используемых технологий, выполняемых процессов и практик, а также средств оценки воздействия изменений на это состояние.

Назначение управления конфигурациями - предоставлять разработчикам и клиентам точные и актуальные данные, сохранять требуемое состояние активов, анализировать и контролировать изменения в выделенных (в соответствии со стратегией управления изменениями) так называемых конфигурационных единицах, рассматриваемых при конфигурировании как отдельно, так и совместно. Примеры конфигурационных единиц: записи о любых обновлениях ПО или проблемах установки, настройки безопасности для систем и их изменения, изменения в требованиях ОИБ, реализация средств управления, результаты анализа ИБ и т. д.

Цель процесса управления конфигурациями – сохранить контроль над установленными конфигурациями работающих продуктов. Его применение обеспечивает следующее²³⁴:

- *используются соответствующие процессы и инструменты для создания и поддержания соответствия между продуктом, требованиями к нему (изложенными в проекте и актуальных ПолИБ) и его свойствами, определенными в документации по конфигурации продукта;*

¹ Tipton H. F., Krause M. Information Security Management Handbook. 6th edition. Taylor & Francis Group, USA, 2007.

² ISO 10007:2003 «Quality Management. Guidelines for Configuration Management».

³ MIL-HDBK-61A «Configuration Management Guidance», 2001.

⁴ ANSI/EIA 649-A «National Consensus Standard for Configuration Management», 2004.

- *гарантируется, что продукт соответствует своим требованиям, достаточно подробно описан и задокументирован для поддержки его жизненного цикла; при этом документация находится под контролем и отражает последний, утвержденный вариант;*
- *о конфигурации продукта предоставляется точная информация и есть возможность интероперабельности (способности к взаимодействию) и взаимозаменяемости продукта и его безопасной эксплуатации и технического обслуживания;*
- *реализация функций, принципов и практик управления конфигурациями в течение всего жизненного цикла продукта осуществляется сбалансировано и последовательно;*
- *облегчается упорядоченное определение свойств продукта и обеспечивается контроль за информацией о продукте и его изменениях, используемых для улучшения его возможностей; исправляются недостатки, улучшается производительность, надежности и управляемость; продлевается срок службы или снижается стоимость, риски и обязательства;*
- *конечные пользователи имеют возможность поддерживать старые и приобретать обновленные версии поставляемых продуктов.*

Перечислим основные функции процесса управления конфигурациями:

- 1) *планирование управления конфигурацией;*
- 2) *идентификация конфигураций;*
- 3) *контроль и управление изменениями конфигураций;*
- 4) *учет состояния конфигураций;*
- 5) *проверка (включая тестирование перед настройкой на конкретных продуктах) и аудит конфигураций;*
- 6) *взаимодействие и обмен данными о конфигурации.*

Процесс управления конфигурациями состоит из следующих под-процессов:

- *установление методологии управления конфигурациями;*
- *идентификации конфигурационных единиц;*
- *поддержание настроек и стандартов для работающих средств;*
- *контроль изменений для выделенных конфигурационных единиц;*
- *информирования о состоянии конфигурации.*

Строгие процедуры управления конфигурацией включают в себя положения о периодических физическом и функциональном аудитах на реальной системе в среде ее эксплуатации. Они не полагаются только на документацию или известные, или предлагаемые изменения. Любые несоответствия обнаруживаются только при непосредственном обследовании АО, ПО и данных.

Хорошо разработанный и применяемый процесс управления конфигурациями лучше всего приспособляется ко всем изменениям и гарантирует, что вся затронутая при этом информация остается понятной, четкой и имеющей силу.

Выбор средств управления конфигурациями для поддержки процесса управления зависит от существующих бизнес-процессов и связанных с ними ресурсов, требующих конфигурирования. Обычно к этим средствам относятся формы, используемые для контроля изменений, соглашения по маркировке конфигурационных единиц, библиотеки ПО, автоматизированные средства управления конфигурациями и т. д.

