Практический подход к построению системы управления ИБ

Андрей Голов, руководитель направления ИБ компании TopS BI, CISSP

Владимир Кузнецов, руководитель проектов департамента системной интеграции компании TopS BI

По мере расширения сферы использования информационных систем и их усложнения, проблема обеспечения информационной безопасности (ИБ) обостряется. Безопасность уже невозможно обеспечить одним лишь набором технических средств и поддерживать только силами подразделения безопасности. Отсутствие регулярной оценки информационных рисков, недостаточная информированность сотрудников о правилах работы с защищаемой информацией и соблюдении режима ИБ, отсутствие формализованной классификации информации по степени ее критичности и представлений о том, сколько стоят информационные активы, - все это может свести на нет усилия компании по обеспечению информационной безопасности. С повышением роли информационных систем в поддержке основных бизнес-процессов компании к этим проблемам добавляются вопросы обеспечения непрерывности функционирования бизнеса в критических ситуациях. Игнорирование проблем ИБ, практика «латания дыр» сегодня могут обойтись компании очень дорого. Решить эти вопросы можно путем построения эффективной системы управления информационной безопасностью (СУИБ).

Задачами СУИБ являются систематизация процессов обеспечения ИБ, расстановка приоритетов компании в области ИБ, достижение адекватности системы ИБ существующим рискам, достижение ее «прозрачности». Последнее особенно важно, так как позволяет четко определить, как взаимосвязаны процессы и подсистемы ИБ, кто за них отвечает, какие финансовые и людские ресурсы необходимы для их обеспечения и т.д. Создание СУИБ позволяет также обеспечить эффективное отслеживание изменений, вносимых в систему информационной безопасности, отслеживать процессы выполнения политики безопасности, эффективно управлять системой в критичных ситуациях.

В целом, процесс управления безопасностью (Security Management) отвечает за планирование, исполнение, контроль и техническое обслуживание всей инфраструктуры безопасности. Организация этого процесса усложняется также тем обстоятельством, что обеспечение информационной безопасности компании связано не только с защитой информационных систем и бизнес-процессами, которые поддерживаются этими информационными системами. На предприятии существуют бизнес-процессы, не связанные с ИТ, но попадающие в сферу обеспечения, например, процессы кадровой службы по найму персонала.

Как построить эффективную систему управления ИБ, которая интегрировалась бы в общую систему управления ИТ? Как выделить и описать процессы обеспечения информационной безопасности? Как обеспечить обнаружение инцидентов (нештатных ситуаций) в системе ИБ и как на них реагировать? Как определить, повлияет ли этот инцидент на другие процессы и работоспособность информационных систем и каким будет это влияние? Что предпринять, чтобы в будущем эта ситуация не повторилась?

Сразу оговоримся, что «готовых рецептов» на все случаи жизни пока не существует. В мировой практике есть разработанные модели систем управления ИБ, например, «Information Security Management Maturity Model» (ISM3 от ISECOM) или «The Systems Security Engineering Capability Maturity Model» или стандарт NIST SP800-33. Существует также ряд международных стандартов. Среди них: ISO/IEC 17799:2005 и первый стандарт новой серии ISO/IEC 27001, пришедший на смену английскому стандарту BS7799-2:2002. В отечественной практике первым в этой области стал стандарт Банка России “Обеспечение информационной безопасности организаций банковской системы Российской Федерации”, СТО БР ИББС-1.0-2006, определяющий основные процессы СУИБ для организаций банковской сферы РФ.

Однако прямое использование этих моделей и стандартов ISO/IEC 27001 и ISO/IEC 17799:2005 для построения СМИБ затруднительно. Они либо слишком конкретизированные, а в любой организации, как правило, уже существует определенная система процессов, ролей, организационно-распорядительных документов информационной безопасности, которые необходимо интегрировать в систему управления ИБ. При этом не определяются приоритеты, т.н. «веса директив», которые обычно применяются в стандартах аудита. Либо, напротив, рекомендации носят слишком общий характер. Например, стандарты содержат либо набор контрольных директив, либо общий подход к системам менеджмента, т.е. определяют, что нужно сделать, но не определяют, как это сделать.

