Как выжить при подготовке к формированию системы менеджмента информационной безопасности (СМИБ)

Евгений Родыгин, Russian Information Security Club (RISC)

Информационная безопасность как составляющая безопасности бизнеса компании должна носить системный характер. Что же понимать под системным характером? Данный термин предполагает, что приоритетом являются не действия, направленные на решение проблем по мере их поступления, а внедрение в компании систем обеспечения информационной безопасности (СОИБ) и менеджмента информационной безопасности (СМИБ).

При этом СОИБ определяет правила безопасного построения и использования информационных систем, обработки данных и применения средств и систем защиты, а СМИБ — конкретные роли сотрудников, ответственных за информационную безопасность в компании, их обязанности и правила взаимодействия.

Если рассматривать среднесрочную перспективу, внедрение СОИБ и СМИБ **всегда** позволяет сократить затраты на ИБ за счет эффективного применения методов и средств защиты информации на направлениях, действительно значимых для безопасности бизнеса.

Читателю может показаться, что настоящая статья посвящена «бумажной» безопасности. «Знаем мы, что такое СМК, — гора стандартов, которые никто практически не выполняет! Это то же самое!» Да, коллеги, я знаю, что такое «мертвые СМК» и что для их выполнения и поддержания в актуальном состоянии нужен штат из десятков человек с функциями, не очевидными для бизнеса.

Я постараюсь дать ряд советов по подготовке к формированию СОИБ и СМИБ без превращения их в болото. И начнем мы с важнейшего этапа — инвентаризации информационных активов компании. Сразу огорчу или обрадую читателя, каким бы красивым и простым ни показалось дальнейшее описание, правильно и красиво по писаному не получится! Ну просто потому, что ни у кого не получалось — никогда!

С суахили на квайгонский

Прежде всего, при построении СОИБ и СМИБ важно понимать, что руководители бизнеса и топ-менеджмент мыслят своими понятиями и

категориями. ИТ оперирует своими категориями, а ИБ — своими. Если этого не понять, можно породить конфликты, способные свести на нет поставленные цели. По сути, вам придется вникать и интерпретировать понятия, цели и задачи бизнеса для обеспечивающих и производственных подразделений. Эта работа требует терпения и дипломатии.

Не спешите немедленно интервьюировать топ-менеджеров, а тем более владельцев бизнеса на предмет целей и задач. Такая попытка приведет к тому, что вы получите общую информацию, делегировать которую на более низкие уровни, обеспечивающие бизнес-процессы, будет весьма затруднительно. К руководителям бизнеса необходимо приходить с подготовленным описанием состояния информационных систем, сценариями нарушения информационной безопасности и вариантами решений. Как подготовить эти сценарии и решения?

Итак, проводим инвентаризацию информационных активов. В некоторых случаях говорят про аудит ИБ, но «инвентаризация» более правильное слово, отражающее смысл. И здесь следует помнить, что собираемые вами данные не будут актуальны всегда! Необходимо озаботиться формой и правилами актуализации этих данных. Не менее важно заинтересовать руководителей ИТ и других участвующих в процессе подразделений тем, что собранные сведения могут помочь и в их деятельности, и состав собираемых данных должен учитывать такое условие.

Тут нужно сделать первое отступление. Дело в том, что любая информационная система представляется многомерной сущностью. В общем случае ИС включает информационную, техническую, организационную, юридическую и административную составляющие. Различные руководители, владельцы бизнес-процессов и сотрудники подразделений видят ИС по-своему, но вам надо свести все уровни представлений и сформировать общую картину с установкой четких границ ИС. Например, с точки зрения ИТ Customer Relationship Management (CRM) — это может быть СУБД, веб-сервер, файловый сервер, пул носителей, комплект системного и прикладного ПО. С точки зрения пользователей — ряд интегрированных веб-сервисов. С точки зрения бизнеса — элементы бизнес-процессов и т. д. С разных точек зрения и в зависимости от способов взаимодействия информационная система — вещь абстрактная, с размытым периметром. И только вы должны собрать этот пазл полностью для оценки ИС как многомерной сущности.