Обязательно составляется план управления конфигурациями, описывающий, что должно быть сделано для внедрения процесса управления конфигурациями в организации, включая процедуры, средства, роли и обязанности ответственных лиц. Его важность для распределенных систем, объединяющих различные подсистемы, так или иначе затрагиваемые при конфигурировании, особенно очевидна. Такой план облегчает обоснование необходимых ресурсов и средств управления конфигурациями. Он должен быть тщательно проверен и утвержден, а также допускать возможность расширения и

внесения необходимых изменений.

Управление конфигурациями, реализуемое в соответствии с установленным планом, дает множество преимуществ организации, в том числе:

- *принятие решений на основе знания всех последствий изменений;*
- *внесение только тех изменений, которые необходимы или дают значительные преимущества;*
- *анализ эффективности предлагаемых изменений;*
- *высокий уровень доверия к информации о продукте или его конфигурациях;*
- *упорядоченное согласование изменяемой информации;*
- *сохранение интересов клиентов;*
- *знание текущей конфигурации систем;*
- *управление конфигурациями через интерфейсы продуктов;*
- *соответствие между конфигурациями систем и соответствующей документацией;*
- *простота обслуживания системы после внесения изменений.*

2. Управление изменениями

Внесение изменений в ПО, АО, ИС, изменение окружающей среды (появление новых угроз ИБ и средств их реализации, обнаружение новых уязвимостей для существующих систем), деградация или недоступность старых защитных мер, окончание срока действия сертификата на систему и многое другое неизбежно в любой организации, что в конечном счете влияет на ее уровень ИБ. Поэтому управление изменениями (англ. change management) является сегодня одной из самых серьезных проблем для многих организаций. В быстро меняющемся мире ИТ и столь же быстро откликающемся рынке соответствующих продуктов управление изменениями - это ключ к тому, чтобы только оправданные и хорошо продуманные изменения вносились в системы до их запуска в массовое производство. Под давлением необходимости быстрых изменений без следования формализованному процессу их внесения много раз возникали критические сбои систем, поскольку тестирование внесенных изменений проводилось в недостаточном объеме или постоянно обнаруживались новые непредвиденные технические проблемы.

Вопросами управления изменениями в ИС занимаются уже более 30 лет, им посвящено много публикаций. Фирма IBM впервые стала рассматривать управление изменениями не как отдельную дисциплину, а как составную часть управления ИС. С тех пор эта область знаний сильно расширилась, были предложены различные подходы к управлению изменениями. В настоящее время процесс управления изменениями обычно связывают с методологией ITIL (согласно ей, целью процесса управления изменениями является обеспечение применения стандартизированных процедур и методов внесения изменений для уменьшения вероятности возникновения после этого различных инцидентов), хотя существуют и другие методологии, например, COBIT, Microsoft Operational Framework и другие.

Известно два аспекта управления изменениями⁵. Первый подразумевает наличие заранее определенных средств управления, гарантирующих, что все изменения, которые предлагаются для существующих систем, надлежащим образом проверены, утверждены и структурированы (логически и систематически запланированы и осуществлены). Другой аспект связан с управлением проектами и разработкой систем. Когда организация готовится к покупке и развертыванию новой или модификации уже существующей системы, она, как правило, в рамках управления проектами контролирует выполнение требований бюджета, обучения, соблюдения сроков и кадрового обеспечения. Обычно (как ожидается в зависимости от типа жизненного цикла) такие проекты претерпевают

⁵ Tipton H. F., Krause M. Information Security Management Handbook. 6th edition. Taylor & Francis Group, USA, 2007.

значительные изменения на протяжении всего жизненного цикла проекта, что определяется в ключевых точках принятия решений. Часть изменений вносятся в проект под воздействием внешних (экономического климата, действенности маркетинга, наличия квалифицированных кадров и т. п.) или внутренних (например, определение новых требований пользователей) факторов. Эти изменения зачастую влияют на область действия (объем необходимых работ и результаты), сроки или бюджет проекта. Изменения, внесенные в проект где-то в середине его жизненного цикла, могут привести к тому, что проект станет очень громоздким, требующим уплаты больших финансовых штрафов (особенно когда речь идет об аутсорсинговой компании), или он не сможет вовремя позитивно повлиять на бизнес-операции. Тогда управлением изменениями должна заняться соответствующая группа, которая будет рассматривать предлагаемые для проекта изменения и согласовывать их в рамках плана проекта.