Наш подход к построению систем управления ИБ, включая разработку процессов обеспечения ИБ, базируется на следующих методических рекомендациях и директивах:

рекомендации ITIL (Information Technology Infrastructure Library, лучший мировой опыт в области организации работы ИТ-службы), а также модели управления ИТ-ресурсами и ИТ-сервисами Microsoft Operations Framework (MOF);

рекомендации Microsoft service management function (SMF);

стандарт ISO 27001.

Целесообразность использования рекомендаций по управлению ИТ-ресурсами и ИТ-услугами (и в первую очередь процессов управления инцидентами, изменениями) при построении СУИБ обусловлена тем, что процессы обеспечения информационной безопасности неразрывно связаны с процессами защиты, а значит, и управления информационными системами и должны быть тесно интегрированы с процессами управления ИТ.

Библиотека ITIL содержит комплекс необходимых для построения СУИБ рекомендаций.

Во-первых, в ITIL с определенной степенью детализации описан процесс управления безопасностью (Security Management).

Во-вторых, предоставление ИТ-услуг, включая сервисы информационной безопасности, относится к ответственности служб информационных технологий и информационной безопасности. Методы эффективной организации деятельности ИТ-служб обобщены в библиотеке ITIL и многократно апробированы.

Кроме того, компании предъявляют сегодня жесткие требования по качеству ИТ-услуг (в том числе и по информационной безопасности), обеспечивающих поддержку базовых бизнес-процессов. Обеспечение гарантированного качества ИТ-услуг - одна из основных задач процессов ITIL.

Важно, что для организации эффективной системы управления ИБ, аналогично управлению ИТ-услугам, необходима четко действующая система оперативного управления изменениями. В ITIL эти задачи решены путем организации процессов управления изменениями .(Change Management).

В настоящее время библиотека ITIL стала фактически стандартом в области управления ИТ услугами и вобрала в себя лучшие подходы и методики, обобщающие накопленный мировой опыт. На рис 1. представлены процессы эталонной модели ITIL.

Согласно методологии ITIL в обеспечении информационной безопасности участвуют практически все процессы эталонной модели ITIL. Связи процесса управления безопасностью с другими процессами ITIL приведены на рис 2.

Интеграция процесса управления безопасностью в систему процессов управления ИТ-ресурсами и ИТ-услугами и применение сервисно-ресурсного подхода при построении СУИБ (когда обеспечение ИБ рассматривается как сервис с определенным уровнем качества, предоставление которого обеспечивается определенными финансовыми, техническими, людскими ресурсами) дает целый ряд преимуществ. В частности, появляется возможность правильной расстановки приоритетов для решаемых задач ИБ, повышения эффективности расходования ресурсов и средств, выделяемых на управление безопасностью, и как следствие - повышение управляемости системы ИБ в целом.

Процессы эталонной модели ITIL

Рис. 1. Процессы эталонной модели ITIL

Связи процесса управления безопасностью с другими процессами ITIL

Рис. 2. Связи процесса управления безопасностью с другими процессами ITIL

Вместе с тем, одних рекомендаций ITIL для построения полнофункциональной СУИБ недостаточно. Во-первых, необходимо поддержание жизнеспособности СУИБ во времени, обеспечить ее жизненный цикл. Необходимые для этого компоненты и свойства СУИБ («контрольные точки») приведены в используемом нами стандарте ISO 27001.

Во-вторых, в ITIL не содержатся некоторые важные составляющие СУИБ, например, планирование обеспечения непрерывности ведения бизнеса. Кроме того, необходимо более глубокое определение процессов обеспечения ИБ и их взаимосвязей. Например, для обнаружения инцидентов необходимо вести мониторинг подсистем ИБ, который связан с процессом мониторинга ИТ-систем, системами Asset Management и т.д. Для устранения инцидентов необходима организация процесса управления инцидентами. Для поддержания жизнеспособности системы ИБ необходимы регулярные внутренние аудиты системы ИБ, что требует определенного обучения сотрудников и, естественно, определенного финансирования. Важными составляющими обеспечения информационной безопасности являются также процессы управления информационными рисками, информирования сотрудников о политике ИБ, правилах работы с конфиденциальной информацией и пр.

