2008 Математические основы компьютерной безопасности № 2(2)
DOI 10.17223/20710410/2/20
УДК 004.056.52

УПРАВЛЕНИЕ ПРОЦЕССОМ ПРЕДОСТАВЛЕНИЯ ПРАВ ДОСТУПА НА ОСНОВЕ АНАЛИЗА БИЗНЕС-ПРОЦЕССОВ

Т.М. Пестунова, З.В. Родионова

Новосибирский государственный университет экономики и управления

E-mail: ptm@nsaem.ru, rodionova@nsaem.ru

В настоящей статье рассматриваются основные аспекты создания системы предоставления прав доступа пользователям и последующего управления изменениями на основе анализа бизнес-процессов организации.

Ключевые слова: *права доступа*, *бизнес-процесс*, *управление правами доступа*, *владелец процесса*, *eEPC*.

На сегодняшний день управление бизнес-процессами[1] организации – это один из самых распространенных путей значительного улучшения деятельности (сокращение затрат, повышение качества предоставления услуг и т.д.). Однако многие современные организации описывают и оптимизируют бизнес-процессы вне связи с их автоматизацией и защитой информации, в результате чего заложенные в автоматизированную информационную систему (АИС) сценарии зачастую не соответствуют бизнес-процессам и даже могут вступать в противоречие с ними, а система разграничения доступа (СРД) создает необоснованные помехи в работе пользователей.

На практике может возникнуть ситуация, когда бизнес-процессы предприятия организованы не самым оптимальным образом, вследствие чего через какую-то точку в структуре организации проходит информация, которая в данной точке для работы совершенно не нужна. Более того, в такой точке могут пересекаться потоки информации, к которой предъявляются существенно разные требования по защите.

Принимая во внимание, что одной из первых задач, решаемых при создании СРД, является категорирование корпоративной информации и определение прав доступа к ней различных сотрудников организации, очевидно, что АИС должна изначально строиться, исходя из требований проведения такого категорирования, а назначение прав доступа должно соответствовать организации бизнес-процессов предприятия.

На сегодняшний день достаточно распространенной практикой в управлении правами доступа является принятие решения о доступе к ресурсу руководителем подразделения (руководителем процесса) или владельцем процесса. Под владельцем процесса понимается должностное лицо, которое имеет в своем распоряжении персонал, инфраструктуру, среду, ведет мониторинг хода процесса и управление ходом процесса, несет ответственность за результат и эффективность процесса. В некоторых организациях функции руководителя подразделения и владельца процесса могут быть соединены и выполняться одним лицом (матричное конструирование процесса). Такой подход реализован в некоторых автоматизированных системах управления безопасностью: например таких, как «КУБ» (компания «Информзащита») и Identity Management (компания «Инфосистемы Джет»).

Подход на основе руководителя или владельца процесса имеет ряд недостатков, которые в целом связаны с доминированием дискреционного принципа назначения прав в такой модели. Помимо случайных ошибок, которые может допустить руководитель или владелец процесса, принимая решение о доступе, проблемы возникают и тогда, когда объекты используются на пересечении процессов. Два (и более) руководителя или владельца процессов должны принять решение о доступе, что создает почву для возникновения противоречий и дает возможность тому или иному владельцу процесса оказывать воздействие на работу стороннего процесса. Помимо всего прочего, владельцев процесса в организации на порядок больше, чем администраторов информационной безопасности, и, давая им такую власть, руководство увеличивает риск безопасности информации. С другой стороны, передать эти полномочия администратору информационной безопасности также не представляется возможным, так как эта категория сотрудников не обладает достаточными знаниями правил функционирования организации.

Управление процессом разграничения прав доступа на основе анализа бизнес-процессов позволяет практически исключить человеческий фактор и выйти на более формальный уровень принятия решения, основываясь на самой сути деятельности организации, ее бизнес-процессах.

[1] В современной практике управленческой и производственной деятельности для обозначения объектов моделирования принято использовать термин «бизнес-процесс». В МС ИСО 9000:2000 принят термин «процесс». Развитие и распространение двух областей знаний привело к сближению терминов. В дальнейшем термины «процесс» и «бизнес-процесс» будут использоваться как синонимы.

