DOI: 10.25728/avtprom.2020.01.06

Управление функциями мобильных приложений в системах управления физическими активами

А.Ю. Молчанов (НПП «СпецТек»)

Информационная система управления физическими активами предприятия получает дополнительные функциональные возможности при наличии в ее составе мобильных устройств и установленных на них приложений. Такие мобильные приложения могут функционировать в условиях наличия прямой связи с другими компонентами информационной системы или в автономном режиме при отсутствии такой связи. При этом необходимо управлять правами пользователей этих приложений на выполнение ими соответствующих функций применительно к различным активам, информация о которых содержится в системе. Представлен обзор базовых правил и особенностей администрирования функций мобильных приложений в системах управления физическими активами.

Ключевые слова: управление физическими активами, EAM, распределенные вычисления, мобильные приложения.

Принципы использования мобильных устройств

При управлении физическими активами предприятий возникает множество задач, требующих решения [1, 2]. Основная цель управления физическими активами заключается в том, чтобы найти оптимальный баланс между производительностью активов, рисками и затратами, связанными с активами [3]. Под физическими активами понимается технологическое оборудование различного назначения, объекты инфраструктуры (транспорт, здания, сооружения, системы связи и др.), а также материальные запасы (материально-технические ресурсы всех видов), контрольно-измерительные приборы и иные объекты организации.

Задача управления физическими активами является комплексной и требует участия всех заинтересованных лиц. Участники управления активами находятся в разных подразделениях (в производственных, ремонтных, финансовых, экономических, кадровых и др.) и на разных уровнях в иерархии управления. При этом многие из них значительную часть времени действуют автономно (в цехах, в удаленных филиалах). Тем не менее, деятельность всех участников управления физическими активами должна быть направлена на достижение единых целей и взаимно согласована.

Согласно ГОСТ Р 55.0.02 необходимым средством поддержки управления активами является информационная система управления физическими активами (ИСУФА) [4]. В силу указанного выше положения участников управления активами, создание и внедрение ИСУФА невозможно без использования технологий организации распределенных вычислений. Распределенные вычисления в такой системе могут быть организованы как в режиме прямой связи (on-line) между компонентами ИС, так и при отсутствии прямой связи между всеми компонентами ИС (off-line). Второй случай предусматривает совмещение возможностей прямой связи и эпизодического обмена данными между разными компонентами ИСУФА. Более подробно различные связанные с этим аспекты рассмотрены в статье [5]. Основу ИСУФА составляет программное обеспечение класса EAM [6].

Существуют различные технологии организации распределенных вычислений, многие из которых так или иначе применяются в ИС [7]. Современные ИСУФА обладают возможностью выполнения части своих функций с помощью мобильных устройств. Любая ИСУФА получает множество дополнительных возможностей и преимуществ, если в ее составе используются мобильные устройства с установленными на них мобильными приложениями.

Мобильное устройство позволяет персоналу выполнять свои функции без существенных ограничений физического перемещения или с минимальными ограничениями. Чаще всего это мобильный телефон (смартфон), реже — планшетный компьютер (планшет). На производстве могут применяться мобильные устройства, защищенные от внешних воздействий, присущих производственному процессу.

Мобильные устройства функционируют не сами по себе, а под управлением программных продуктов, так или иначе обеспечивающих выполнение ими своих функций. Программное обеспечение мобильных устройств, как и любых других вычислительных устройств, можно разделить на две основных группы — системные и прикладные программы [7]. Конечные пользователи ИСУФА, как правило, имеют дело с прикладными программами — мобильными приложениями.

Какие конкретно мобильные приложения будут использоваться в составе ИСУФА, зависит от способа организации распределенных вычислений и обмена данными между компонентами этой системы. Если это распределенные вычисления исключительно в режиме прямого соединения (on-line), то задача мобильных приложений сводится в основном к обеспечению пользовательского интерфейса. В этом случае достаточно имеющегося на любом мобильном устройстве приложения для навигации по сети (браузер).

