Особенности использования мандатной политики управления доступом в системах микрофинансирования населения

Б.Р. Досмухамедов, С.В. Белов

Введение

Использование мандатной политики управления доступом к различным информационным ресурсам микрофинансовой организации (МФО) в настоящее время является непременным условием обеспечения надежности и безопасности обработки данных, тем самым, обеспечения эффективности работы современных ИТ-технологий. Более того, требование включения мандатного контроля доступом включено во многие стандарты по обработке данных [1]. При реализации режимов удаленного обслуживания клиентов возникают дополнительные проблемы, связанные с тем, что среда передачи (в частности, интернет-сети) имеют свои принципы организации безопасности, которые не согласуются с требованиями мандатной политики. Использование систем электронного документооборота (СЭД) в качестве технологии передачи и обмена данными позволяет внедрить требования мандатного управления, в том числе и при удаленном обмене информацией. По проблеме обеспечения безопасности информации в СЭД применительно к МФО работ найти не удалось. Близкие результаты имеются в работах автора [2, 3]. Различные аспекты обеспечения безопасности информации в различных социально-экономических системах, к числу которых относятся и микрофинансовые организации, рассматриваются в работах [4-10].

1. Анализ процесса движения документов в СЭД

Рассмотрим возможный вариант реализации мандатной политики управления доступом в системах электронного документооборота.

Мандатное управление доступом – это система разграничения доступа субъектов к объектам, основанная на назначении метки конфиденциальности для информации, содержащейся в объектах, и выдаче официальных разрешений (допус-

ка) субъектам на обращение к информации такого уровня конфиденциальности. Основное отличие мандатного управления от классического дискреционного заключается в следующем: при дискреционном управлении объектом контроля являются права доступа субъектов и уровни секретности объектов; при мандатном же управлении объектом контроля являются отдельные элементы информационного потока - транзакты (файлы, пакеты), которые для этого снабжаются уникальными метками. Отметим, что метками могут наделяться любые изолированные ресурсы: технические устройства (компьютер, принтер, флешка и т.д.) и их подсистемы (сетевые карты, процессоры и т.п.), информационные ресурсы (пакеты программ, базы данных, отдельные каталоги, файлы). Контроль на уровне информационных потоков означает, что контролируются не только сами транзакты, но и направления их движения в информационном потоке. Основное требование: не должно происходить движение транзакта от менее приоритетного субъекта/объекта к более приоритетному субъекту/объекту. Для этого при мандатном правлении доступом каждый объект и каждый субъект снабжаются специальными уникальными метками. Между метками устанавливается отношение порядка. Направление движение транзакта определяется характером действий, которые выполняются при его обработке; в частности, при чтении информационный поток движется от объекта к субъекту, а при записи – в обратном направлении. Таким образом, мандатное управление, в отличие от дискреционного, позволяет контролировать процесс обработки также по типу выполняемых действий.

В качестве транзактов в СЭД обычно рассматриваются отдельные документы и даже отдельные элементы и фрагменты документов. Поэтому мандатное управление в СЭД обеспечивает контроль безопасности на уровне отдельных документов и их ключевых элементов, учитывая также характер выполняемых действий над ними.

Одним из возможных решений могло бы быть организация корпоративных или частных сетей. Однако, МФО обычно не имеют достаточных финансовых возможностей для приобретения и, тем более, сопровождения подобных сетей (с

учетом потенциального наличия большого числа оконечных терминалов и относительно невысокой их загруженности). Поэтому целесообразно найти варианты решений, не использующие виртуальных сетей. Проведем анализ возможных вариантов.

Для проведения анализа вначале рассмотрим общую структуру системы СЭД. Общая схема структуры приведена на рис. 1. Отметим, что современные СЭД являются клиент-серверными приложениями.