Рассмотрим в общем виде методику построения системы управления правами доступа и последующего управления изменениями на основе ролевой модели с использованием бизнес-процессов. Можно формализовать этапы создания системы управления правами доступа в следующем виде (рис. 1).

Рис. 1. Этапы создания системы управления правами доступа
на основе ролевой модели доступа с использованием бизнес-процессов

Первый этап создания системы управления правами доступа – это описание бизнес-процессов организации. Для проведения указанных работ необходимо определить способ описания. Не существует какого-то одного определенного способа описания, наилучшим образом отображающего деятельность организации, хотя «продвинутые» сотрудники многих организаций постоянно делают попытки его изобрести [1]. Наиболее часто для комплексного описания деятельности организации с целью внедрения автоматизированной системы используются следующие типы моделей:

- модели процессов управления (описание функций процесса, порядок их выполнения и управления, например в IDEF0, IDEF3, EPC);
- модель потока информации (например, в DFD);
- модель данных (например, в IDEF1X1).

Для выбора конкретной модели описания бизнес-процессов необходимо определить требования, предъявляемые к ней со стороны СРД.

Модель бизнес-процесса должна давать ответы на следующие вопросы:

- кто выполняет процедуры процесса (исполнитель);
- в каком из подразделений состоит тот или иной исполнитель;
- какие информационные ресурсы необходимо привлечь для выполнения процесса (например: информация о клиенте, информация о сделке и т.д.);
- какие функциональные модули участвуют в процессе;
- какие процедуры преобразования используются в функциональных модулях (например: копирование, удаление, чтение и т.д.);
- какие существуют связи между ролями и подсистемами.

Можно с уверенностью сказать, что модель данных не может использоваться в предлагаемой ситуации, так как не дает ответы ни на один ранее сформулированный вопрос. Модель потока информации также не рационально использовать, поскольку она не позволяет однозначно определить исполнителя процесса, подразделение, в котором он работает, а также процедуры преобразования. С помощью модели IDEF0 затруднительно вычленять информационные ресурсы, а определить, из какого подразделения исполнитель, вообще невозможно. Таким образом, остается модель eEPC (расширенная цепочка процесса), которая и дает ответы на большинство поставленных вопросов.

Общий вид модели бизнес-процесса в нотации eEPC представлен [2] на рис. 2.

Для прохождения следующих четырех этапов и заключительного построения модели доступа необходимо получить следующие данные из модели: множество пользователей системы, множество ролей пользователей, возможные домены ролей (подмножество объектов системы; например, систему можно разбить на отделы, так что каждый из начальников отделов будет играть роль «начальник» только в домене, соответствующем его отделу), множество информационных ресурсов, множество процедур преобразования, множество аналитических процедур, закрепление процедур за подсистемами.

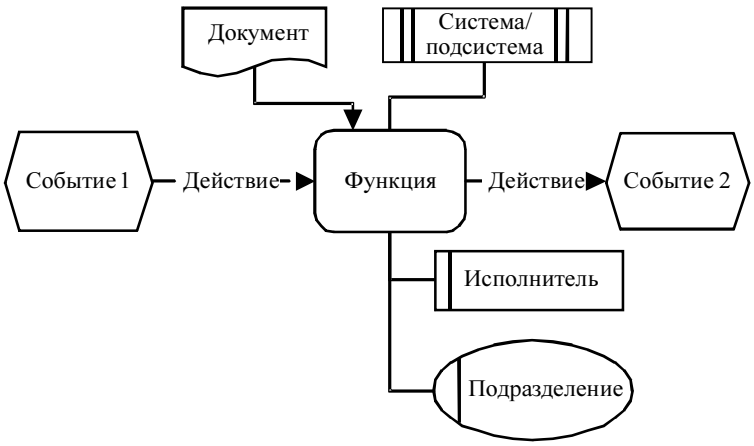

Рис. 2. Общий вид модели в нотации eEPC

Чтение модели позволяет получить следующие данные (табл. 1):

