УДК 004.056

Вестник СибГАУ
2014. № 5(57). С. 78–84

МАТРИЦА ДОСТУПА КАК ПАССИВНЫЙ ЭЛЕМЕНТ ЗАЩИТЫ ИНФОРМАЦИОННЫХ РЕСУРСОВ

И. З. Краснов

Сибирский федеральный университет
Российская Федерация, 660041, г. Красноярск, просп. Свободный, 79
E-mail: bk_24@bk.ru

В условиях современного бизнеса роль эффективного управления на основе достоверной информации возрастает многократно. Ошибки менеджмента, основывающиеся на недостаточных или неверно интерпретированных данных, могут привести к краху даже крупные компании. Современная, сложная и динамичная рыночная среда требует от российских предприятий постоянного совершенствования своих систем управления и информационных систем их поддержки. Одним из основных направлений создания эффективной системы управления предприятием является применение процессного подхода к организации и управлению деятельностью. Наиболее мощным инструментом в руках менеджера становится информация. Эффективное управление невозможно без сбора информации и ее обработки различными методами. Методы получения информации многообразны и не являются предметом рассмотрения в данной работе. Гораздо больший интерес вызывают методы целевого распределения информации по адресатам, что и отражено в данной работе.

Рассматривается проблема управления доступом к информационным ресурсам организации. Формулируются цели системы управления доступом. Определяется взаимосвязь целей защиты информации и имеющихся угроз безопасности. Предлагается использовать матрицу доступа как пассивный элемент защиты информационных ресурсов. Формулируются задачи, которые необходимо решать в любой системе управления доступом. Ставится задача исключения избыточности при проведении мер защиты информационных ресурсов. Предлагается методика формирования матрицы доступа. Описывается процедура категорирования информации, выявления групп риска, формирования профилей доступа, закрепления прав доступа в регламентирующих документах организации.

Ключевые слова: матрица доступа, информационные ресурсы, защита информации, процессный подход.

Vestnik SibGAU
2014, No. 5(57), P. 78–84

ACCESS MATRIX AS A PASSIVE ELEMENT IN THE PROTECTION OF INFORMATION RESOURCES

I. Z. Krasnov

Siberian Federal University
79, Svobodnyi Av., Krasnoyarsk, 660041, Russian Federation
E-mail: bk_24@bk.ru

In modern business environment the role of effective governance on the basis of reliable information increases many times is very important. Error management based on insufficient or incorrectly interpreted data, can lead to the collapse of even a large company. Modern, complex and dynamic market environment requires from Russian companies continuous improvement of their management systems and information systems support. One of the main directions of creation of effective system of enterprise management is the application of the process approach to organization and management. Information becomes the most powerful tool in the hands of the manager. Effective management is impossible without information gathering and processing by various methods. The methods of obtaining information are diverse and are not considered in this work. The methods of the targeted distribution of information on the recipients were much more interesting, which is reflected in this work.

In this work the author considers a problem of management of access to information resources of the enterprises. The purposes of a control system of access are formulated. Interrelation of the purposes of information security and available threats of safety is defined. It is suggested to use an access matrix as a passive element of protection of information resources. The tasks which need to be solved in any control system of access are formulates. A task of an exception of redundancy when carrying out measures of protection of information resources is set. A technique of formation of a matrix of access is offered. The procedure of categorization of information, identification of groups of risk, formation of profiles of access, fixing of access rights in regulating documents of the organization is described.

Keywords: matrix of access, information resources, information protection, process approach.

Введение. В современных условиях информатизации общества одним из решающих факторов, определяющих надежное функционирование и устойчивость деятельности организации, является информационная безопасность. Основная деятельность по обеспечению информационной безопасности организации концентрируется на защите информационных ресурсов с точки зрения человеческого ресурса, допущенного к основным активам.

Одним из основных условий формирования системы безопасности организации является четкое определение понятия информационной безопасности (ИБ), в которое входит управление и контроль доступом. Основой является категорирование корпоративной информации и разграничение прав доступа сотрудников организации. Очевидно, что информационная система должна изначально строиться исходя из требований по проведению категорирования и разграничения. Эта информация следует из анализа и «настройки» рабочих процессов. Бизнес-процессы в организации зачастую выстроены не самым оптимальным образом, вследствие чего через точку доступа в структуре организации смешиваются потоки разных уровней конфиденциальности. В результате этой ошибки в ИС возникает уязвимость, значительно снижающая эффективность системы защиты информации или требующая значительного увеличения расходов на безопасность.

