УДК 004.896

Сковиков Н.А.
студент
2 курс, факультет «Математики, информационных и авиационных технологий»
Федеральное государственное бюджетное образовательное учреждение высшего образования «Ульяновский государственный университет»
Россия, г. Ульяновск

ОБЕСПЕЧЕНИЕ РАБОТОСПОСОБНОСТИ И КАЧЕСТВА ФУНКЦИОНИРОВАНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ НА ОСНОВЕ ITSM

Аннотация: *Статья посвящена комплексу мер по поддержанию работоспособности и качества функционирования информационных систем в плане обеспечения информационной безопасности предприятия (организации). Эффективным способом решения этой задачи является использование процессной модели ITSM. В работе демонстрируется каким образом методология ITSM способствует повышению качества защиты каждого сервиса в отдельности и всей системы безопасности в целом.*

Ключевые слова: *ITIL, ITSM, информационная безопасность, управление доступностью, ИТ-менеджмент, служба поддержки пользователей, сервисы безопасности.*

Annotation: *An important component of information security is a set of measures to maintain the efficiency and quality of functioning of information systems. The aim of the work is to substantiate the solution of this problem based on the ITSM. The authors demonstrate how the ITSM methodology helps to improve the quality of protection for each security service individually and for the entire security system as a whole.*

Key words: *ITIL, ITSM, information security, accessibility management, IT management, Service Desk, security services.*

Комплекс мероприятий, обеспечивающих поддержание работоспособности и качества функционирования информационных систем, является неотъемлемой частью интегрированной системы информационной безопасности. Ошибка или халатность системного администратора способны разрушить до основания самую инновационную, и тщательно продуманную политику безопасности. Данное направление регламентирует стратегическую и оперативную деятельность ИТ-службы организации или предприятия, включая меры, обеспечивающие предоставление пользователям услуг ИТ-сервисов заданного качества (мощность, доступность, непрерывность, безопасность, пропускная способность и т.д.); организацию эффективной службы мониторинга инцидентов и поддержки пользователей (Service Desk); предоставление пользователям доступа к ИТ-сервисам, используемым в бизнес-деятельности предприятия; управление конфигурациями информационных систем; организацию работы ИТ-департамента в плане управления ИТ-инфраструктурой, актуализации репозитория (базы данных), служащего для описания элементов конфигурации, их взаимосвязей и атрибутов; поддержку программного обеспечения; управление ИТ-проектами, релизами и носителями информации, в том числе разработку регламентов резервного копирования, функционирования библиотеки эталонного программного обеспечения (DSL); создание системы, обеспечивающей внедрение только обоснованных изменений в ИТ-инфраструктуре и фильтрацию потенциально опасных проектов; организацию постоянного аудита оборудования и программного обеспечения; обязательное документирование всех процессов и изменений; проведение регламентных работ, четкое разграничение зон ответственности и полномочий пользователей и персонала ИТ-службы; формализацию и доведение до

заинтересованных сторон измеримых критериев качества работы; формирование действенных механизмов мониторинга состояния процессов и корректирующих воздействий в случае необходимости. Решение указанных задач позволит добиться соответствия уже использующихся и только еще планирующихся ИТ-сервисов динамике изменений в информационных потребностях бизнеса, происходящих перманентно.

Все эти вопросы нашли свое отражение в методологии обеспечения эффективности деятельности ИТ-департамента предприятия — ITSM (Information Technology Service Management, управление ИТ-услугами), основанной на результатах, полученных в ходе реализации проекта ITIL (The Information Technology Infrastructure Library, библиотека инфраструктуры информационных технологий). В этом, по сути, стандарте сконцентрирован и обобщен передовой опыт тысяч организаций в области управления информационными технологиями. Новые подходы к организации ИТ-менеджмента, формализованные в виде модели управления качеством информационных услуг, появились в результате осознания трансформации роли и места ИТ-департаментов в структуре предприятия. Согласно новой трактовке, акценты деятельности ИТ-подразделений смещаются в сторону качественного обслуживания основных бизнес-процессов компании, а сами ИТ-службы должны гармонично вписаться в основную производственную деятельность, выступая в роли поставщиков информационных сервисов для нужд бизнес-подразделений.

Дополнительным мотивом внедрения типовых моделей бизнес-процессов ИТ-департамента является широкая поддержка концепции ITSM ведущими разработчиками программного обеспечения. На рынке доминируют программные решения в области ИТ-менеджмента от Hewlett Packard (OpenView), IBM (Tivoli), Microsoft (пакет приложений).

Рассмотрим некоторые процессы, направленные на поддержание работоспособности информационной системы, немного подробнее.

Прежде всего отметим постоянно возрастающее значение службы поддержки пользователей (Help Desk или Service Desk). При этом акцент в деятельности службы поддержки смещается с реактивной парадигмы, на проактивные методы и подходы, подразумевающие анализ проблемных ситуаций специалистами и предотвращение на основе проведенных исследований новых сбоев и нарушений.