Таблица 1

Чтение модели

Графическое представление	Описание	Значение для СРД
Функция	Служит для описания функций (работ, процедур)	Категория информации, аналитические процедуры, информационные ресурсы
Событие 1	Служит для описания реальных состояний системы, управляющих выполнением функций	–
Действие	Описывает тип отношений между функциями	Процедуры преобразования; закрепление процедур преобразования за подсистемами
Документ	Отражает реальные носители информации, например бумажный документ	Частично категория информации, аналитические процедуры, информационные ресурсы
Система/ подсистема	Отражает прикладную систему	Для выявления принадлежности информационного ресурса к объектам автоматизации
Исполнитель	–	Данные для определения ролей
Подразделение	–	Данные для определения домена ролей

Таким образом, чтение модели eEPC позволяет получить всю необходимую информацию для построения модели управления правами пользователей.

После того, как модель построена и введена в действие, управление правами доступа осуществляется на основе сравнения состояния модели бизнес-процессов до и после внесения каких-либо изменений. Так, например, если создается новое подразделение, то в бизнес-процессе происходят соответствующие изменения, появляется новое подразделение, новые сотрудники, происходит перераспределение обязанностей. На основе анализа нового состояния модели бизнес-процесса в модель доступа добавляются новые роли, изменяются права доступа для уже существующих ролей и т.д.

Рассмотрим действие предложенной методологии на примере процесса «шифрования экзаменационных работ» при проведении вступительных испытаний в вузе. Под шифрованием письменных работ понимается присвоение каждой работе уникального кода, который обеспечивает невозможность идентифицировать автора. Процесс шифрования экзаменационных работ является достаточно значимым и защищаемым процессом вуза, он требует высокого уровня обеспечения безопасности шифрования. Автоматизация этого процесса реализована в АИС «Абитуриент», которая автоматизирует работу по приему документов, проведению вступительных испытаний и зачислению абитуриентов. Никто из участников процесса, кроме ответственного секретаря приемной комиссии, не должен получить информацию о том, кому принадлежит проверяемая работа, в этом выражается беспристрастность и объективность проверки. В общем виде процесс шифрования экзаменационных работ представлен на рис. 3.

