УДК 004.056

А.А. Пономарёв

РЕШЕНИЕ ЗАДАЧИ ВЫДЕЛЕНИЯ И ЗАЩИТЫ ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ С ИСПОЛЬЗОВАНИЕМ ПРОЦЕССНОГО ПОДХОДА

Решается задача защиты информации на предприятии исходя из его бизнес-процессов. Выявляются достоинства процессного подхода к формализации деятельности на предприятии с точки зрения защиты информации. Для целей бизнес-моделирования применён стандарт IDEF0, на основе которого разработана модель внедрения режима коммерческой тайны на предприятии.

Ключевые слова: защита информации, бизнес-моделирование, IDEF0 (Р 50.1.028-2001), модель внедрения режима коммерческой тайны на предприятии.

Введение

Одной из самых важных целей при подготовке проекта системы защиты информации является четкая и правильно понимаемая постановка задачи. Для достижения этой цели необходимо исследовать все происходящие финансово-хозяйственные процессы и соответствующие им потоки информации на предприятии, выявить те из них, которые должны быть защищены в первую очередь. Для построения эффективной системы защиты информации недостаточно знать организационно-штатную структуру организации. Дело в том, что кроме собственно организационно-штатной структуры важнейшее значение имеет система взаимодействия между ее элементами. Такая система взаимодействия имеет пять основных аспектов: административный; финансовый; материальный (товарный); информационный; коммуникационный.

Существование любого предприятия связано с выполнением бизнес-процессов. Бизнес-процесс – структурированный набор действий, охватывающий различные сущности предприятия и подчиненный определенной цели (ISO/CD 15531-1). Целью любого коммерческого предприятия в конечном итоге является получение прибыли. Прибыль же извлекается из бизнес-процессов, происходящих на предприятии и охватывающих собой всю структурированную деятельность предприятия. По сути, коммерческое предприятие нуждается в защите своих бизнес-процессов. Исходя из этого и должна быть построена система защиты информации на предприятии. Такой подход позволяет более детально расставить приоритеты в защите той или иной информации.

Можно выделить следующие угрозы безопасности информации на предприятии: угроза конфиденциальности, угроза целостности, угроза доступности, угроза достоверности. Исходя из бизнес-процессов предприятия, можно расставить приоритеты угроз по каждому бизнес-процессу. Например, для банка важнейшую угрозу составит угроза целостности, для Интернет-магазина угроза доступности, а для предприятия, занимающегося разработками медицинских препаратов, – угроза конфиденциальности.

Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне» посвящен охране коммерческой тайны в большей степени от угрозы конфиденциальности. Им установлено, какая информация является коммерческой тайной, определено понятие режима коммерческой тайны на предприятии, зафиксированы те первоочередные мероприятия, которые следует произвести собственнику информационных ресурсов, дабы информация приобрела статус коммерческой тайны, а также какие мероприятия должны быть организованы на предприятии, чтобы считался введенным режим коммерческой тайны. Но в законе не сказано, каким образом должны быть выполнены те или иные пункты по установлению этого режима. Выполнение всех требований закона выливается в целую цепочку организационных мероприятий. Перечень таких мероприятий можно найти в работе [3]. При этом одним из наиболее сложных процессов является разработка перечня сведений, составляющих коммерческую тайну предприятия, и структурирование каждого пункта перечня до конкретного носителя – составление реестра документов и носителей, составляющих КТ предприятия. Причём для формирования перечня сведений, составляющих КТ предприятия, обычно предлагается формировать постоянно действующую экспертную комиссию (ПДЭК). В ПДЭК входят руководители функциональных подразделений предприятия, руководит комиссией либо директор предприятия, либо его заместитель. Но сегодня современные предприятия отказываются от функционального подхода к организации труда в связи с появлением более эффективных её форм.

Функциональный подход основан на использовании разделения труда по выполняемым функциям и иерархическом представлении структуры предприятия. Организация и управление деятельностью осуществляется по структурным элементам (отдел, департамент, цех), взаимодействие которых осуществляется вертикально – через должностных лиц. Недостатками функционального подхода являются: фрагментарность (на уровне структурных подразделений); дублирование ответственности и отсутствие контроля над результатом; отсутствие ориентации отдельных видов функций на результаты деятельности предприятия. Так и при формировании перечня сведений не исключено, что отдельные члены экспертной комиссии, во-первых, преувеличат значимость информации, обрабатываемой в их подразделении, во-вторых, решат, что информацию защищать не следует, в-третьих, что это не относится к их компетенции.