Управление изменениями обязывает, чтобы все изменения в АО, ПО, документации и процедурах тщательно анализировались квалифицированными специалистами до их реализации. Даже самые незначительные изменения в конфигурации или установке нового оборудования могут вызвать катастрофические отказы в системе. В некоторых случаях изменение может создать новую уязвимость, что остается незамеченным в течение длительного периода времени. Изменения в документации должны вноситься таким образом, чтобы все используемые документы относились к одной и той же версии продукта, документация была полной и понятно написанной, а все программы и системы имели соответствующую документацию. Кроме того, копии важной документации должны храниться за пределами участка ее использования, чтобы обеспечить их доступность в случае крупного стихийного бедствия или потери доступа к основным площадям организации.

При принятии решения о внесении изменений обязательно анализируется срочность их внесения, наравне с вопросами обеспечения процесса ресурсами, технической поддержкой и т. п. По мере внесения изменения сохраняются все записи, свидетельствующие о том, что, как, кем и когда изменялось.

Если какая-либо новая технология рассматривается с целью ее дальнейшего применения, соответствующий анализ демонстрирует эффект от этого с нескольких точек зрения:

- *затраты на приобретение, установку, обслуживание и мониторинг;*
- *положительное/отрицательное взаимодействие с существующими технологиями или архитектурами;*
- *производительность;*
- *уровень ИБ;*
- *удобство использования;*
- *методы управления, которые должны быть модифицированы для применения новой технологии;*
- *человеческие ресурсы, которые должны быть обучены корректному использованию новой технологии (например, пользователь или провайдер).*

После внесения изменений осуществляется их анализ, в ходе которого выясняется, удалось ли осуществить изменение, достигнут ли ожидаемый эффект, какие возникли сложности в ходе его осуществления и т.д. Иногда изменения могут не привести к ожидаемому результату, или, что еще хуже, оказать неблагоприятное воздействие на работу различных систем и приложений. В этом случае все системы, как правило, возвращают к состоянию, предшествующему внесению изменения.

После внесения существенных изменений продукты, ранее имевшие сертификаты, как правило, должны повторно сертифицироваться (ре- сертифицироваться). Поэтому каждое изменение рассматривается с целью выяснения его влияния на предыдущие условия сертификации. Если изменилась окружающая среда продукта или его возможности по обеспечению требований ИБ, тогда продукт также подлежит ресертификации.

3. Управление обновлениями ИБ

Известно три основных типа обновлений для систем⁶:

- 1) обновления ИБ (англ. *security patches*), корректирующие известные уязвимости, используемые угрозами ИБ;
- 2) функциональные обновления (англ. *functionality patches*), исправляющие некорректное функционирование систем, не связанное с ИБ;
- 3) обновления характеристик (англ. *feature patches*), добавляющие новые возможности или функции в существующие ОС и приложения.

Во многих случаях процесс управления обновлениями подразумевает обновления ИБ. Как правило, разработчики внедряют остальные два типа во время фазы тестирования приложения или обновления ПО, но обычно не в рамках самого процесса управления исправлениями. Поэтому далее будем рассматривать управление именно обновлениями ИБ.

Всеобъемлющий процесс управления обновлениями ИБ является одним из основных в настоящее время для любой организации, использующей для ведения бизнеса компьютеры, сети и приложения. Внедрение этого процесса обеспечивает своевременное, эффективное и результативное устранение уязвимостей в информационных активах организации. Управление обновлениями ИБ обязывает к большей ответственности и дисциплине при решении задач обнаружения, анализа и исправления уязвимостей, влияющих на общий уровень ИБ организации.