Целью обеспечения информационной безопасности в организации является исключение или существенное уменьшение возможности нанесения ущерба субъектам, интересы которых затрагиваются при использовании объекта защиты, материального ущерба, морального или иного случайного или преднамеренного вреда, обеспечение условий соблюдения конфиденциальности коммерческой тайны, персональных данных, а также сохранения устойчивого функционирования ИС [1].

Процессный подход. Построение системы информационной безопасности начинается на уровне организации бизнес-процессов организации [2–4].

Одним из основных направлений создания эффективной системы управления предприятием является применение процессного подхода к организации и управлению деятельностью [5]. В настоящее время на российских предприятиях доминирует применение структурного подхода к организации и управлению финансово-хозяйственной деятельностью. Структурный подход основан на использовании различных типов организационной структуры предприятия, как правило, иерархической. В этом случае организация и управление деятельностью осуществляется по структурным элементам (бюро, отделам, департаментам, цехам и т. п.), а взаимодействие структурных элементов – через должностных лиц (начальников отделов, департаментов и цехов) и структурные подразделения более высокого уровня. Недостатками структурного подхода к организации и управлению деятельностью предприятия являются следующие:

– разбиение технологий выполнения работы на отдельные, как правило, не связанные между собой фрагменты, которые выполняются различными структурными элементами организационной структуры;

– отсутствие цельного описания технологий выполнения работы; в лучшем случае существует только фрагментарная (на уровне структурных элементов), и то не совсем актуальная документируемость технологий;

– отсутствие ответственного за конечный результат и контроль над технологией в целом, а также ориентации на клиента (внешнего или внутреннего);

– отсутствие ориентации на внешнего клиента, а также внутренних потребителей промежуточных результатов деятельности;

– высокие накладные расходы, как правило, непонятно откуда появляющиеся;

– неэффективность информационной поддержки, обусловленная наличием «лоскутной» автоматизации деятельности отдельных структурных элементов и неудачными попытками внедрения корпоративных информационных систем.

Несколько по-иному обстоит дело при процессном подходе. Этот подход ориентирован, в первую очередь, не на организационную структуру предприятия, а на бизнес-процессы, конечными целями выполнения которых является создание продуктов или услуг, представляющих ценность для внешних или внутренних потребителей.

Процессный подход [5; 6] был разработан и применяется с целью создания горизонтальных связей в организациях. Подразделения и сотрудники, задействованные в одном процессе, могут самостоятельно координировать работу в рамках процесса и решать возникающие проблемы без участия вышестоящего руководства. Процессный подход к управлению позволяет более оперативно решать возникающие вопросы и воздействовать на результат.

В отличие от функционального подхода, управление процессами позволяет концентрироваться не на работе каждого из подразделений, а на результатах работы организации в целом. Процессный подход меняет понятие структуры организации. Основным элементом становится процесс. В соответствии с одним из принципов процессного подхода организация состоит не из подразделений, а из процессов.

Процессный подход основывается на нескольких принципах. Внедрение этих принципов позволяет значительно повысить эффективность работы, однако, вместе с тем требует и высокой корпоративной культуры [7; 8]. Переход от функционального управления к процессному требует от сотрудников постоянной совместной работы, несмотря на то, что они могут относиться к различным подразделениям.

Процессный подход предполагает наличие ключевых элементов, без которых он не может быть внедрен в организации. К таким ключевым элементам относятся:

– вход процесса;
– выход процесса;
– ресурсы;
– владелец процесса;
– потребители и поставщики процесса;
– показатели процесса.

Входами процесса являются элементы, претерпевающие изменения в ходе выполнения действий. В качестве входов процессный подход рассматривает материалы, оборудование, документацию, различную информацию, персонал, финансы и пр.

Выходами процесса являются ожидаемые результаты, ради которых предпринимаются действия. Выходом может быть как материальный продукт, так и различного рода услуги или информация.