Процессный подход позволяет преодолеть недостатки функционального подхода, поскольку учитываются сквозное управление процессами и методы их внутренней организации, взаимосвязи процессов (в частности, информационных потоков), которые определяются технологическими особенностями. Процессный подход –это представление о бизнес-процессе как последовательности операций, реализуемых во времени в соответствии с определенной технологией для извлечения прибыли (получение какого-то результата).

Описание бизнес-процессов предприятия

Деятельность по выявлению и описанию существующих бизнес-процессов (анализ бизнес-процессов), а также проектированию новых (проектирование бизнес-процессов) называется бизнес-моделированием.

Существует множество нотаций для описания бизнес-процессов. Самыми авторитетными стали нотации IDEF, которые были приняты как стандарты, в частности, в России. Стандарт [2] предназначен для использования при анализе и синтезе производственно-технических и организационно-экономических систем методами функционального моделирования. Рекомендации содержат описание комплекса средств для наглядного представления широкого спектра деловых, производственных и других процессов и операций предприятия на любом уровне детализации, а также организационные и методические приемы применения этих средств. На основе данных стандартов выпущено множество программных продуктов, позволяющих представить деятельность организации с помощью бизнес-процессов.

Концепция IDEF0

Методология IDEF0 основана на следующих концептуальных положениях [1]:

1. Модель – искусственный объект, представляющий собой отображение (образ) системы и её компонентов. Считается, что M моделирует A, если M отвечает на вопросы относительно A. Здесь M – модель, A – моделируемый объект (оригинал). Модель разрабатывается для понимания, анализа и принятия решения о реконструкции (реинжиниринге) или замене существующей, либо проектировании новой системы. Система представляет собой совокупность взаимосвязанных и взаимодействующих частей, выполняющих некоторую полезную работу. Частями (элементами) системы могут быть любые комбинации разнообразных сущностей, включающие людей, информацию, программное обеспечение, оборудование, изделия, сырье или энергию (энергоносители). Модель описывает, что происходит в системе, как ею управляют, что она преобразует, какие средства использует для выполнения своих функций и что производит.

2. Блочное моделирование и его графическое представление. Основной концептуальный принцип методологии IDEF – представление любой изучаемой системы в виде набора взаимодействующих и взаимосвязанных блоков, отображающих процессы, операции, действия, происходящие в изучаемой системе. В IDEF все, что происходит в системе и её элементах, принято называть функциями. Каждой функции ставится в соответствие блок. На IDEF0-диаграмме, основном документе при анализе и проектировании систем, блок представляет собой прямоугольник. Интерфейсы, посредством которых блок взаимодействует с другими блоками или с внешними по отношению к моделируемой системе средой, обозначаются стрелками, входящими в блок или выходящими из него. Входящие стрелки показывают, какие условия должны быть одновременно выполнены, чтобы функция, описываемая блоком, осуществилась.

3. Средства IDEF0 облегчают передачу информации от одного участника разрабатываемой модели к другим. К числу средств, облегчающих понимание IDEF0-моделей, относятся:

- диаграммы, основанные на простой графике блоков и стрелок, легко читаемые и понимаемые;
- метки на естественном языке для описания блоков и стрелок, а также глоссарий и сопроводительный текст, уточняющие смысл элементов диаграммы;
-древовидные схемы иерархии диаграмм и блоков, обеспечивающие обозримость модели в целом и входящих в нее деталей, что особенно важно при моделировании больших систем.

4. Строгость и формализм. Разработка модели в IDEF0 требует соблюдения ряда строгих формальных правил, обеспечивающих преимущества методологии в отношении однозначности, точности и целостности сложных многоуровневых моделей.

5. Отделение «организации» от «функций». При разработке моделей обычно придерживаются двух принципов: строят модель, отражающую реальное положение дел на предприятии, – модель «как есть» либо строят идеальную модель бизнес-процесса – модель «как должно быть». Понятно, что, если речь идет о построении модели для конкретного предприятия, начинать следует с построения модели «как есть», а затем оптимизировать модель и в итоге прийти к модели «как должно быть». Процесс перевода предприятия в новую организационную структуру, соответствующую модели «как должно быть», принято называть реинжинирингом бизнес-процессов.