Вернемся к сбору данных. Я рекомендую его начинать не с уровня бизнеса, а с ИТ-подразделения и сформировать данные лучше всего в виде трехуровневых таблиц:

Первый уровень — перечень информационных систем (ИС) с указанием их наименования, владельца, ответственного за функционирование, пользователей, статуса и описания целей применения.

Второй уровень — должен представлять собой декомпозицию для каждой ИС на уровне сервисов и услуг с указанием наименования подсистемы, сервиса/услуги, ответственного, потребителей, числа пользователей, статуса сервиса и описания.

Третий уровень — декомпозиция для каждой ИС на техническом уровне с указанием места, типа, состава аппаратной и программной составляющих на системном и прикладном уровне и т.п .

Добавлю несколько замечаний. Уровень абстракции собираемой информации должен быть достаточным для понимания всеми сторонами, формирования требований к СОИБ, СМИБ, и их интерпретации для оценки рисков владельцами информации и руководителями бизнеса. Указание владельцев, ответственных и потребителей необходимо на уровне ролей/должностей/бизнес-единиц, а не ФИО конкретных специалистов.

Прежде чем приступить к оформлению собираемых данных, вам необходимо договориться (не установить, а именно договориться) с участниками о том, какие объекты инфраструктуры попадут в первый уровень, а какие — во второй и третий. Не всегда удается четко установить разницу между сервисами и информационными системами, поэтому нужно помнить про элемент нечеткости данных.

Почему не рекомендую формировать данные с помощью информационных систем? Потому что процесс итерационный! Вам просто не удастся изначально сформировать модель данных. В процессе сбора данных вы будете вносить уточнения в формы, и особенности вашей инфраструктуры учесть сразу невозможно.

Классификация и классики

Вы уже заметили, что в полученных данных инвентаризации, которые, кстати, могут использоваться не только в интересах ИБ, пока нет ничего про защищаемую информацию. Но в собранных данных есть полный перечень ИС и сервисов, необходимых бизнесу. Теперь надо

перейти к следующей фазе — уточнению и сбору данных о степени использования бизнесом информационных систем и сервисов, а также приступить к сбору и классификации информации, обрабатываемой бизнесом в этих ИС. О системных данных, необходимых для устойчивого функционирования ИС я сделаю отступление ниже.

Из собранных таблиц выделяются отдельные подразделения или бизнес-единицы, у которых необходимо получить сведения о порядке использования информационных систем и сервисов, характеристики данных, обрабатываемых в этих ИС с учетом используемых сервисов. После сбора этих данных следует подготовить перечни обрабатываемой информации и сценарии нарушения целостности, конфиденциальности и доступности этой информации с учетом порядка ее обработки и таких характеристик как ценность информации. Полученные сценарии необходимо согласовать с ИТ подразделением и представить руководству для оценки влияния полученных сценариев на безопасность бизнес-процессов.

Дать совет по оформлению данных, связанных с перечнем обрабатываемой информации отдельными подразделениями и бизнес-единицами, весьма сложно. Тут я вам посоветовать не осмелюсь. У каждого эти данные персонализированы, и не факт, что форма их представления одинакова для различных потребителей информационных систем. Единственное, что важно помнить, — собираемые сведения нужно периодически обновлять, и форма должна это учитывать.

Мы помним, что к топ-менеджменту нужно идти в последнюю очередь. Поэтому начинайте сбор данных с ИТ-подразделения. И тут надо сделать второе отступление и вспомнить К. Маркса.

Например, есть в компании некая информационная система. Эту ИС обслуживает подразделение ИТ или отдел бизнес-систем (ОБС), и у этой ИС есть потребители — бизнес-единицы (БЕ). Вы собираете по БЕ перечни информации, которые они обрабатывают с помощью этой ИС, и рассматриваете с ними сценарии нарушения конфиденциальности, целостности, доступности и чего-то еще с точки зрения БЕ. Все бы хорошо. Но теперь давайте вспомним отца «Капитала» и уясним, что потребителем ИС является и тот, кто ее обслуживает! Потому что эта ИС для них — орудие труда! Которое должно быть в порядке!