Ресурсами являются элементы, необходимые для процесса. В отличие от входов, ресурсы не изменяются в процессе. Такими ресурсами процессный подход определяет оборудование, документацию, финансы, персонал, инфраструктуру, среду и пр.

Владелец процесса – процессный подход вводит это понятие как одно из самых главных. У каждого процесса должен быть свой владелец. Владельцем является человек, имеющий в своем распоряжении необходимое количество ресурсов и отвечающий за конечный результат (выход) процесса.

У каждого процесса должны быть *поставщики и потребители*. Поставщики обеспечивают входные элементы процесса, а потребители заинтересованы в получении выходных элементов. У процесса могут быть как внешние, так и внутренние поставщики и потребители. Если у процесса нет поставщиков, то процесс не будет выполнен. Если у процесса нет потребителей, то процесс не востребован.

Показатели процесса необходимы для получения информации о его работе и принятии соответствующих управленческих решений. *Показатели процесса* – это набор количественных или качественных параметров, характеризующих сам процесс и его результат (выход).

В процессе жизнедеятельности бизнес-системы за счет выполнения бизнес-процессов осуществляется достижение определенной совокупности целей. В общем случае она имеет иерархический вид (дерево целей), и каждая цель имеет свой вес и критерий достижимости (количественный или качественный).

В свою очередь, бизнес-процессы реализуют *бизнес-функции* предприятия. Под бизнес-функцией понимают вид деятельности предприятия. Множество бизнес-функций представляет собой иерархическую декомпозицию функциональной деятельности предприятия. Таким образом, дерево функций представляет собой функциональное отражение реализации дерева целей предприятия. Бизнес-функции связаны с показателями деятельности предприятия, из которых также можно построить дерево показателей. Эти показатели затем образуют систему показателей оценки эффективности выполнения бизнес-процессов [9–12]. Как правило, владельцы бизнес-процессов контролируют свои бизнес-процессы с помощью данной системы показателей. Наиболее общими показателями оценки эффективности бизнес-процессов являются:

– количество производимой продукции заданного качества, оплаченное за определенный интервал времени;

– количество потребителей продукции;

– количество типовых операций, которые необходимо выполнить при производстве продукции за определенный интервал времени;

– стоимость издержек производства продукции;

– длительность выполнения типовых операций;

– капиталовложения в производство продукции.

Как правило, основу для классификации бизнес-процессов составляют четыре базовые категории:

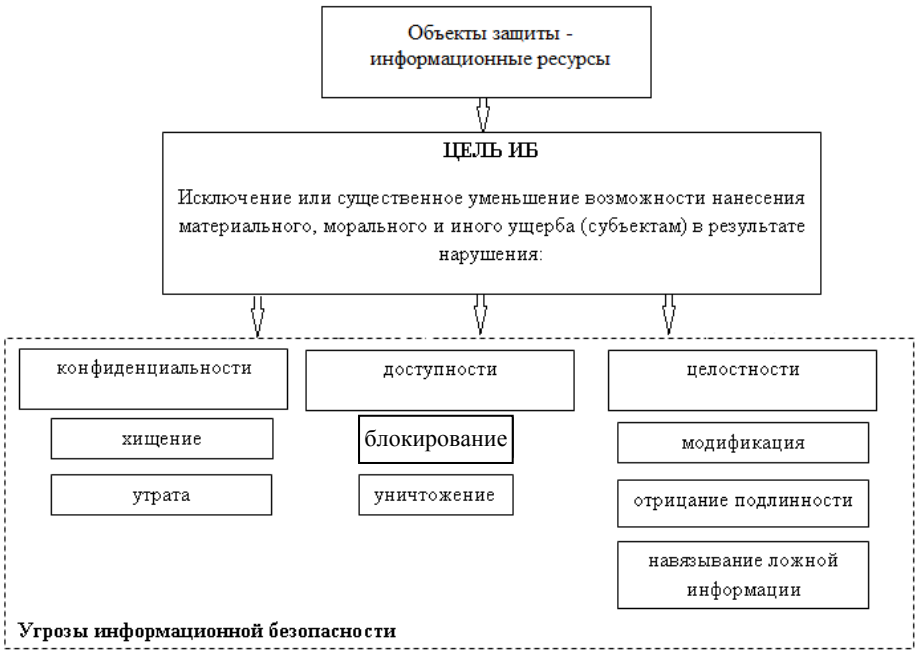
1) основные бизнес-процессы;

2) обеспечивающие бизнес-процессы;

3) бизнес-процессы развития;

4) бизнес-процессы управления.