Синтаксис графического языка IDEF0. Набор структурированных компонентов языка, их характеристики и правила, определяющие связи между компонентами, представляют собой синтаксис языка. Компоненты синтаксиса IDEF0 – блоки, стрелки, диаграммы и правила. Блоки представляют функции, определяемые как деятельность, процесс, операция, действие или преобразование. Внутри каждого блока помещается его имя и номер. Стрелки представляют данные или материальные объекты, связанные с функциями, они показывают, какие данные или материальные объекты должны поступить на вход функции для того, чтобы эта функция могла выполняться.

Семантика языка IDEF0. Поскольку IDEF0 есть методология функционального моделирования, имя блока, описывающее функцию, должно быть глаголом или глагольным оборотом. Каждая сторона функционального блока имеет назначение с точки зрения связи блок/стрелки. Стрелка (и), входящая (ие) в левую сторону блока,– вход (ы). Входы преобразуются или расходуются функцией, чтобы создать то, что появится на ее выходе. Стрелка (и), входящая (ие) в блок сверху, – управление (я). Управление определяет условия, необходимые функции, чтобы произвести правильный выход. Стрелка, покидающая блок справа, – выход, то есть данные или материальные объекты, произведенные функцией. Стрелки, входящие в нижнюю сто-

рону блока, представляют механизмы, то есть все то, с помощью чего осуществляется преобразование входов в выходы. Стрелки, выходящие из нижней стороны блока, представляют вызовы. Стрелки вызова обозначают обращение из данной модели или данной части модели к блоку, входящему в состав другой модели или другой части модели. Стандартное расположение стрелок показано на рис. 1.

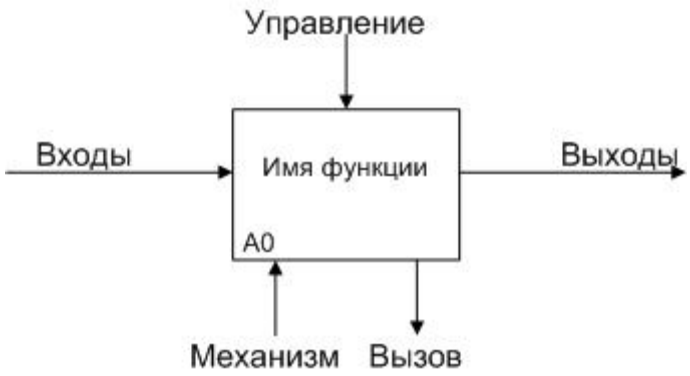

Рис. 1. Семантика языка IDEF0

IDEF0-модель внедрения режима коммерческой тайны на предприятии

Для построения IDEF0-модели рассматриваемого процесса воспользуемся стандартом [2]. Результаты представлены на рис. 2 – 7.

Поясним рисунки, иллюстрирующие IDEF0-модель процесса внедрения коммерческой тайны. На рис. 2 система представлена в общем виде, показаны входы, механизм, управление и выходы системы. Входами системы являются бизнес-процессы организации, так как, рассматривая бизнес-процессы предприятия, можно построить эффективную систему защиты информации. «Механизм», занимающийся внедрением режима КТ на предприятии, – это специалист по защите информации (условное название лица или органа, занимающегося внедрением режима КТ на предприятии), ПДЭК и руководитель организации. Управление – то, чем должен руководствоваться «механизм» при осуществлении своих функций, в нашем случае законом о КТ (указан только основополагающий закон – понятно, что система защиты информации строится на основе принципа законности, то есть ненарушения действующего законодательства). Выходы системы – то, что должно получиться в результате действий «механизма». Показаны только основные документы, чтобы не засорять модель. На рис. 4 показаны этапы формирования перечня конфиденциальной информации. Все документы, формируемые в процессе выполнения данной функции, также могут быть помещены в выходы системы.