Если же ИСФА допускает в своем составе компоненты без обязательного прямого соединения с другими компонентами ИС (off-line), и в качестве таких компонентов могут выступать мобильные устройства, то функции мобильного приложения уже не сводятся только к организации взаимодействия с пользователями. В таком варианте мобильное приложение должно также обрабатывать данные и хранить их (по крайней мере, до момента обмена данными

с другими компонентами ИСУФА), то есть мобильное приложение должно выполнять все основные операции из типового стека технологий, используемого для организации распределенных вычислений [5, 7]. Такие функциональные возможности может предоставить только специализированное мобильное приложение из состава ИСУФА, установленное на мобильном устройстве. Поэтому наличие в составе ИСУФА специализированных мобильных приложений является обязательным условием обеспечения возможности автономного функционирования мобильных устройств в составе такой системы.

Современные ИСУФА допускают возможность обоих вариантов использования мобильных устройств: и в режиме прямого соединения с другими компонентами ИС, и в режиме автономного функционирования. Соответственно на мобильных устройствах в составе ИС в зависимости от режима их работы могут использоваться разные типы мобильных приложений. Технические аспекты, связанные с функционированием мобильных приложений, подробно рассмотрены в статье [5].

Базовые принципы администрирования функций мобильных приложений

Использование мобильных устройств и мобильных приложений в составе ИСУФА не может быть полноценно организовано без управления их функциями и данными, которые они обрабатывают, то есть без администрирования. Каждый пользователь мобильного устройства должен выполнять только те функции, которые ему разрешены, и обрабатывать только те данные, которые ему доступны. В целом принципы администрирования мобильных приложений и других программных компонент, входящих в состав ИС, не должны отличаться.

Для получения доступа к функциям мобильного устройства в составе ИСУФА любой пользователь должен пройти аутентификацию (проверку подлинности). После этого мобильное приложение должно выполнить авторизацию пользователя, то есть предоставить ему разрешенные для него функции и данные. Выполнение этих административных функций мобильными приложениями в составе ИСУФА существенно зависит от того, какая функциональность ИСУФА реализована на мобильных устройствах и как эти устройства могут взаимодействовать с другими компонентами системы.

Аутентификация пользователей мобильных приложений чаще всего выполняется, как и для других приложений в составе ИСУФА, путем ввода уникального имени пользователя и его пароля. Поскольку предполагается, что пароль пользователя известен только ему лично, корректный ввод пароля при его адекватной сложности считается достаточным основанием для подтверждения подлинности данного пользователя. Однако современные мобильные устройства часто имеют дополнительные технические средства аутентификации пользователей, основанные на контроле их биометрических параметров (чаще всего это отпечаток пальца, реже — фотография сетчатки глаза и др.). За счет этого мобильное устройство обеспечивает более надежную аутентификацию — даже если пароль станет известен стороннему лицу, контроль биометрических параметров существенно усложнит для него доступ в ИС от чужого имени. Для использования этих возможностей мобильное приложение должно получить от остальных компонентов ИСУФА информацию о биометрических данных пользователей этой системы. Соответственно в этом случае в такой ИСУФА должна быть предусмотрена возможность хранения биометрических данных.

Авторизация пользователя мобильного приложения в составе ИСУФА, как правило, выполняется по тем же правилам, что и в других приложениях. Чаще всего для авторизации используется ролевая модель. Для ее реализации необходимо определить как минимум следующие компоненты.

• Обозначить перечень функций ИСУФА, доступность которых будет регулироваться средствами авторизации. Как правило, каждая функция однозначно определяется уникальным обозначением или числовым кодом, заранее известным всем компонентам, входящим в состав ИС. Коды или обозначения функций чаще всего заранее определяются на этапе разработки ИС и в дальнейшем не изменяются. Кроме функций могут быть также дополнительно идентифицированы сами данные, по отношению к которым выполняются эти функции. Для идентификации данных чаще всего применяются уникальные ключи, соответствующие этим данных в базе данных (БД) ИСУФА.