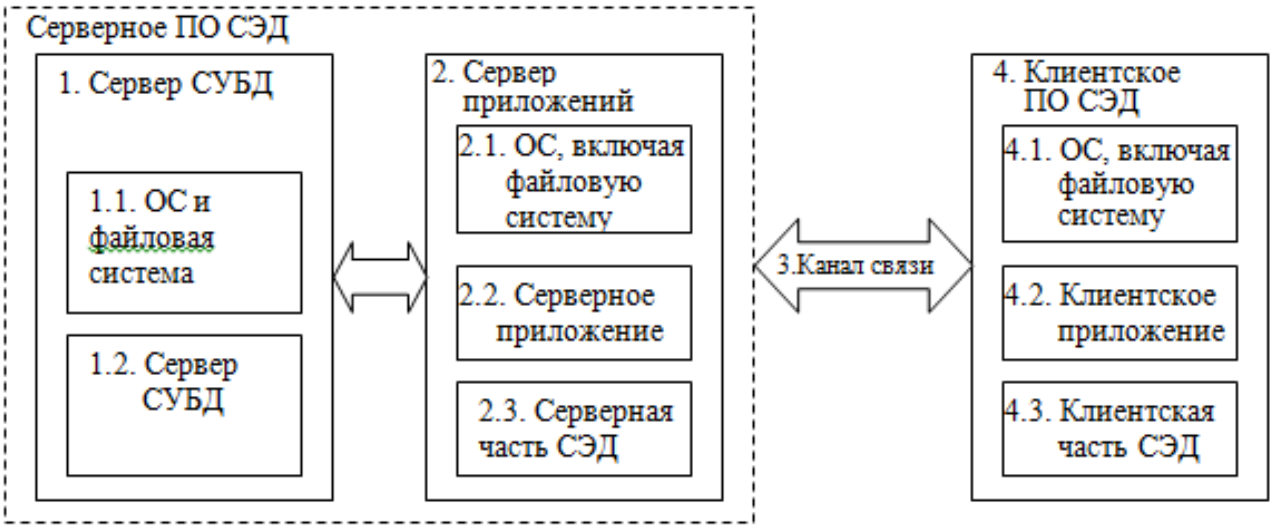

Рис. 1. Общая структура движения данных в СЭД.

Серверы приложений - это программное обеспечение, предназначенное для создания систем с выделенными сервисами бизнес-логики МФО, реализованными, как правило, в виде компонентов. Обычно серверы приложений выполняются под управлением серверных операционных систем. Компоненты, реализующие бизнес-логику распределенного приложения и выполняющиеся под управлением сервера приложений, обычно представляют собой объекты, реализующие транзакционную логику. Помимо собственно хостинга компонентов многие серверы приложений позволяют реализовать приложения, устойчивые к сбоям, а также поддерживают создание кластеров. В настоящее время серверы приложений являются основой многих корпоративных решений, например распределенных приложений, что особенно привлекательно для МФО; в частности, реализующие важные для МФО схемы «предприятие - потребитель» (business-to-consumer) и

«предприятие - предприятие» (business-to-business), такие как виртуальные торговые площадки, позволяющие заключать торговые сделки между предприятиями. Важным достоинством современных серверов приложений является возможность построения кластеров и распределения нагрузки, а также наличие средств восстановления после сбоев. Последнее важно для МФО, поскольку требования к надежности и производительности приложений в микрофинансовой деятельности весьма высоки.

Серверы приложений обычно располагаются между сервером баз данных и Web-сервером либо между сервером СУБД и клиентскими приложениями. Нередко функциональность Web-сервера реализуется в сервере приложений. В схеме рис. 1. и реализована подобная схема.

На современном рынке серверов приложений доминирует стандарт Java 2 Enterprise Edition (J2EE), версия 1.3 которого описывает минимальный набор требований к производительности и возможностям серверов приложений, который и предлагается использовать в схеме рис. 1.

Сервер СУБД выполняет обслуживание и управление базой данных и отвечает за целостность и сохранность данных, а также обеспечивает операции ввода-вывода при доступе клиента к информации. Базы данных (БД) в МФО имеют важное значение, так как вся основная информация о клиентах накаливается и сосредотачивается в них. В МФО целесообразно использование клиент-серверной архитектуры с технологией тонкого клиента, так как часто, в особенности, удаленные клиенты часто не обладают требуемой квалификацией, а компьютеры-клиентов могут не удовлетворять требованиям, необходимым для использования других технологий. Отметим, что имеются севери СУБД, которые совместимы со многими известными серверами приложений; например сервер СУБД Oracle9i Application Server (Oracle9iAS) совместим с сервером приложений J2EE.

