Описание механизмов обеспечения информационной безопасности (ИБ) в iDecide 1.5

1. Введение

Цель настоящего документа – описание механизмов обеспечения информационной безопасности (далее – ИБ), используемых в составе решения iDecide 1.5.

2. Описание архитектуры решения

Решение iDecide 1.5 построено по принципу клиент-серверной архитектуры и состоит из Интеграционного Сервера (далее - ИС), предназначенного для сбора и управления данными, полученными из внешних сервисов и провайдеров информации (таких как Microsoft Exchange) и Мобильного Клиента (далее — клиент), предназначенного для визуализации информации, собранной Интеграционным сервером.

Все внешние сервисы находятся в intranet-сегменте сети заказчика и необходимая защита взаимодействия между ними и сервером осуществляется инфраструктурными средствами заказчика. В контексте обеспечения информационной безопасности мы будем понимать интеграционный сервер и внешние сервисы для интеграции как монолитную систему и называть сервером.

3. Общие положения

Выбор механизмов обеспечения ИБ обусловлен необходимостью гарантировать необходимый уровень безопасности всех компонентов решения:

- Интеграционный сервер
- канал передачи данных между интеграционным сервером и конечным мобильным устройством
- конечное устройство (мобильный планшет)
- специализированное приложение (АРМ руководителя)
- данные, передаваемые из ИС на конечное устройство.

4. Описание механизмов обеспечения ИБ

4.1. Защита Интеграционного сервера

Как упоминалось выше, Интеграционный сервер и внешние сервисы устанавливаются в защищенную intranet-сеть предприятия и не требуют дополнительных средств для обеспечения информационной безопасности.

4.2. Защита канала передачи данных между Интеграционным сервером и конечным мобильным устройством.

Защита канала взаимодействия осуществляется средствами решения КриптоПРО sTunnel, позволяющее организовать защищенное соединение, отвечающее отечественным стандартам безопасности. Общение сервера и клиента реализовано как взаимодействие двух экземпляров приложения sTunnel, один из которых расположен в интранете и экранирует сервер от внешней информационной среды (DMZ-зона), а второй находится на клиенте и экранирует

специализированное приложение от внешней среды. Взаимодействие осуществляется TLS-алгоритмами, реализованными КриптоПРО, и требует двустороннюю подпись, передаваемую с помощью ЭЦП.

Взаимодействие sTunnel и сервера осуществляется внутри интранета и защищено инфраструктурой сети заказчика. Взаимодействие второго экземпляра sTunnel с мобильным клиентом осуществляется по клиент-серверной архитектуре в пределах мобильного устройства и защищено аппаратной архитектурой устройства.

4.3. Аутентификация пользователя конечного устройства (мобильного планшета)

Аутентификация пользователя приложения осуществляется средствами физически отделимых токенов различных производителей (в зависимости от требований клиента). Такие токены могут быть как беспроводные (Secure Messaging over Bluetooth технология), так и физически присоединяемые к мобильному устройству со специализированным приложением. Такой токен содержит личный ключ пользователя, позволяющий производить аутентификацию в приложении.

4.4. Контроль целостности специализированного приложения

Контроль целостности приложения осуществляется средствами операционной системы iOS. Операционная система iOS организует изолированное информационное пространство для каждого работающего приложения и архитектурно не допускает воздействие любого приложения на информационное пространство другого приложения.

4.5. Контроль целостности данных, передаваемых из ИС на конечное устройство

Контроль целостности данных осуществляется средствами двусторонней ЭЦП, которая требуется при использовании КриптоПРО sTunnel.

4.6. Дополнительная функциональность

В качестве дополнительного средства безопасности сервер позволяет инициировать удаление конфиденциальной информации с устройства. Также при смене пользователя вся информация предыдущего, хранимая локально, уничтожается.

Вся информация, хранимая на мобильном устройстве, расположена в защищенной операционной системой приватной зоне. Данные в этой зоне недоступны вне приложения, это обеспечивает архитектура iOS. Тем не менее, по дополнительному запросу возможно организовать шифрование хранимой информации средствами КриптоПРО для защиты несанкционированного доступа к флеш-памяти на физическом уровне (разборка мобильного устройства).