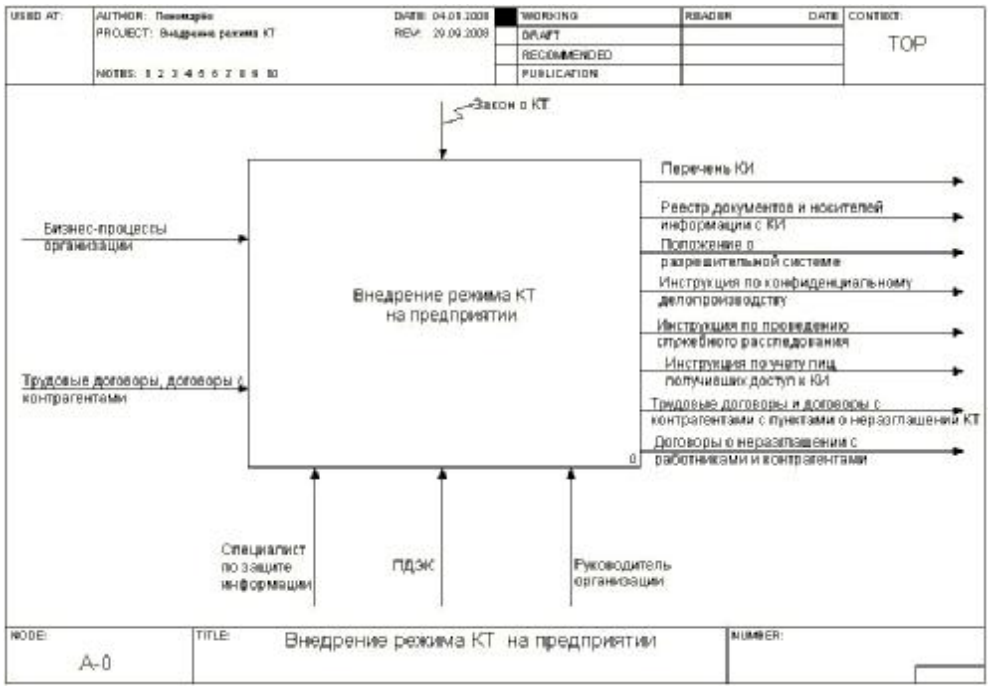

Рис. 2. Общее представление системы

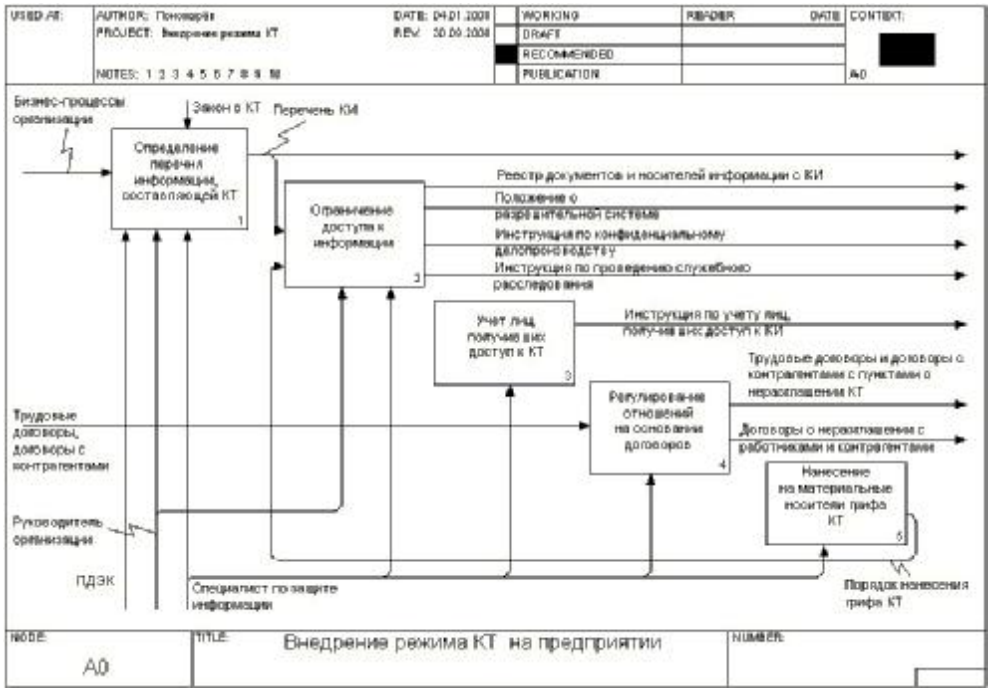

Рис. 3. Декомпозиция системы

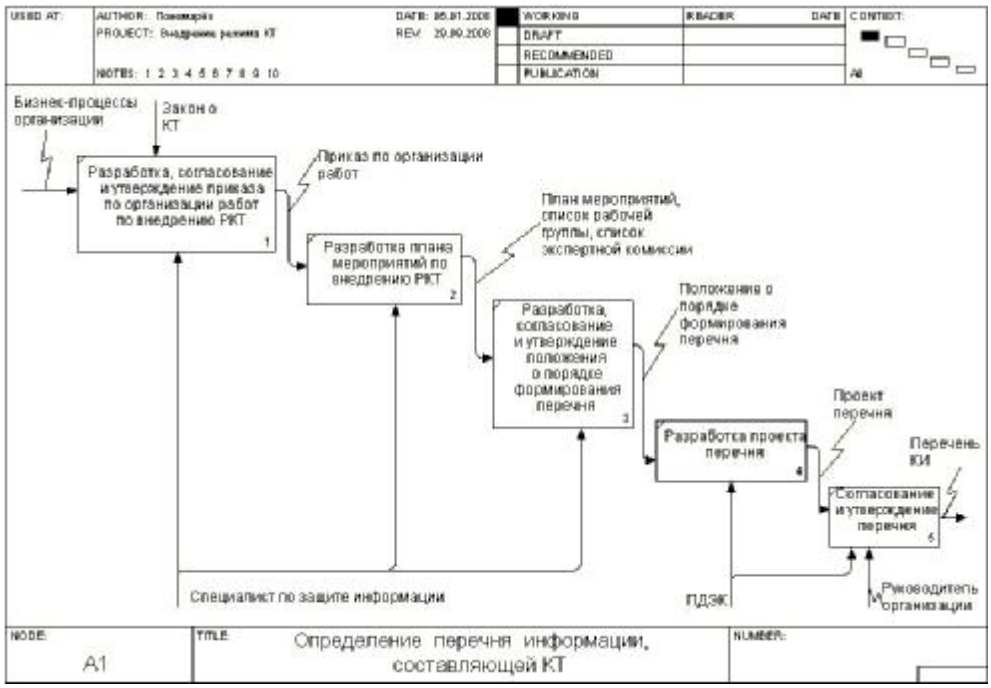