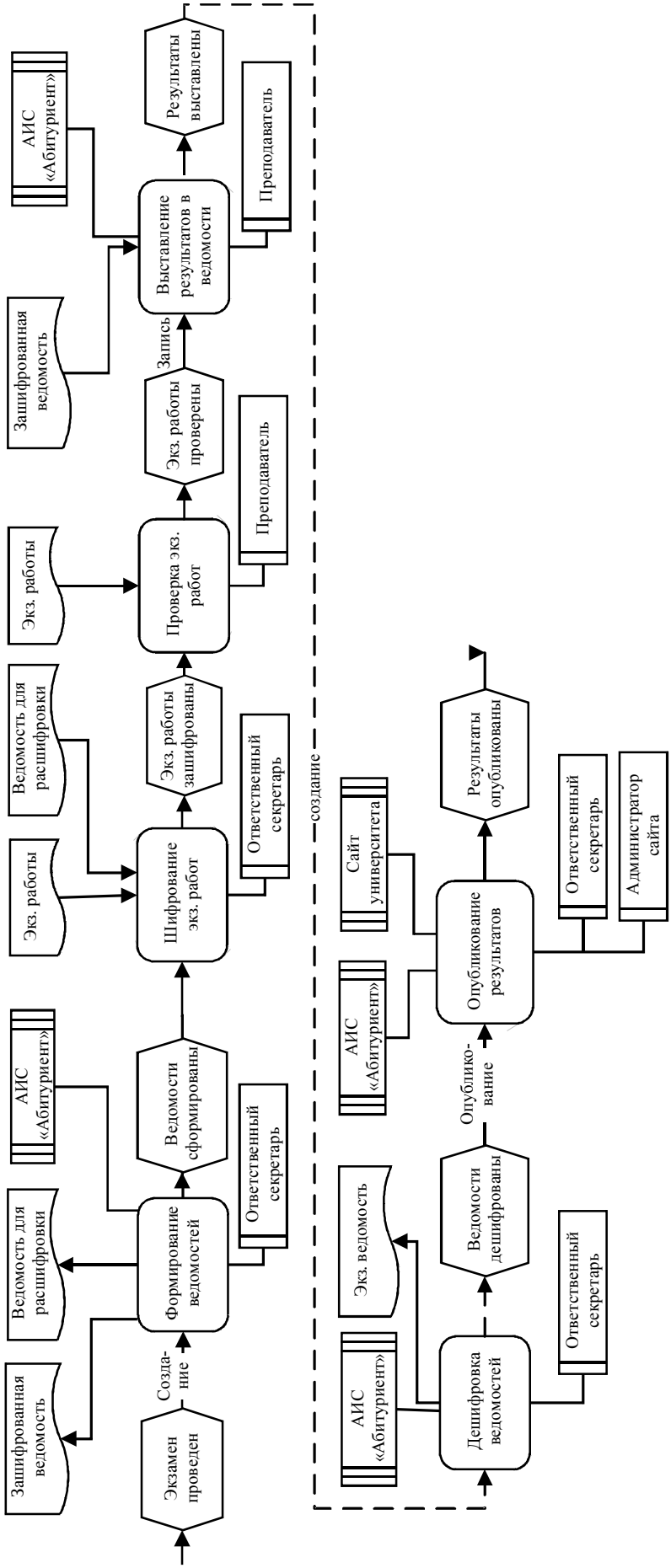

Рис. 3. Процесс шифрования экзаменационных работ при проведении вступительных испытаний в вузе

Второй этап (в соответствии со схемой рис. 1) по категорированию информации проводится на основе бизнес-процесса высшего уровня (формирование контингента вуза). При этом будем считать, что при категорировании вся используемая в рассматриваемом примере информация отнесена к одному классу, а все роли и объекты в примере связаны с функциональным модулем «Абитуриент».

Третий этап связан с выявлением ролей. Будем считать, что в вузе есть только одно подразделение, которое выполняет функции по приему абитуриентов – приемная комиссия, так что о выделении доменов ролей речь не пойдет. В качестве исходных данных для определения ролей можно идентифицировать всех «исполнителей» процесса: ответственный секретарь, преподаватель, администратор сайта. Конечно, не всегда пользователи информационной системы определяются исходя из организационно-штатной структуры, это может происходить и на основе похожести индивидуальных потребностей пользователя, но рассмотрение этого подхода выходит за рамки целей статьи. В указанном примере вполне применим подход выделения ролей исходя из организационно-штатной структуры.

Следующий этап связан с выявлением информационных ресурсов, которые можно выделить из функций (только те функции, которые выполняются с помощью АИС) и документов (учитываются только те бумажные документы, которые изначально формируются в АИС и являются объектами системы): формирование ведомости; результаты экзаменационных работ; зашифрованная ведомость; ведомость для расшифровки; ведомость.

Процедуры преобразования отображаются на диаграмме с помощью объекта «действие»: создание; запись; опубликование.

Все вышеуказанные действия позволяют сформировать простейшую модель доступа (табл. 2):

Таблица 2

Распределение доступа (подсистема «Абитуриент»)

Роль	Процедура преобразования	Информационный ресурс
Ответственный секретарь	Создание	Формирование ведомости
	Запись Опубликование	Результаты экзаменационных работ
	Создание	Зашифрованная ведомость
	Создание	Ведомость для расшифровки
	Создание	Ведомость
Преподаватель	Запись	Результаты экзаменационных работ (зашифрованных)
Администратор сайта	Опубликование	Результаты экзаменационных работ

ЛИТЕРАТУРА

1. *Репин В.В.*, *Елиферов В.Г.* Процессный подход к управлению. Моделирование бизнес-процессов. М.: СИА «Стандарты и качество», 2004. 210 с.
2. *Каменнова М.*, *Громов А.*, *Ферапонтов М.*, *Шматалюк А.* Моделирование бизнеса. Методология ARIS. Практическое руководство. М.: Весть-Метатехнология, 2001. 327 с.