• Создать механизм управления перечнем доступных ролей. При этом каждая роль характеризуется списком разрешенных для нее функций. Каждая функция в составе роли может быть разрешена безусловно (без дополнительных ограничений и по отношению к любым данным, для которых она применима), либо с заданными условиями, которые могут ограничивать ее применение только по отношению к тем данным, которые соответствуют этим условиям. Перечень ролей может быть фиксированным — тогда он задается в процессе разработки ИСУФА и может изменяться только при ее модификации, либо настраиваемым — тогда он создается и наполняется при внедрении ИСУФА теми ее участниками, кто имеет соответствующие права, и впоследствии может дополняться и изменяться ими в процессе эксплуатации системы. При использовании настраиваемого перечня ролей в составе ИСУФА чаще всего имеется только одна предопределенная роль администратора, а все остальные роли должны создаваться и настраиваться в ходе администрирования ИСУФА.

• Обеспечить возможность назначения ролей из доступного перечня различным участникам ИСУФА — пользователям, группам пользователей и другим субъектам (в качестве которых могут выступать,

например, внешние по отношению к данной ИСУФА приложения). Каждому участнику ИСУФА может быть доступно любое число ролей, из них каждая роль может быть назначена ему без ограничений или с дополнительными условиями (в том числе, например, с ограничениями по времени).

Авторизация пользователя при использовании ролевой модели сводится к проверке доступности ему каждой функции ИСУФА, которая этой моделью регулируется. При выполнении такой проверки функция считается доступной пользователю, если она доступна (при соблюдении всех условий) хотя бы в одной из ролей, которая назначена пользователю в данный момент времени. Если для функций есть ограничения по отношению к данным, над которыми они выполняются, то при авторизации проверяются также и все условия, связанные с обрабатываемыми данными.

Применение ролевой модели для администрирования мобильных приложений практически ничем не отличается от ее использования для других компонентов ИСУФА. В ряде случаев авторизация некоторых функций ИСУФА, характерных для использования мобильных устройств, может выполняться отдельно, тогда им присваиваются индивидуальные обозначения или коды. Но чаще всего при администрировании функциональности ИСУФА применяется общее правило: если какая-либо функция должна быть доступна пользователю, то она может быть выполнена им любым возможным способом как с использованием мобильных приложений, так и без него.

В том случае, когда мобильное приложение функционирует в режиме прямого обмена данными (on-line) и его основные функции сводятся только к организации взаимодействия с пользователем, задача реализации функций аутентификации и авторизации пользователей мобильных приложений ложится на другие компоненты ИСУФА. При выполнении аутентификации пользователя задача мобильного приложения сводится лишь к тому, чтобы получить от него данные аутентификации (имя и пароль либо данные биометрической информации) и передать их серверным компонентам ИС, которые проверят подлинность этих данных. Для исключения фальсификации или перехвата передаваемых по сети данных обычно используется защищенный протокол обмена данными — чаще всего в этой роли выступает широко распространенный протокол HTTPS (HyperText Transfer Protocol Secure — протокол передачи гипертекста с защитой), являющийся расширением HTTP — основного стандартного протокола сети Internet.

При выполнении авторизации пользователя в режиме прямого соединения мобильное приложение для каждой реализованной в нем функции должно запрашивать права пользователя на выполнение этой функции, передавая компонентам ИСУФА, ответственным за авторизацию, внутренний код пользователя, внутренний код или обозначение функции и другие необходимые данные. В ответ мобильное приложение получает информацию о том, может ли эта функция быть выполнена пользователем в данный момент или нет — и в зависимости от полученного ответа предоставляет или не предоставляет пользователю права на ее выполнение.

Если же ИСУФА управления физическими активами допускает возможность автономного функционирования мобильных устройств и установленных на них мобильных приложений в режиме эпизодического обмена данными с другими компонентами ИСУФА (off-line), тогда часть задач, связанных с администрированием функций пользователей мобильных устройств возлагается непосредственно на мобильные приложения. Чаще всего в этом случае подготовка данных, необходимых для выполнения аутентификации и авторизации пользователей мобильных устройств, выполняется вне мобильных приложений иными средствами ИСУФА (как правило, одни и те же инструменты используются для администрирования всех пользователей ИСУФА как использующих мобильные устройства, так и не использующих их). В тот момент, когда мобильное приложение устанавливает связь с другими компонентами ИС и выполняет обмен данными [5], оно получает также и все необходимые административные данные. А использование подготовленных административных данных и само выполнение функций аутентификации и авторизации на их основе может происходить или в момент взаимодействия мобильного приложения с серверной частью ИС, или уже непосредственно в мобильном приложении на мобильном устройстве в зависимости от применяемых в ИС методов администрирования мобильных приложений, которые будут рассмотрены далее.