Рис. 4. Декомпозиция функции «Определение перечня информации, составляющей КТ

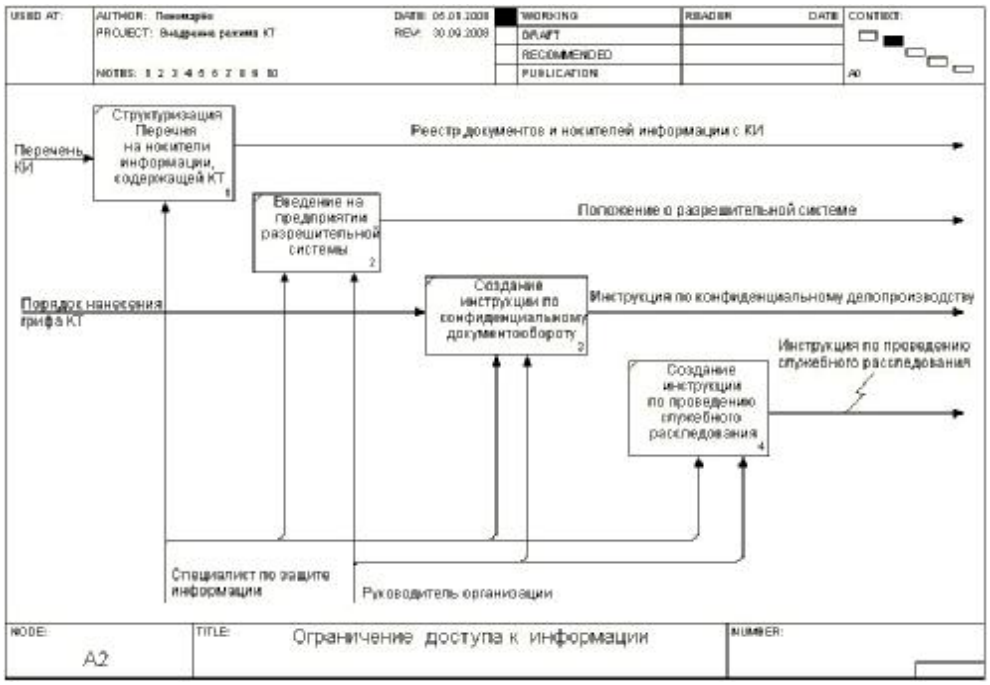

Рис. 5. Декомпозиция функции «Ограничение доступа к информации»