Решаемые в рамках данного процесса задачи очень разнообразны. Он выполняет следующие функции:

- *расширяет процесс управления ИБ большой проблемной областью управлением уязвимостями, необходимым по мере поступления информации о только что обнаруженных уязвимостях, эффективно расставляющим приоритеты для дальнейших действий и уменьшающим требуемые для этого ресурсы;*
- *усовершенствует способ защиты организации от современных, постоянно увеличивающихся угроз ИБ;*
- *способствует распространению информации среди пользователей, владельцев и администраторов ИС и сетей, ответственных за своевременную установку обновлений ИБ;*
- *формализует хранение записей для последующего контроля и написания отчетности;*
- *вводит автоматизированный порядок, который может быть при необходимости легко адаптирован;*
- *улучшает подотчетность для ролей, несущих ответственность за ИБ активов.*

Установить обновления ИБ на рабочие станции при имеющемся темпе их выпуска в неделю просто невозможно (это огромный поток обновлений!), особенно используя ручные методы. Компания Gartner оценила, что администраторы систем каждый день около двух часов вынуждены заниматься установкой таких обновлений. И если, например, только Microsoft выпускает в среднем новое обновление каждые пять дней, как им быть в крупных организациях?

Сложность и трудоемкость процесса определяется необходимостью сортировки растущего числа оповещений, выяснением применимости к уникальным ИТ-средам и конфигурациям, тестированием обновления до начала его массового использования и, наконец, самой своевременной установкой обновлений. Это не всегда под силу даже организациям, обладающим большими ресурсами в области поддержки ИТ. Иногда установка нового обновления может в конечном счете породить больше проблем, чем

⁶ Tipton H. F., Krause M. Information Security Management Handbook. 6th edition. Taylor & Francis Group, USA, 2007.

решить – могут появиться новые уязвимости. Без систематизированного, повторяемого и проверяемого процесса управления обновлениями ИБ некоторые из них забывают применить вообще, а другие устанавливают по несколько раз. Но единого, готового для всех организаций решения на сегодня не существует.

Ясно, что управление обновлениями ИБ требует комплексного подхода, охватывающего людей, процессы и технологии. Поэтому в организации обязательно должен быть разработан формализованный процесс, который будет применяться для отражения растущих угроз ИБ, использующих известные и устраняемые уязвимости информационных активов, и тем самым повышающим их защищенность.

Практика управления обновлениями ИБ предполагает реализацию нескольких этапов этого процесса, количество которых зависит от организации - ее информационной инфраструктуры (централизованной или децентрализованной), размера, используемых АО, ПО и ИС, степени автоматизации и модернизации, доступности ресурсов, окружающей среды и т. п. Базовые составляющие этого процесса - оценка, применение и мониторинг, которые по мере освоения данного вида управления организация может расширить.

Для управления обновлениями ИБ устанавливают политики (например, по срокам и применению обновлений, для конфигурационных стандартов, для проверки совместимости, консультирования и обмена информацией и т.д.) и процедуры, определяют зоны ответственности и терминологию. Некритичные обновления для некритичных систем можно устанавливать по расписанию в специально выделенное для этого время. Эти обновления нужно выполнять как можно раньше после обеспечения их стабильной работы и только если они устраняют имеющуюся проблему. Критичные обновления должны устанавливаться во внерабочее время как можно раньше после обеспечения их стабильной работы.

Для внедрения программы и плана управления обновлениями ИБ организация разрабатывает весь жизненный цикл процесса управления, обеспечивающего своевременное и точное применение обновлений ИБ во всей организации.

Хотя процессы управления обновлениями ИБ в настоящее время хорошо известны и связаны с другими ключевыми ИТ-операциями и вспомогательными процессами управления (изменения, системы и активы), требуется выполнить большой объем предварительной работы по планированию, проектированию, интеграции и внедрению эффективной и гибкой программы управления обновлениями ИБ.

Жизненный цикл процесса управления обновлениями ИБ состоит из следующих этапов.