В принципе, возможно существование ИСУФА, в которых функции администрирования вообще не распространяются на мобильные устройства и установленные на них мобильные приложения. В этом случае считается, что если пользователь такой системы располагает мобильным устройством, на котором установлено мобильное приложение, имеющее возможность автономного функционирования в составе этой ИСУФА, то он может выполнять любые действия в пределах функциональных возможностей данного мобильного приложения. Действия эти могут выполняться над всеми данными, которые так или иначе были переданы на мобильное устройство и которые могут быть модифицированы на нем в процессе автономной работы. При очередном обмене данными все выполненные изменения становятся доступны другим компонентам ИСУФА. Такой подход допустим, пока функциональные возможности мобильных приложений достаточно ограничены. Но с ростом функциональных возможностей мобильных приложений (что характерно для современных ИСУФА) такой принцип их администрирования становится неприемлемым.

Способы администрирования функций мобильных приложений

Простейший способ администрирования мобильных приложений, имеющих возможность функционировать автономно, может быть основан на использовании уникального идентификационного кода, которым снабжено каждое мобильное устройство. В этом случае средства администрирования ИСУФА должны иметь возможность сопоставить учетную запись пользователя с уникальным идентификационным кодом мобильного устройства, которое использует данный пользователь. Тогда во время сеанса связи мобильное приложение передает серверной части ИСУФА уникальный идентификатор мобильного устройства, на основании которого выполняется аутентификация пользователя данного устройства. Схема этого процесса представлена на рис. 1.

В этом случае авторизация пользователя мобильного приложения также будет выполняться на серверной стороне ИС, и он будет получать только те данные и тот набор функций, которые ему доступны.

Такой способ администрирования мобильных приложений достаточно надежен, так как технически сложно подменить или подделать уникальный идентификационный код мобильного устройства, но имеет существенное организационное ограничение: при его применении подразумевается, что каждое мобильное устройство в составе ИСУФА используется индивидуально. Это характерно для мобильных устройств, находящихся в личном пользовании (которые, в принципе, тоже могут применяться для работы персонала в ИСУФА), но в производственных условиях одно и то же мобильное устройство чаще всего может использоваться несколькими участниками производственного процесса.

Поэтому данный способ администрирования мобильных приложений на производстве применить сложно, но он может быть использован как дополнительное ограничение в сочетании с другими методами. Для этого с данными каждого пользователя ИС сопоставляется не один, а несколько уникальных кодов мобильных устройств, определяя тем самым список всех мобильных устройств, с которыми может работать конкретный пользователь. Этот дополнительный контроль только ограничивает возможность подключения к ИСУФА сторонней техники, а проверка подлинности пользователя и определение доступных ему прав осуществляются другими методами.

Более гибкий вариант администрирования мобильных приложений предполагает традиционную схему аутентификации пользователей, когда каждому пользователю соответствует уникальное имя (login), а проверка подлинности имени выполняется путем ввода пароля, известного только данному пользователю. Как уже было сказано выше, для повышения надежности идентификации пользователя можно вместо ввода пароля или дополнительно к нему сверять биометрические параметры пользователя, если у мобильного устройства есть соответствующие технические возможности, а в самой ИСУФА необходимые для этого данные.