Структура системы мандатного контроля доступа в СЭД в МФО

Из приведенной на рис.1 диаграммы следует, что для реализации мандатного управления доступом в СЭД необходимым и достаточным условием является, чтобы мандатная политика управления доступом была адекватно организованна в отношении всех перечисленных на диаграмме рис.1 модулей, и, прежде всего, на уровне файловой системы ОС и СУБД – как в серверном, так и в клиентском ПО СЭД. Что касается клиент-серверного ПО СЭД, то в данном случае достаточно программной совместимости клиент-серверного ПО СЭД с защищенной файловой системой ОС и СУБД. Рассмотрим возможности реализации мандатной политики применительно к каждому из компонентов диаграммы рис.1.

Мандатное управление доступом в ОС реализовано в ряде операционных систем. Изначально принцип мандатной политики доступа был воплощён в ОС с архитектурой Flask (Flux Advanced Security Kernel), которая является архитектура безопасности операционной системы, обеспечивая гибкую поддержку политик безопасности. Прототип архитектуры FLASK был реализован в исследовательской операционной системе Fluke. Некоторые компоненты и интерфейсы Flask были позже портированны из прототипа Fluke в OSKit. Также архитектура Flask была реализована для операционной системы Linux (Security-Enhanced Linux, SELinux) для того, чтобы передать технологию многочисленным сообществам пользователей и разработчиков.

В настоящее время архитектура Flask является основой для технологий реализации систем принудительного контроля доступа, таких как Security-Enhanced Linux (SELinux), OpenSolaris FMAC, TOMOYO Linux, системы безопасности Novell AppArmor и которые включены в стандартные дистрибутивы Linux на ядре 2.6.

Реализация мандатного контроля доступа в ОС основана на контроле пути к файлу. Недостаток такого подхода заключается в ориентации на внешнюю оболочку (имя файла), а не на сущность (содержимое) объекта. Например, если скопировать файл /etc/shadow куда-нибудь в /backup/etc/shadow, то он не перестанет

быть критично важным для безопасности системы, хотя его назначение и использование могут кардинально отличаться от первоначального. Таким образом, вопрос управления информацией возлагается на плечи администратора системы – он должен следить за тем, чтобы права доступа к объектам соответствовали содержимому самих объектов.

Резюмируя вышесказанное, приходим к выводу, что мандатный контроль доступа в современных ОС не реализован в полном объеме.

Для реализации мандатной политики доступа на уровне СУБД можно использовать СУБД Oracle Enterprise Edition с дополнительным модулем подсистемы OLS (Oracle Label Security). Модуль подсистемы OLS представляет собой технологическое решение для организаций, которым необходим низкоуровневый, построчный контроль доступа для защиты конфиденциальной информации. Основанная на многоуровневой технологии безопасности, OLS позволяет сохранять в одной базе данных информацию с разной степенью конфиденциальности; при этом доступ к данным ограничивается категориями допуска. Построчный контроль доступа дополняет безопасность, основанную на правах доступа к объектам, позволяя реализовать низкоуровневую модель привилегий.

OLS предоставляет доступ к строке в таблице базы данных, основываясь на метке, содержащейся в строке, метке, ассоциированной с каждой сессией, и привилегий, присвоенных сессии. Метки служат для классификации данных по уровням безопасности. Так как данные классифицированы по уровням безопасности метками, каждый конкретный пользователь получает ограниченный доступ к данным. Он может оперировать только с данными, находящимися на том уровне секретности, который соответствует его статусу и на уровнях ниже. Любой пользователь может в своем SQL-запросе потребовать выдать все записи из таблицы. СУБД проверит уровень безопасности пользователя и в ответ на запрос возвратит только те строки, которые удовлетворяют условиям, сформулированным в запросе, и соответствуют уровню доступа пользователя. Отсюда следует что на уровне СУБД мандатный контроль доступа реализован в полном объеме.