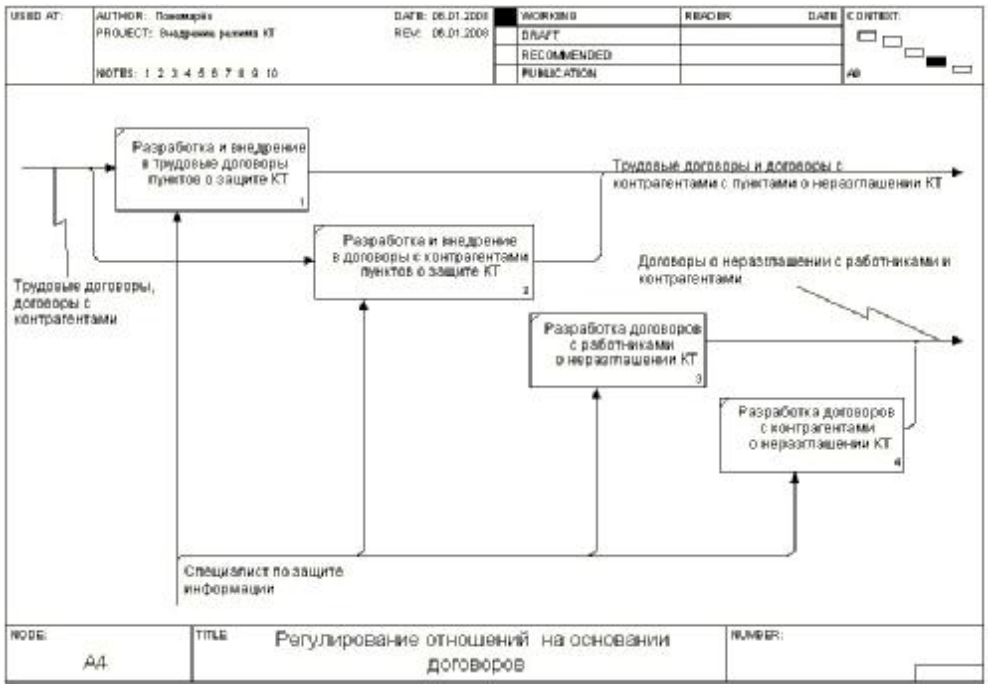

Рис. 6. Декомпозиция функции «Регулирование отношений на основании договоров»