Кроме того, необходимо наложение на модель процессов ролевой модели СУИБ, то есть определение владельцев процессов, ролей сотрудников, которые эксплуатируют подсистемы ИБ и отвечают за соответствующие сегменты системы. Тогда в случае инцидента ИБ, например, нарушения сетевой защиты, можно будет проследить его влияние на другие процессы и подсистемы ИБ, определить ответственных за устранение таких инцидентов, оценить экономические параметры (какой ущерб нанесен, какие средства понадобятся для предотвращения такого рода инцидентов и т.д.). Определенные рекомендации по построению ролевой модели содержатся в документах Microsoft service management function (SMF).

Поэтому при построении СУИБ мы используем приведенные выше рекомендации и стандарты и на их основе строим процессную модель СУИБ компании-заказчика, содержащую три уровня процессов.

Процессы стратегического уровня – управление рисками, управление непрерывностью ведения бизнеса, разработка и развитие политики ИБ верхнего уровня.

Тактические процессы – разработка и развитие процедур ИБ, технической архитектуры системы ИБ, классификация ИТ-ресурсов, мониторинг и управление инцидентами и другие.

Процессы операционного уровня – управление доступом, управление сетевой безопасностью, проверка соответствия и др.

Определяются взаимосвязи процессов. В результате мы получаем трехуровневую процессно-сервисную модель системы управления ИБ, соответствующую требованиям стандарта ISO 27001, на которую накладывается ролевая модель.

Модель СУИБ формализуется в едином комплексе нормативных документов. В этот комплекс входят следующие основные документы.

1. Концепция обеспечения ИБ.

2. Политика информационной безопасности.

3. Положение об информационной безопасности компании.

4. План обеспечения непрерывной работы и восстановления работоспособности информационной системы в кризисных ситуациях.

5. Правила работы с защищаемой информацией.

6. Журнал учета нештатных ситуаций.

7. План защиты информационных систем компании.

8. Положение о правах доступа к информации.

9. Инструкция по внесению изменений в списки пользователей и наделению их полномочиями доступа к информационным ресурсам компании.

10. Инструкция по внесению изменений в состав и конфигурацию технических и программных средств информационных систем.

11. Инструкция по работе сотрудников в сети Интернет.

12. Инструкция по организации парольной защиты.

13. Инструкция по организации антивирусной защиты.

14. Инструкция пользователю информационных систем по соблюдению режима информационной безопасности.

15. Инструкция администратора безопасности сети.

16. Аналитический отчет о проведенной проверке системы информационной безопасности.

17. Требования к процессу разработки программного продукта.

18. Положение о распределении прав доступа пользователей информационных систем.

19. Положение по учету, хранению и использованию носителей ключевой информации.

20. План обеспечения непрерывности ведения бизнеса.

21. Положение по резервному копированию информации.

22. Методика проведения полного анализа и управления рисками, связанными с нарушениями информационной безопасности.

С чего начинать?

Первый шаг в построении процессно-ролевой модели управления системы ИБ – это составление и/или анализ CMDB (configuration management database) - базы элементарных единиц, содержащей активы системы ИБ (ПО, аппаратное обеспечение, сотрудники и процедуры). Как правило, какие-то процессы управления ИТ у компании уже есть. К сожалению, они зачастую недостаточно организованы, не формализованы и плохо соответствуют требованиям ITIL. Поэтому для начала нужно понять, что есть в компании, затем проанализировать ключевые процессы, которые необходимо улучшать. Выбрать один-два процесса, наиболее важных и требующих модернизации. Как правило, большинство компаний начинают с организации службы Help Desk (современное название-это Service Desk) и внедрения процесса управления инцидентами. В некоторых компаниях система Help Desk уже существует и работает, а более актуальным остается вопрос создания процесса управления изменениями. В любом случае, требуется расставить приоритеты внедрения процессов и соотнести их с планами создания СУИБ.

Все услуги (текущие, вновь разработанные и запланированные) должны придерживаться строгих корпоративных стандартов, касающихся безопасности информации.