Управление доступом. Взаимосвязь целей обеспечения информационной безопасности (ИБ) организации и угроз безопасности при разработке, создании, развитии и эксплуатации ИС приведена на рисунке.



Взаимосвязь целей обеспечения ИБ и угроз безопасности

Главной целью любой системы управления доступом к информационным ресурсам является определение таких правил доступа к информации, чтобы каждому субъекту информационной системы соответствовал строго определенный информационный ресурс.

Для этого необходимо решить следующие задачи:

1. Определить критичные ресурсы (содержащие или обрабатывающие конфиденциальную информацию), используемые для выполнения бизнес-процесса организации.

2. Оценить сложившуюся в организации картину в отношении прав доступа пользователей к ресурсам в виде матрицы доступа.

3. Выявить избыточные права пользователей.

4. Построить результирующую матрицу доступа как на уровне бизнес-процессов, так и персонального доступа каждого сотрудника организации (включив ее в элемент политики информационной безопасности).

5. Создать профили доступа для менеджеров, специалистов и руководителей каждого подразделения.

6. Периодически осуществлять проверку пользователей на добросовестное использование вверенных им ресурсов организации (т. е. производить контроль результата, выявление и анализ отклонений, установление причин отклонений).

Для реализации этих этапов необходимо провести обследование (аудит) системы доступа к ресурсам на соответствие требованиям стандарта безопасности [13].

Использование матрицы установления полномочий подразумевает применение матрицы доступа (таблицы полномочий). В указанной матрице (табл. 1) строками являются идентификаторы субъектов, имеющих доступ в информационной системе, а столбцами – объекты (информационные ресурсы). Каждый элемент матрицы может содержать имя и размер предоставляемого ресурса, право доступа (чтение, запись и др.), ссылку на другую информационную структуру, уточняющую права доступа, ссылку на программу, управляющую правами доступа, и др.

Таблица 1

Фрагмент матрицы установления полномочий*

Субъект	Каталог d:\Heap	Программа prty	Принтер
Пользователь 1	cdrw	e	w
Пользователь 2	r		w с 9:00 до 17:00

*c – создание, d – удаление, r – чтение, w – запись, e – выполнение.

Для оценки состояния системы доступа к ресурсам организации проводится внутренний аудит. В границах проведения аудита проводится обследование распределения доступа к информационным и программным ресурсам между сотрудниками организации. Задачами такого обследования является:

– оценка соответствия системы распределения доступа к ресурсам, существующим стандартам в области информационной безопасности;

– анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ресурсов ИС;

– разработка организационно-распорядительных документов по защите информации в установленных границах обследования;

– постановка задач для ИТ-персонала, касающихся обеспечения защиты информации в установленной области;

– участие в обучении пользователей и обслуживающего ИС персонала вопросам обеспечения информационной безопасности;

– итоговая оценка соответствия системы распределения доступа к ресурсам выбранному стандарту в области ИБ после внедрения предложений по повышению ИБ.

Согласно ГОСТ Р ИСО/МЭК 27001 [13], в первую очередь, организация должна определить подход к оценке рисков. В данной работе автор решил ограничиться качественным подходом к оценке рисков, так как численный ущерб от реализации той или иной угрозы и вероятность реализации самой угрозы (количественный подход) должна оценивать специальная экспертная комиссия.

Во-вторых, предприятие должно идентифицировать и оценить риски (табл. 2), что означает необходимость [12–14]:

– идентифицировать активы и владельцев этих активов;

– идентифицировать угрозы этим активам;

– идентифицировать последствия реализации угрозы в результате возможной утраты конфиденциальности, целостности, доступности информации;

– оценить риски;

– определить, являются ли риски приемлемыми или требуют обработки.