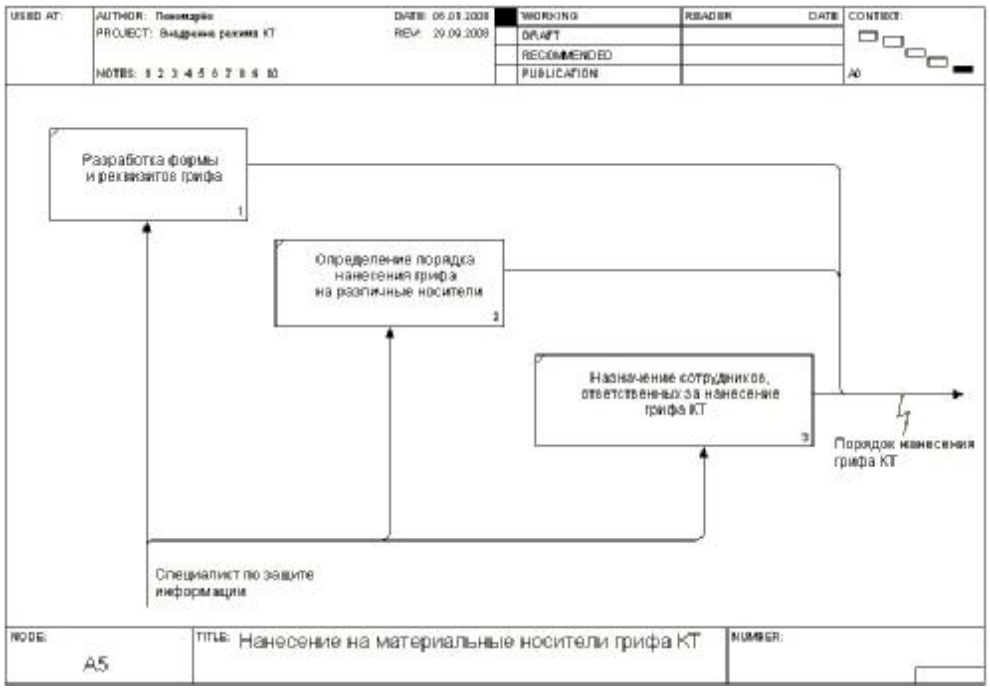

Рис. 7. Декомпозиция функции «Нанесение на материальные носители грифа КТ»

На рис. 3 система, изображенная на рис. 2, подвержена декомпозиции с выделением основных функциональных блоков, которые получены из ст.10 закона о КТ. Далее, на рис. 4-7 декомпозиции подвергается каждый блок, кроме блока А3 – учет лиц, получивших доступ к КТ. Блок А3 включает в себя одну задачу, поэтому в декомпозиции не нуждается.

Важно заметить, что все инструкции, приказы, договоры подписывает руководитель организации и с этого момента они начинают действовать на предприятии.

Заключение

Выявление бизнес-процессов организации является важной задачей для руководства компании, так как позволяет оптимизировать деятельность предприятия, исключив дублирование функций, лишние связи и другие проблемы в организации деятельности. Построение эффективной системы защиты информации, должно начинаться с выявления основных бизнес-процессов организации, так как именно они обычно нуждаются в защите их информационной составляющей.

Было показано, что и деятельность специалиста по защите информации (отдела), тоже может быть формализована в виде IDEF0-модели. Получена модель внедрения закона о КТ на предприятии, который призван защитить информацию в большей части от угрозы конфиденциальности. Однако, как мы отметили выше, угроза конфиденциальности информации является лишь одной из множества угроз информации предприятия. Не следует забывать и о других угрозах, которые могут причинить предприятию не меньший, а в некоторых случаях больший вред, чем угроза конфиденциальности.

В случае реализации угроз бизнес-процесс может прерваться, прекратиться, либо может быть повторён на конкурирующем предприятии. В результате этого предприятие потерпит убытки либо разорится. Например, заражение вирусом компьютера, управляющего производственной линией предприятия, может остановить выпуск продукции и нанести огромный ущерб предприятию. При этом разглашение, каким именно оборудованием и программным обеспечением управляется производство, либо не нанесет вреда предприятию, либо нанесет только косвенный ущерб в случае выполнения других факторов. Тогда понятно, что для построения полноценной СЗИ на предприятии следует изучить, какие бизнес-процессы существуют на предприятии, и исходя из этого построить СЗИ.

Вывод

Стандарт IDEF0 может эффективно применяться как для формализации бизнес-процессов организации, так и для построения систем защиты информации.

* * *

1. Федеральный закон Российской Федерации от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне» // СПС «Гарант».
2. ГОСТ Р 50.1.028-2001 Информационные технологии поддержки жизненного цикла продукции. Методология функционального моделирования. М., 2001.
3. Фадеев Ю.И., Лупачева А.П. Организация защиты информации на предприятии на основе закона о коммерческой тайне // Вестн. Удм. ун-та. Сер. Правоведение. – 2006. – Вып.1

Поступила в редакцию 11.02.08

A.A. Ponomaryov, *postgraduate student*

Solution of the task of highlighting and protection information at an enterprise using the process approach

The task of protecting information at an enterprise is solved based on the business processes at the enterprise. The advantages of the process approach to the activity formalization at the enterprise are pointed out in terms of information protection. The IDEFO standard is applied for the purposes of business modeling. A model of introducing the commercial secret regime at the enterprise has been developed on the basis of this standard.

Пономарёв Артемий Александрович, аспирант
ГОУВПО «Удмуртский государственный университет»
426034, Россия, г. Ижевск,
ул. Университетская, 1 (корп. 4)