Получается, что отдел БС также является потребителем ИС, но риски для них специфичные и в большей части связаны с обеспечением устойчивости, а не конфиденциальности. Рассматриваемая информационная система, опять же, функционирует не на пустом месте.

Если на прикладном уровне ее обслуживает отдел БС, то на системном уровне, пожалуй, отдел ИТ! И, по сути, отдел БС — это потребитель услуг уже отдела ИТ в части сервисов для построения ИС. Но, опять же, отдел ИТ — потребитель своих же ИС на системном уровне, и это их орудия труда! И отдел ИТ так же оценивает риски со своей спецификой. Например, качество электроэнергии, сроки лицензий системного ПО, выход из строя аппаратной части и т.п.

Конфиденциальность не в чести

Закончив формирование сценариев нарушения ИБ и сбор оценок рисков у ИТ и топ-менеджеров в такой многоуровневой модели, вы получите 2–3 уровня рисков связных систем, которые после систематизации выдают более полную картину для обработки рисков в целом по компании. В данном случае мы не рассматриваем отношения с внешним миром (партнеры, подрядчики и т. д.). Нужно отметить, что многие ответы на вопрос «что и как защищать?» станут очевидны.

Теперь обратимся к рискам. Может быть, для кого-то это станет открытием, но на сегодняшний день для большинства компаний обеспечение конфиденциальности информации не является приоритетной задачей информационной безопасности! Конфиденциальность необходимо поддерживать для узкого круга тендерной, финансовой, договорной информации и того, что составляет проценты от общего числа защищаемой информации. Также оказывается, что уничтожение или потеря доступности информации производственного характера существенно критичнее, чем утечка ее самой. Это связано в первую очередь с тем, что злоумышленник не может легко монетизировать такую информацию!

Не стоит увлекаться методами их оценки. В ряду качественных и количественных оценок существует множество методов и средств. Однако, уверяю вас, что два-три опытных эксперта выдают в результате оценки рисков вполне хорошие результаты. А вот для оценки эффективности мер – рекомендую применять автоматизированные средства, которых на рынке вполне достаточно.

Таким образом, нарушение устойчивого функционирования информационных систем может нанести больший ущерб, чем утечки или нарушение конфиденциальности для большей части информации, обрабатываемой в ИС компании! (*Одно из правил, с которым приходится сталкиваться начинающим специалистам звучит так: Тебя учили*

обеспечивать конфиденциальность информации, а придется обеспечивать устойчивость используемых информационных систем.)

В подобных условиях очевидными и первоочередными становятся задачи по локализации отдельных информационных систем, обрабатывающих информацию, требующую защищать ее конфиденциальность, и защита периметра ИС компании. Что в свою очередь определяет вектор усилий, выбор базовых средств и систем защиты. При выборе средств и систем защиты приоритет нужно отдавать Enterprise-, а не Endpoint-решениям.

Списывать нужно с умом

Вернемся к построению СОИБ и СМИБ. При их формировании рекомендую воспользоваться лучшими практиками, но не слепо. К лучшим практикам относятся ISO 27001, СТО БР и другие стандарты. Но чтобы не утонуть и не обременять себя выполнением всех положений, которые могут вас не касаться, возьмите последние версии стандартов и адаптируйте их под нужды вашей компании. Просто возьмите стандарт и смело перепишите, вырезая лишнее и уточняя особенности вашей компании. Вовсе не нужно смотреть на стандарты как на иконы!

В результате у вас получится документ, содержащий базу для формирования трех высокоуровневых документов: политики ИБ компании, требований к СОИБ и требований к СМИБ.

В общем, структура документов СОИБ и СМИБ включает четыре уровня.

1. Документы, определяющие корпоративную политику ИБ.
2. Документы, формирующие частные политики ИБ.
3. Документы, формирующие процедуры и правила по реализации частных политик.
4. Документы, содержащие свидетельства выполненной деятельности в части ИБ.

Как формировать базовые документы и внедрить их я постараюсь рассказать в следующий раз.