Во многих современных СЭД также имеются возможности организации мандатного управления доступом к документам. Из наиболее распространенных СЭД, например, в DocsVision 5 используется мандатное управление доступом к документам.

Наиболее слабым звеном с точки зрения обеспечения ИБ на диаграмме рис.1, является канал связи, поскольку данные находятся во внешней по отношению к МФО и неконтролируемой со стороны МФО среде. Теоретически можно создать или арендовать защищенный канал и передавать по нему данные. Однако, применительно к обслуживанию удаленных абонентов со стороны МФО данный подход практически невозможен, поскольку часто удаленные абоненты проживают в таких местах, где нет возможностей (технических, кадровых и др.) по поддержанию защищенного канала. Кроме того, стоимость эксплуатации подобного канала обычно бывает достаточно высока, что может привести к чувствительному удорожанию услуг МФО и, как следствие, значительному уменьшению числа удаленных клиентов. Поэтому необходимо при организации системы безопасного обмена информацией опираться на открытые сети и каналы передачи. Но в открытых каналах невозможно проведение какой-либо политика контроля доступа к данным со стороны МФО, так как канал связи (проводной) находится под контролем другой организации, а беспроводной вообще невозможно контролировать. Следовательно, надо исходить из следующих положений:

1) поскольку невозможно избежать хищения и даже уничтожения данных, то необходимо их преобразовать к виду, непригодному для использования злоумышленником; наиболее типичный способ – шифрование данных. Для противодействия уничтожению данных необходимо организация многоэтапных защищенных протоколов (криптографических протоколов) обмена с подтверждением о получении данных. Достаточно полно описанные вопросы рассмотрены в [68, раздел 4.2];

2) после реализации мероприятий пункта 1) канал связи рассматривать не как логический элемент общей схемы функционирования СЭД в удаленном ре-

жиме, а как технический элемент, не требующий включения его в общую технологию контроля и управления доступом. Как техническое звено канал связи является ненадежным, медленно работающим звеном, так как через этот элемент наиболее вероятно нарушение ИБ, а процесс передачи по каналу обременен целым рядом процедур защиты (аутентификация, шифрование, двустороннее подтверждение). В этом случае канал связи не включается в систему мандатного управления доступом;

3) сформировать систему ответственного отношения владельца канала связи (при его аренде) к вопросам обеспечения защиты данных на основе возможного административного и финансового наказания его.

Таким образом, при организации системы безопасности на основе соблюдения перечисленных трех положений канал связи исключается из схемы рис.2 как элемент системы мандатного управления доступом.

Опишем непосредственно процедуру организации мандатного управления доступом. Напомним, предполагается, что компьютер клиентской стороны удаленного взаимодействия расположен в некотором доверенном месте; например, в одном из следующих пунктов: в здании местной администрации, в почтовом отделении, в местной школе, в отделениях других разветвленных систем, представленных в данном населенном пункте. В пункте размещения этого компьютера должны быть выполнены нормативные требования по безопасности с целью обеспечения возможности аутентификации компьютера. Именно на этом компьютере и должно размещаться клиентское ПО СЭД. Непосредственно за мандатное управление доступом через канал связи отвечает ОС сервера СУБД. Все диалоги и весь документооборот по каналу связи контролируется системой мандатного управления доступом сервера СУБД и СЭД. Важной задачей является разграничение полномочий между тремя системами мандатного управления: ОС, СУБД и СЭД.

Технология передачи данных между серверной и клиентской частями системы может быть представлена следующим образом (см. рис. 2):