В этом варианте возможны две принципиально разных схемы реализации процесса:

1) в момент сеанса связи пользователь вводит данные, необходимые для его аутентификации. Сам процесс аутентификации и последующей авторизации пользователя происходит в серверной части ИСУФА. После этого мобильное приложение получает от ИСУФА только данные, доступные конкретному пользователю, а также информацию о том, какие функции он может выполнять с этими данными. В целом эта схема очень похожа на схему, представленную на рис. 1, но вместо уникального идентификатора устройства мобильное приложение передает в серверную часть ИСУФА данные для аутентификации пользователя;

2) в момент сеанса связи аутентификация и авторизация пользователя не выполняются, но все

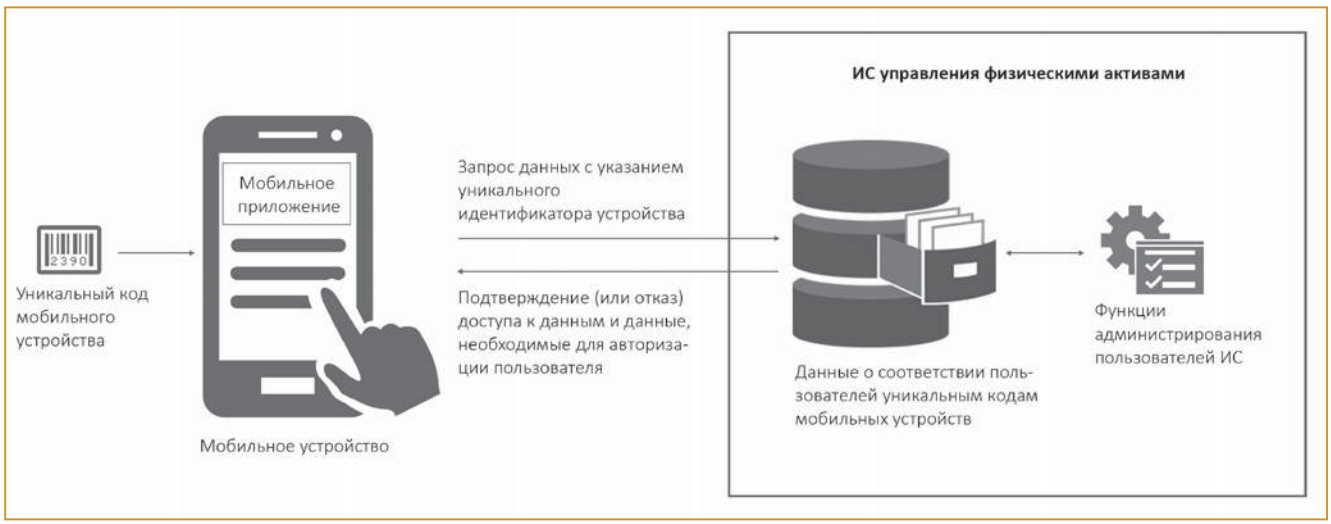

Рис. 1. Администрирование пользователей мобильных приложений с использованием уникальных идентификаторов мобильных устройств

данные, необходимые для этого, передаются из серверной части ИСУФА на мобильное устройство. Аутентификация и авторизация пользователя в этом случае выполняются в тот момент, когда он начинает работу с мобильным приложением.

В первом случае процесс использования мобильных устройств существенно лимитирован. Пользователь мобильного приложения не может быть изменен до следующего сеанса связи. Таким образом, в этом случае мобильное устройство не должно передаваться другому участнику производственного процесса между сеансами связи с серверной частью ИСУФА. В случае необходимости передать мобильное устройство пользователь должен завершить работу с мобильным приложением, а другой участник может начать работу с ним только после обмена данными с серверной частью ИСУФА, пройдя процесс аутентификации и авторизации заново.

Это, конечно, создает некоторые дополнительные неудобства, но они не настолько жесткие, чтобы существенно ограничить возможность использования такой схемы в реальном производственном процессе, как в случае прямой привязки данных пользователей к идентификационным кодам мобильных устройств. Поэтому такая схема администрирования пользователей мобильных приложений может иметь реальное практическое применение.

Используемая во втором случае схема аутентификации пользователя предполагает, что заранее не известно, какой именно пользователь ИСУФА будет работать с данным мобильным устройством (и установленным на нем приложением). Следовательно, мобильное приложение должно заранее получить информацию обо всех своих потенциально возможных пользователях и данные для их аутентификации, а также авторизации. В общем виде эта схема процесса представлена на рис. 2.

Такая схема является более гибкой и удобной для производственного процесса. Преимущество заключается в том, что в любой момент времени любой его участник может завершить работу с мобильным приложением и передать мобильное устройство другому участнику, который, в свою очередь, может начать работу без обязательного выполнения обмена данными с серверной частью ИСУФА. Однако с точки зрения мобильного приложения и самой ИСУФА эта схема администрирования является более сложной для реализации.