1. *Разработка системы управления инвентаризацией основного ПО с автоматизированным или ручным интерфейсом с другими системами управления - активами, изменения, конфигурациями и т. д. и четко определенной информацией по каждому объекту инвентаризации (АО, производитель, ОС, номер версии, IP-адрес, физическое местонахождение устройства, системный администратор, владелец, критичность системы, роль компьютера, контактная информация и т. п.). Для этого на регулярной основе могут использоваться различные сканеры.*
2. *Разработка плана стандартизации конфигураций ПО для всей организации: все поддерживаемое ПО должно иметь одну и ту же версию, выпуск, пакет обновления и т. д., все изменения должны быть зафиксированы; для любых изменений должны быть записаны имя/номер обновления, ранее установленное обновление, функциональное описание предпринятых действий, источник кода (откуда он был получен), даты загрузки и установки кода, имя установщика. Должен быть определен цикл установки обновлений, позволяющий своевременно применять все выпуски и обновления. Обновления или изменений конфигураций должны быть интегрированы в соответствующие конфигурационные стандарты для приложений/систем.*

3. *Определение наилучшего источника информации по оповещениям и новым обновлениям ПО и возможным проблемам по их установке, включая различные подписки и рассылки (электронные и печатные), информацию от производителя, посещение соответствующих вебсайтов и т. п.*
4. *Оценка готовности организации к эксплуатации обновлений: есть ли квалифицированный персонал, понимание важности и поддержка процесса управления обновлениями, уже используемая практика в этой области и т. д.*
5. *Тщательная оценка риска ИБ для окружающей среды и разработка рейтинговой системы для критичных обновлений, включая оценку уровня уязвимости, вероятности применения средств, использующих их (англ. exploit), серьезности угрозы ИБ и ее воздействия на общий уровень ИБ организации, стоимости-эффективности ее устранения (по сравнению с ценностью находящихся под угрозой активов) и стоимости восстановления после ее реализации. Эти действия рекомендуется завершить в срок не позднее, чем двое суток после идентификации уязвимости. Для уязвимости, затрагивающей важные бизнес-процессы, все последующие действия выполняются немедленно. В результате принимается решение о необходимости устранения уязвимости в зависимости от ее серьезности и сложности в использовании, типов и путей распространения атак на ее основе, критичности активов и их расположения, риска ИБ для активов, доступности обновлений ИБ и т. п.*
6. *Тестирование в лабораторных условиях на соответствующем макете всех обновлений до их использования, поскольку иногда они бывают не очень качественными, из непроверенного источника или с нарушенной целостностью.*
7. *Разработка и внедрение стратегии установки и развертывания обновлений, учитывающей, что в один момент времени можно устанавливать только одно обновление (а не несколько сразу). При этом важно строго следовать документации по установке. Для всех систем, приложений, данных и конфигурационных файлов, затрагиваемых обновлениями, до начала процесса нужно создать резервные копии. Также необходима разработка плана технического восстановления (с детализированными указаниями по шагам, необходимым для устранения уязвимости), а также плана возврата к исходному состоянию в случае непредвиденных проблем, вызванных внедрением плана восстановления, и сроки внедрения обоих планов. Должны быть определена контактная информация. При необходимости вносите изменения в стратегию. Процесс развертывания обновлений по возможности должен быть автоматизирован. Необходимо вести документирование жизненного цикла каждой уязвимости, включая подготовку отчетов и отслеживание мер восстановления для всех бизнес-направлений.*
8. *Обеспечение постоянного мониторинга и оценки текущей ситуации (по отслеживанию уязвимостей в активах организации, стандартных конфигураций, установленных обновлений) с подготовкой соответствующей отчетности (по установке обновлений, проверкам совместимости и инвентаризации).*

В процессе управления обновлениями ИБ в организации обычно участвуют администраторы ИБ и систем, устанавливающие обновления для этих систем, и риск-менеджеры, оценивающие воздействие уязвимостей на активы организации. Конечно же, требуется поддержка всего процесса со стороны как высшего руководства (в стратегических вопросах), так и руководства среднего звена (в тактических вопросах).

Контрольные вопросы

1. Каковы основные цели и функции процессов управления конфигурациями, изменениями и обновлениями? Что между ними общего и в чем различия?
2. Опишите жизненный цикл процесса управления обновлениями ИБ.

Задание

Отчет по лабораторной работе выполняется по стандарту, описанному в методических указаниях