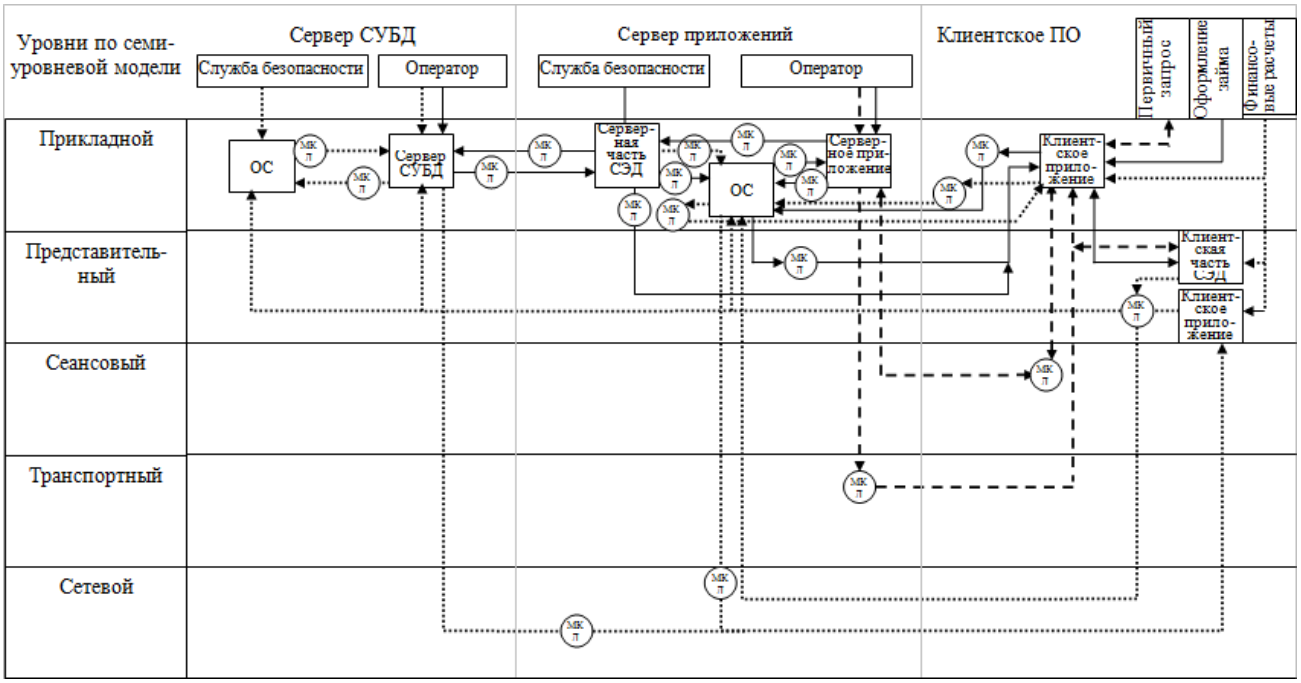

Рис.2. Технологическая схема функционирования системы мандатного управления доступом СЭД МФО

На диаграмме круг с надписью «МКД» указывает на мандатный контроль доступа.

При построении схемы обеспечивалось выполнение следующих требований:

1. Так как каждый из четырех компонентов серверной программной среды системы (ОС, СУБД, Сервер приложений и СЭД), вообще говоря, имеют свою систему мандатного управления доступом, то возникает проблема, какая из систем мандатного управления при взаимодействии компонентов между собой должна контролировать процесс доступа. Предлагается при информационном взаимодействии между этими программными компонентами исходит из следующего принципа: процесс доступа контролируется тем из компонентов, из которого в процессе взаимодействия будет направлен (то есть будет вытекать) информационный поток. Парадигма указанного принципа следующая: кто может больше пострадать от информационного обмена, тот и больше заинтересован в обеспечении его корректного выполнения и поэтому и должен контролировать процесс обмена. Например, если происходит запись документа из СЭД в базу данных, то информационный поток направлен из СЭД в БД; поэтому процесс доступа контролируется системой мандатного управления

СЭД. Если же СЭД обратилась к СУБД с целью получения данных, то процесс передачи этих данных в СЭД контролируется системой мандатного управления СУБД.

2. При взаимодействии серверов с клиентской стороной за контроль доступа отвечает тот из компонентов, который непосредственно при данном сеансе взаимодействует с глобальной сетью. При этом, если системы мандатного контроля доступа у всех компонентов одинаково эффективны, по видимому, целесообразно меньше промежуточных звеньев контроля включать в процесс контроля. Поясним на примере: можно организовать процесс взаимодействия клиентского приложения с СЭД через операционную систему и ее систему контроля доступа, а можно организовать непосредственное взаимодействие СЭД с клиентским приложением. В данном пункте при одинаковой надежности и эффективности обеих систем контроля предлагается обеспечить непосредственное взаимодействие СЭД с клиентским приложением; если же система контроля доступа у ОС более эффективна, то взаимодействие СЭД с клиентским приложением следует организовать через ОС. Отметим, что системы мандатного управления доступом во всех перечисленных выше программных продуктах достаточно эффективны, так что на практике возможно использование схем с непосредственным взаимодействием серверных компонентов с клиентским приложением.