Во-первых, в этом случае мобильное приложение должно хранить и соответствующим образом обрабатывать все данные, необходимые для проверки подлинности пользователя и предоставления ему соответствующих прав. Обработка данных аутентификации (то есть проверки подлинности) обычно не представляет собой какой-либо сложности. Но вот система авторизации (распределения прав) пользователей в ИСУФА может быть достаточно нетривиальной. Здесь уже необходимо учесть специфику именно ИСУФА, пользователи которой могут находиться на разных уровнях производственного процесса и имеют широкий набор совершенно разнородных прав по отношению к различным объектам, информация о которых содержится в данной ИСУФА. Поэтому механизм управления правами в подобной ИСУФА должен быть достаточно гибким и обладать широким набором возможностей. При выполнении авторизации на стороне мобильного приложения оно должно обладать адекватными возможностями. Конечно, далеко не все участники ИСУФА потенциально могут использовать мобильные приложения в автономном режиме работы. Поэтому можно несколько

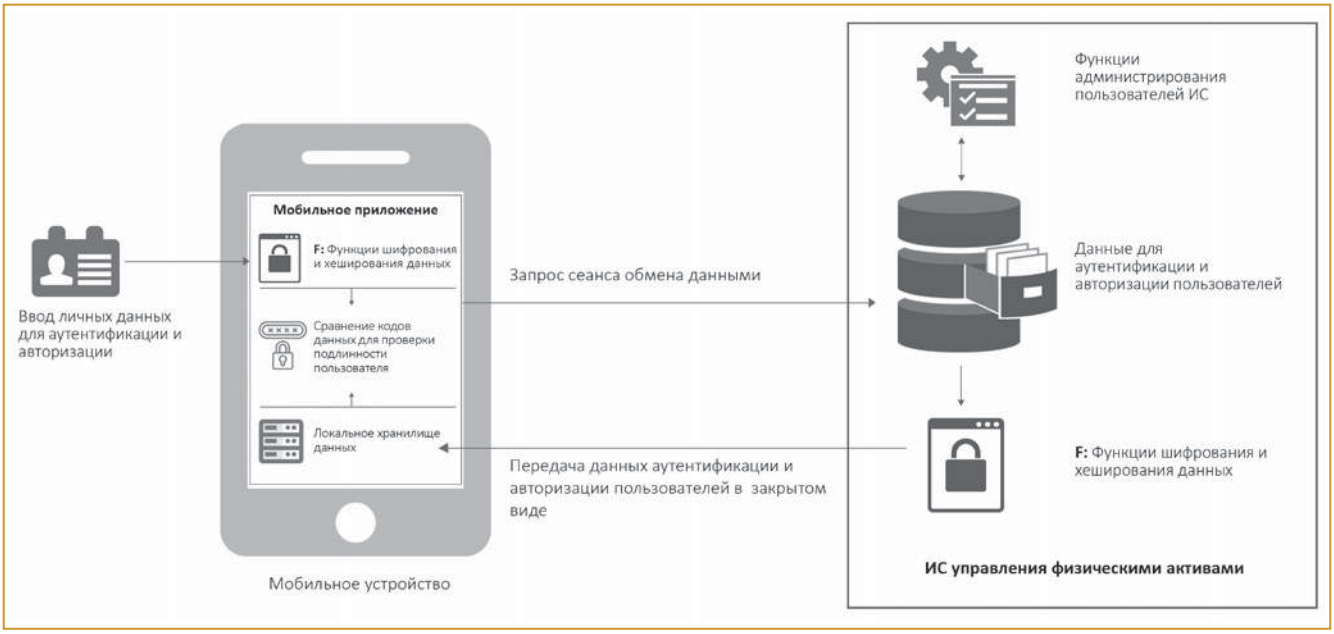

Рис. 2. Администрирование пользователей мобильных приложений с использованием аутентификации на стороне мобильного устройства

упростить задачу, ограничив перечень потенциально возможных пользователей приложения и доступных им функций. Тем не менее даже в этом случае функциональность авторизации пользователей в мобильном приложении будет необходима.