Решающим фактором в обеспечении эффективности процесса поддержки пользователей является создание единой точки обращений по вопросам, касающимся любых недостатков в отношении информационных сервисов (инцидентов, согласно терминологии ITSM). Необходимо уметь в общем потоке обращений выделять проблемные моменты, связанные с информационной безопасностью.

В рамках процесса управления доступностью организация обеспечивает устойчивый, экономически обоснованный и удовлетворяющий запросам бизнеса режим функционирования ИТ-сервисов, включая информационные услуги, предоставляемые внешними поставщиками. Способность информационных систем выдерживать заданное качество обслуживания потребностей бизнес-структур предприятия или его клиентов основывается на надежности (независимость результатов от сбоев оперативного характера) и восстанавливаемости рабочего состояния ИТ-инфраструктуры (например, за счет дублирования).

Целостность массивов деловой информации обеспечивается процессами поддержки программного обеспечения, максимальной автоматизации ручных, рутинных операций, управления конфигурациями, резервного копирования и мониторинга носителей данных. Должен быть организован постоянный контроль версий и корректности установленного на вычислительных машинах программного обеспечения. Вообще, самодеятельность пользователей в плане выбора используемых приложений почти наверняка приведет к появлению новых брешей в системе безопасности или возможностей обхода

действующих средств защиты. Не менее опасна анархия в плане несанкционированного изменения кода приложений, конфигураций систем или прав доступа к защищаемым информационным объектам. Задача процесса управления конфигурациями — контроль и учет всех произведенных изменений и модификаций. Тщательный аудит позволит в случае необходимости легко восстановить одно из предыдущих рабочих состояний информационной системы. Разумеется, должен поддерживаться банк эталонного программного обеспечения, хранящий работоспособные версии всех компонентов программного обеспечения. Восстановить утраченные или испорченные данные позволят строго исполняемые регламенты резервного копирования. Место для хранения копий должно тщательно выбираться с учетом технических характеристик используемых носителей информации и требований по обеспечению конфиденциальности данных. С определенной периодичностью следует проверять техническое состояние бэкапов.

Управление носителями информации следует рассматривать как отдельный процесс, строго регламентированный в соответствии с политикой безопасности и обеспечивающий все три аспекта информационной безопасности в отношении хранимых данных. Средства защиты должны не только пресекать попытки получения несанкционированного доступа, но и свести к минимуму вредное воздействие окружающей среды.

Центральным звеном системы информационной безопасности, затрагивающим все ее составляющие, является процесс документирования. Актуальность документации (от политики безопасности и журналов учета до инструкций пользователей) непосредственно влияет на общее состояние защиты. Хранение документов является самостоятельной задачей, зачастую с противоречивыми требованиями в отношении обеспечения конфиденциальности, целостности и доступности.

В жизненном цикле информационных систем имеется несколько критичных в плане обеспечения безопасности периодов. Один из них —

регламентные работы, во время которых отдельные специалисты (зачастую еще и не состоящие в штате компании) получают исключительные права доступа. Контролировать их действия становится крайне затруднительно.

Как бы хорошо ни была выстроена система безопасности, необходимо заранее и тщательно спланировать комплекс мер реагирования на случаи нарушения политики безопасности. Этот список должен включать действия по обнаружению и нейтрализации совершенных атак. Вполне вероятно, что полностью ликвидировать последствия прорыва системы безопасности не удастся. Поэтому выделим следующие, вполне реальные задачи процесса реагирования на нарушения режима безопасности: локализация атаки; максимально возможное уменьшение наносимого вреда (обычно этому благоприятствуют скорость и координация ответной реакции); обнаружение нарушителя (чаще всего это самая сложная задача из списка); коррекция системы зашиты с целью предупреждения повторных атак.

В данном исследовании демонстрируется как на основе процессной модели ITSM можно улучшить отдельные аспекты комплексной системы информационной безопасности. Безусловно, внедрение этой методологии в полном объеме повысит качество системы безопасности в целом и каждого отдельного сервиса защиты в частности. Наличие достаточного числа готовых программно-аппаратных решений от ведущих вендоров (Hewlett Packard, IBM, Microsoft и др.) существенно облегчает эту задачу.

Использованные источники: (ПРИМЕР)

1. Галатенко В. А. Основы информационной безопасности: Курс лекций: учебное пособие / В. А. Галатенко. - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2012. - 205с.

2. Долженко А.И. Управление информационными системами: Учеб. Пособие / А. И. Долженко. - Ростов на/Д.: Ростовский государственный экономический университет «РИНХ», 2009. - 191с.

3. Ингланд Р. Овладевая ITIL. Скептическое руководство для ответственных лиц / Р. Ингланд. - М.: «Livebook», 2011. - 200с.