Таблица 2

Возможные риски

Угроза ресурсам	Последствия реализации угрозы	Возможный ущерб	Вариант обработки риска
Использование полномочий авторизованного пользователя	Нарушение конфиденциальности и целостности информации	Высокий	Избегаем риск
Несанкционированное чтение, копирование информации	Нарушение конфиденциальности путем прямого получения конфиденциальной информации	Высокий	Избегаем риск
Подключение съемных носителей информации	Утечка конфиденциальной информации, привнесение компьютерных вирусов, вредоносного ПО	Высокий	Избегаем риск

Окончание табл. 2

Угроза ресурсам	Последствия реализации угрозы	Возможный ущерб	Вариант обработки риска
Внедрение дезинформации	Нарушение целостности и доступности баз данных и информационных ресурсов	Высокий	Снижаем риск
Несанкционированное изменение полномочий	Нарушение конфиденциальности и целостности путем превышения полномочий авторизованных пользователей по чтению и изменению информации	Высокий	Снижаем риск
Перехват управления ИС	Нарушение конфиденциальности, целостности и доступности путем уничтожения, модификации информации, перегрузки системных ресурсов, нарушения нормальной работы	Высокий	Снижаем риск

Таблица 3

Категории защищаемой информации организации

№ п/п	Категория	Сокращение	Определение
1	Конфиденциальная информация	КИ	Информация, представляющая ценность для организации, доступ к которой ограничивается на законном основании, а также на основе локальных нормативных актов организации. Виды конфиденциальной информации: персональные данные, служебная тайна, коммерческая тайна полезной модели или промышленного образца
2	Информация для внутреннего использования	ВИ	Вся внутренняя информация, циркулирующая в сети, потеря которой не влечет серьезных последствий для ее деятельности. Информация, которая не может быть отнесена к конфиденциальной на основе законодательства, но доступ к которой должен быть ограничен
3	Общедоступная информация	ОД	Информация, доступ к которой нельзя ограничивать в соответствии с законодательством, и информация, предоставляемая для свободного распространения

Для разграничения прав доступа между подразделениями / сотрудниками, в первую очередь, необходимо изучить их функционал. На основе интервью с руководителями подразделений составляется таблица, состоящая из двух полей:

– отдел–должность;

– функционал.

Описание исследуемых ресурсов. Для разграничения доступа к информации должно проводиться её категорирование (классификация). Цель категорирования состоит в обеспечении уверенности в том, что информация защищена на надлежащем уровне. Категории доступа (уровни конфиденциальности приведены в табл. 3) и связанные с ними меры защиты для корпоративной информации должны учитывать необходимость в коллективном использовании информации или ограничении доступа к ней, а также ущерб для предприятия, связанный с несанкционированным доступом или повреждением информации.

Ответственность за присвоение категории доступа конкретному виду информации, например, документу, файлу данных или носителю, а также за периодическую проверку этой категории возлогается на владельца информации.

Описание активов дает уверенность в том, что обеспечивается их эффективная защита, оно может также потребоваться для целей обеспечения безопасности труда, страхования или решения финансовых вопросов (управление активами). Организация должна идентифицировать свои активы с учетом их относительной ценности и важности. Основываясь на этой информации, можно обеспечивать заданные уровни защиты, соответствующие ценности и важности активов. Каждый актив должен быть четко идентифицирован и классифицирован с точки зрения безопасности а его владельцы должны быть определены. Стандарт Р ИСО/МЭК 27002:2005 «Информационные технологии. Методы обеспечения безопасности. Практические правила управления информационной безопасностью» выделяет следующие виды активов:

– информационные активы;

– активы программного обеспечения;

– физические активы;

– услуги (человеческий капитал).

Инвентаризация заключается в составлении перечня ценных активов организации. Как правило, данный процесс выполняют владельцы активов. Понятие «владелец» определяет лиц или стороны, которые имеют утвержденные руководством обязанности по управлению созданием, разработкой, поддержанием, использованием и защитой активов.

Для создания матрицы по существующим правам доступа проведено исследование с использованием Active Directory, где созданы группы по доступу к конкретным папкам (с указанием права доступа), программам, Интернету, почте. Среди членов этих групп выделены сотрудники организации, и каждому определены свои права доступа в составе отдела.

Уровней доступа к информационному ресурсу может быть два: чтение – только просмотр содержимого ресурса без возможности внесения изменений

и удаления, модификация – возможность редактирования, удаления ресурса.