3. Поскольку обычно клиентское приложение основано на технологии «тонкого клиента», то нет необходимости использовать описанные выше технологии взаимодействия серверных компонентов между собой в клиентской части системы. Это означает, что при взаимодействии клиентского приложения с некоторым компонентом серверной части процесс доступа контролируется полностью системой доступа этого компонента.

4. Из процесса взаимодействия клиентской части с серверной части МФО выделены три наиболее важных подпроцесса: а) первичное обращение клиента по вопросу получения микрозайма; б) оформление микрозайма; б) контроль процесса выполнения обязательств по микрозайму. По каждому из этих подпроцессов процедура взаимодействия с серверной частью, а, значит, и процедура контроля доступа различны.

5. Для повышения надежности и безопасности процесса контроля доступа предлагается в зависимости от характера доступа разнести процесса контроля доступа по разным уровням семиуровневой модели МОС по взаимодействию открытых систем. Это связано со следующим соображениями. Во-первых, чем ниже уровень в модели, тем сложнее злоумышленнику добраться до атрибутов доступа, поскольку при переходе от нижнего уровня к следующему верхнему, в соответствии с существующим протоколами взаимодействия, пакет передачи включает как часть содержимого в новый пакет (то есть «одевается» в еще одну оболочку) и поэтому при попытке проникновения к содержимому пакета злоумышленник должен раскрывать все вышестоящие оболочки. С другой стороны, если контролировать доступ толь на самых нижних уровнях, то злоумышленником может быть похищена информация с более верхних (неконтролируемых) уровней, которая может оказаться критичной для данного пакета. Следовательно, уровень защиты следует выбирать исходя из требования: информация, содержащаяся на более верхних уровнях не является критичной для данного пакета. Именно на основе этих соображений и сформированы переходя по уровням на диаграмме. Отметим, что при необходимости мандатная процедура доступа может одновременно использоваться на нескольких уровнях.

Опишем более детально содержание диаграммы.

1. При первичным обращении в МФО по вопросу получения микрозайма взаимодействие связано с получением справочной информации из МФО и передачи первичных данных в МФО; поэтому нет необходимости использования СЭД и СУБД. При этом обращение клиента в МФО контролируется на сеансовом уровне, отвечающем за безопасность непосредственно организации взаимодействия пользователя с системой (контроль фальшивых сайтов, несанкционированное прерывание и вмешательство в процесс взаимодействия). Поскольку на этой стадии пока не передается никаких данных, то контроль доступа на представительском уроне, отвечающем за корректность используемых данных, не критичен. Также не критичен контроль на пользовательском уровне, отвечающем за процесс взаимодействия пользовательских программ, поскольку изначально понятна цель обращения клиента в МФО. Однако, при обратном обращении МФО к клиенту (по вопросам передачи справочных дан-

ных, индивидуальных возможных вариантов и условиях договора и т.п.) важно обеспечить безопасную и надежную доставку этих материалов клиенту, за что отвечает транспортный уровень модели; поэтому целесообразно контролировать процесс доступа на транспортном уровне. Нетрудно провести анализ и убедиться, что возможное хищение данных на более высоких уровнях при этом некритично.

2. При оформлении микрозайма может происходить, во-первых, взаимодействие клиента с оператором МФО с целью уточнения данных, а, во-вторых, по процедуре непосредственного оформления договора – в этом случае взаимодействие происходит с серверной частью СЭД. Оба варианта отображены на схеме. Отметим также, оформленный договор передается в БД для хранения. Уровень контроля доступа выбирается из следующих соображений. Для операций и действий, связанных с уточнением пунктов договора основное общение связано с прикладным уровнем, причем основное общение идет через ОС сервера приложений с участием сервера приложений. При непосредственно оформлении договора необходимо обеспечить, прежде всего, защиту всех данных, содержащихся в договоре; поэтому взаимодействие связано в основном с представительским уровнем, который обеспечивает также выполнение требований юридической доказуемости положений договора и неотказуемости сторон от подписанного договора.