Во-вторых, в данном случае, поскольку на момент выполнения обмена данными не известно, какой именно пользователь будет работать с мобильным приложением, должна быть предусмотрена возможность передачи на мобильное устройство всех данных, необходимых для аутентификации и авторизации любого возможного пользователя. В результате административные данные ИСУФА оказываются на мобильном устройстве, которое менее защищено от любого программного или физического воздействия, чем другие компоненты ИСУФА. Поэтому в этом случае необходимо принять во внимание вопросы, связанные с информационной безопасностью и защитой данных. Хранение административных данных мобильного приложения должно быть организовано таким образом, чтобы, даже получив доступ к этим данным, злоумышленник не мог использовать их для доступа в ИСУФА от чужого имени или для расширения своих прав.

Таким образом, схема администрирования мобильных приложений, когда аутентификация и авторизация пользователей выполняются непосредственно самим мобильным приложением, является более гибкой и удобной, но при этом более сложной в реализации и требует дополнительных мер по защите административных данных на мобильном устройстве. При этом функции, используемые мобильным приложением для работы с административными данным, должны быть полностью идентичны аналогичным функциям, применяемым в других компонентах ИСУФА (рис. 2).

Заключение

Возможности современной ИСУФА существенно расширяются при использовании мобильных устройств. При этом актуален автономный режим работы мобильных устройств без наличия прямой связи с другими компонентами ИСУФА. Такой режим функционирования мобильного устройства требует наличия специализированного мобильного приложения из состава ИСУФА, установленного на данном устройстве. Для администрирования пользователей подобных мобильных приложений необходимо выполнять проверку подлинности (аутентификацию) и управление правами доступа (авторизацию), как

Если вы не используете мобильные приложения для управления физическими активами, не беспокойтесь - ваши конкуренты сделают это за вас.
Ремейк по фразе Джейми Тернер

и для всех других участников ИСУФА. Основные данные для выполнения этих функций должны быть подготовлены в серверной части ИСУФА.

В простейшем случае аутентификация пользователя может сводиться к получению им физического доступа к мобильному устройству, а авторизация ограничиваться всем доступным на данном устройстве набором функций и составом загруженных на него данных. Однако в условиях постоянного расширения функций мобильных приложений в составе ИСУФА такой тривиальный подход неприемлем. Поэтому реальные мобильные приложений, установленные на мобильных устройствах в составе ИСУФА, должны иметь функции администрирования пользователей, которые могут выполняться как на самом мобильном приложении, так и другими компонентами ИСУФА во взаимодействии с мобильным приложением в зависимости от способа администрирования, принятого в данной системе. Специфика ИСУФА налагает дополнительные требования на выполнение данных функций.

Список литературы

1. *Кац Б.А.* Чем управляют в системах управления активами? Часть 1. //Журнал главного инженера. 2018. №1. С. 69-79.
2. *Кац Б.А.* Чем управляют в системах управления активами? Часть 2. //Журнал главного инженера. 2018. №2. С. 34-49.
3. *Иорш В.И.* Концепция создания правильной системы управления физическими активами // Менеджмент сегодня. 2017. №4 (100). С. 288-303.
4. *Антоненко И.Н.* Информационные технологии управления эксплуатацией инфраструктуры // Информационные ресурсы России. 2018. №2. С. 39-43.
5. *Молчанов А.Ю.* Мобильные приложения в системах управления физическими активами // Автоматизация в промышленности. 2019. №8. С. 13-20.
6. *Антоненко И.Н.* EAM-система TRIM: от автоматизации ТОиР к управлению активами // Автоматизация в промышленности. 2015. №1. С. 40-43.
7. *Молчанов А.Ю.* Организация распределенных вычислений для управления физическими активами // Автоматизация в промышленности. 2017. №8. С. 23-28.

Молчанов Алексей Юрьевич *– канд. техн. наук, директор по разработкам ООО «НПП «СпецТек», доцент ГУАП. Контактный телефон +7 (812) 329-45-60. E-mail: mill@spectec.ru*