Следует понимать, что в каждом подразделением кроме руководителя есть сотрудники с разными уровнями доступа. Поэтому такая матрица на самом деле должна представлять собой трехмерный объект, где в глубину раскрываются права конечных пользователей отдела.

На пересечении строки и столбца отражено, имеет ли хоть кто-либо из данного подразделения право на доступ к данному ресурсу:

« » – нет доступа;

«r» – доступ только на чтение;

«m» – модификация.

Из построенных матриц доступа выявляются следующие группы риска:

– группы сотрудников совместно используют ресурс для общих целей;

– многочисленные права доступа к ресурсам всего одного-двух сотрудников, что ставит необходимость такого доступа под вопрос.

Выявляются логические несоответствия функционала подразделений и назначения ресурса. Определяется наличие избыточных прав, повышающее вероятность возникновения каналов утечки по вине сотрудников.

Для построения итоговых матриц доступа проводится работа с руководителями отделов. Являясь владельцами ресурсов, они имеют полное представление о необходимости ресурса сотруднику для выполнения им должностных обязанностей.

Разница между начальными и итоговыми матрицами составляет избыточные права, а именно, оказались ненужными права доступа к ресурсам.

Наличие избыточных прав повышает риск утечки конфиденциальной информации. Профили доступа ставят в соответствие каждой должности минимальный набор прав, который необходим сотруднику для выполнения служебных обязанностей. Профиль доступа приведен в табл. 4.

Достоинства профилей доступа:

– исключается удовлетворение непродуманных запросов прав «впрок», «на всякий случай»;

– увеличивается оперативность рассмотрения заявок на предоставление прав отделом информатизации;

– упрощается процедура согласования прав доступа отделом ИБ;

– оптимизируется задача руководителей отделов приема сотрудника на работу продумывать доступ к ресурсам. В результате сокращается вероятность вынужденных простоев сотрудников и финансовых потерь в ожидании предоставления прав.

Согласно ГОСТ Р ИСО/МЭК 27002:2005 требования по обеспечению контроля в отношении логического доступа необходимо документально оформлять. Главная цель закрепленных в них организационных и технических мер ИБ – не только регламентировать действия пользователей, но и установить ответственность за нарушения правил ИБ.

После утверждения правил разграничения доступа политикой информационной безопасности и закрепления ответственности, внедряются регламенты деятельности в соответствии с условиями, определяемыми матрицей доступа.

Заключение. Разработанная методика управления доступом была внедрена на ряде реальных объектов информатизации региона и позволила снизить риски информационной безопасности.

Таблица 4

Профиль доступа

Ресурс	Право на чтение / модификацию
Главный бухгалтер	
G:\out_buh\Common	m
G:\out_buh\Audit	m
Ресурс	Право на чтение/модификацию
G:\Sap	r
G:\Katalog\dogovora	m
1С Бухгалтерия «Аутсорс-Бухгалтерия»	–
Внешняя почта	–
Зам. ген. директора	
G:\IT\Audit	m
G:\out_buh\Common	m
G:\KT\Buh	m
G:\Sap	r

Библиографические ссылки

1. Обеспечение информационной безопасности бизнеса / В. В. Андрианов [и др.]; под ред. А. П. Курило. М. : Альпина Паблишер, 2011. 392 с.

2. ГОСТ Р ИСО/МЭК 9001:2008. Системы менеджмента качества. Требования. М. : Стандартинформ, 2009.

3. Александров С. Л. Процессы организаций при выполнении требований ГОСТ Р ИСО 9001 // Методы менеджмента качества. 2009. № 1. С. 340.

4. ГОСТ Р ИСО/МЭК 17799:2005. Практические правила управления информационной безопасностью. М. : Стандартинформ, 2006.

5. Менеджмент процессов / пер. с нем. под ред. Й. Беккера, [и др.]. М. : Эксмо, 2007. 384 с.

6. Бизнес-процессы. Инструменты совершенствования / пер. с англ. Б. Андерсен. М. : РИА «Стандарты и качество», 2004. 272 с.

7. Кондратьев В. В., Кузнецов М. Н. Показываем бизнес-процессы (на спирали). М. : Эксмо, 2008. 480 с.

8. Новиков М. В. Моделирование бизнес-процессов управления. [Электронный ресурс] URL: http://www.intalev.ru.