3. При реализации процедур связанных с финансовыми расчетами, наиболее важными показателями являются сохранность всех финансовых данных и правильность доставки всех данных по адресатам. Поэтому наряду с прикладным уровнем, связанным с инициализацией начала процедуры расчета, контроль доступа при непосредственно выполнении расчетов проводится на представительском и транспортном уровнях – на представительском контролируется непосредственно финансовые и иные данные, а на транспортном уровне возможен контроль непосредственно маршрута передачи данных. При этом документ об оплате одновременно передается в ОС сервера приложений и в сервер приложений для контроля, а также в сервер СУБД, откуда клиент получает ответное сообщение о получении и правильности оплаты. Если возникают несоответствия в полученных документах с документами кли-

ента, то проводится более основательная проверка с подключением ОС сервера СУБД (как мера дополнительного контроля).

Заключение

Таким образом, сформирована технологическая схема организации мандатного контроля доступа в процессе функционирования МФО применительно к трем основным процессам микрофинансирования: предварительные контакты с клиентом по вопросам получения микрозайма, непосредственно оформление микрозайма и контроль выполнения обязательств сторон (прежде всего, финансовых) по договору. Приведенная схема опирается на международный стандарт по организации взаимодействия открытых систем.

Литература:

1. Спецификация MoReq2. Типовые требования к управлению электронными официальными документами [Текст] // М.:РОО «Гильдия управляющих документацией», 2008. – 286с.
2. Белов С.В., Досмухамедов Б.Р. Оценка степени привлекательности различных компонентов объекта защиты с целью злоумышленных воздействий. [Текст] // Вестник АГТУ, Серия: Управление, вычислительная техника и информатика, 2013г., №1, -стр.14-20.
3. Досмухамедов Б.Р. Моделирование и подходы к управлению бизнес-процессами в микрофинансовых организациях [Текст] // Вестник АГТУ, Серия: Управление, вычислительная техника и информатика, 2013г., №2, -стр.121-130.
4. Досмухамедов Б.Р., Построение модели управления в удаленном режиме бизнес-процессами в микрофинансовых организациях [Текст] // Прикаспийский журнал, Астраханского Государственного Университета, Серия - Управление и высокие технологии, 2013, № 3 (23), 180–193.
5. Мельников В.В. Безопасность информации в автоматизированных системах. [Текст] // – М.: Финансы и статистика, 2003. – 368с.

6. WebKnacKer Alex. Быстро и легко. Хакинг и антихакинг: защита и нападение [Текст] // Alex WebKnacKer. – М.: Лучшие книги, 2004. – 400 с.
7. Williamson, Graham; Yip, David; Sharni, Ilan; Spaulding, Kent (September 1, 2009). *Identity Management: A Primer*. MC Press. ISBN 978-1-58347-093-0.
8. Pounder, C. N. M. (2008). "Nine principles for assessing whether privacy is protected in a surveillance society". *Identity in the Information Society* December 2008, Volume 1, Issue 1, pp 1-22. doi:10.1007/s12394-008-0002-2.
9. А.Ю. Гуфан, А.Р. Тикиджи-Хамбурьян Стойкая модификация стеганографического метода [Электронный ресурс] // «Инженерный вестник Дона», 2013, №4. – Режим доступа: http://www.ivdon.ru/magazine/archive/n4y2013/1849 (доступ свободный) – Загл. с экрана. – Яз. рус.
10. Чернов А.В., Паращенко И.Г. Классификация моделей надежности программного обеспечения [Электронный ресурс] // «Инженерный вестник Дона», 2012, №4. – Режим доступа: http://www.ivdon.ru/magazine/archive/n4p2y2012/1319 (доступ свободный) – Загл. с экрана. – Яз. рус.