9. Чертовской В. Д., Брусакова И. А. Информационные системы и технологии в экономике. М. : Финансы и статистика, 2007. 364 с.

10. Бизнес-процессы. Инструменты совершенствования / пер. с англ. Б. Андерсен; под ред. Ю. П.Адлер. М.: РИА «Стандарты и качество», 2003. 272 с.

11. Евдокиенко Е. Бизнес-процессы, процессное управление и эффективность [Электронный ресурс] URL: http://www. finansy.ru/publ/mend/009.htm.

12. Балдин К. В. Риск-менеджмент : учеб. пособие. М. : Эксмо, 2006. 368 с.

13. Ковалев А. И. Составные и динамические процессы менеджмента // Стандарты и качество. 2010. № 2. С. 72–73.

14. Астахов А. М. Искусство управления информационными рисками. М. : ДМК Пресс, 2010. 312 с.

15. Репин В. Бизнес-процессы. Моделирование, внедрение, управление. М. : Манн, Иванов и Фербер, 2013. 512 с.

References

1. Andrianov V. V., Marshmallows S. L., Golovanov V. B., Golduev N.A., Kurylo A. P. *Obespechenie informatsionnoy bezopasnosti biznesa* [Providing business information security]. Moscow, Alpina Publisher, 2011, 392 p.

2. *GOST R ISO/MEK 9001:2008. Sistemy menedzhmenta kachestva. Trebovaniya.* [State Standart 9001:2008 Quality management systems – Requirements (IDT)]. Moscow, Standartinform Publ., 2009.

3. Aleksandrov S. L. *Protsessy organizatsiy pri vypolnenii trebovaniy GOST R ISO 9001* [Organizations process in the executions requirements ISO 9001:2008]. *Metody menedzhmenta kachestva*. 2009, no. 1, p. 340 (In Russ.).

4. *GOST R ISO/MEK 17799:2005. Prakticheskie pravila upravleniya informatsionnoy bezopasnost'yu.* [ISO 17999:2005. Code of practice for information security management]. Moscow, Standartinform Publ., 2006.

5. Becker Th. et al. *Menedzhment protsessov Per. s nem*. [Management processes. Per. with German]. Moscow, Eksmo Publ., 2007, p 384.

6. Andersen B. *Biznes-protsessy. Instrumenty sovershenstvo-vaniya Per. s angl.* [The business processes. Tools improvement. Per. from English]. Moscow, RIA “Standarty i kachestvo” Publ., 2004, 272 p.

7. Kondratyev V. V., Kuznetsov M. N. *Pokazyvaem biznes-protsessy (na spirali).* [Show business processes (spiral)]. Moscow, Eksmo Publ., 2008, 480 p.

8. Novikov M. C. *Modelirovanie biznes-protsessov upravleniya.* [Modeling the business process management]. Available at: http://www.intalev.ru.

9. Chertovskoy V. D., Brusakova I. A. *Informatsionnye sistemy i tekhnologii v ekonomike.* [Information systems and technologies in Economics]. Moscow, Finansy i statistika Publ., 2007, p. 364.

10. Andersen B. *The business-processesy. Instrumenty sovershenstvo-vaniya Per. s angl.* [The business processes. Tools improvement. Per. from English]. Moscow, RIA “Standarty i kachestvo” Publ., 2003, 272.

11. Evdokimenko E. *Biznes-protsessy, protsessnoe upravlenie i effektivnost'* [Business processes, process management and efficiency]. Available at: http://www. finansy.ru/publ/mend/009.htm.

12. Baldin K. V. *Risk-menedzhment* [Risk management]. Moscow, Eksmo Publ., 2006, 368 p.

13. Kovalev A. I. [Composite and dynamic processes management]. *Standarty i kachestvo.* 2010, no. 2, p. 72–73 (In Russ.).

14. Astakhov A. M. *Iskusstvo upravleniya informatsionnymi riskami.* [The art of managing information risk]. Moscow, DMK Press Publ., 2010, 312 p.

15. Repin V. *Biznes-protsessy. Modelirovanie, vnedrenie, upravlenie.* [Business Processes. Modeling, implementation, management]. Moscow, Mann, Ivanov and Ferber Publ., 2013, 512 p.