Технические спецификации

Remote Update of Firmware

(RUF)

© Компания DORS 2015 г.

Все права защищены.

Телефон:(495) 725-23-23; 725-23-25, Факс:(495) 725-23-22

E-mail: support@dors.com

СОДЕРЖАНИЕ

1 ВВЕДЕНИЕ

1.1 Список сокращений, основных понятий и определений

Перечень сокращений с их расшифровкой, а также список основных понятий и определений приведен в документе: «ЭД. Термины и определения. RUF».

1.2 Наименование программного продукта

Полное наименование программного обеспечения (далее – ПП) – Remote Update of Firmware (Система удаленного обновления программного обеспечения и прошивок устройств).

Краткое наименование ПП – RUF (СУО).

1.3 Назначение и цели документа

Данный документ представляет собой технические спецификации модулей ПП.

1.4 Область и условия применения документа

Документ ориентирован на технических специалистов и применяется как руководство для более детального ознакомления с внутренним устройством ПП RUF.

1.5 Назначение и цели ПП

ПП предназначен для обновления прошивок устройств BVS с помощью сети Интернет, без обращения в сервисный центр ГК ДОРС.

Целью ПП является повышение качества распознавания банкнот устройствами BVS за счёт оперативного обновления алгоритмов распознавания, а также сокращение обращений покупателей устройств в сервисные центры.

1.6 Перечень объектов автоматизации, на которых используется ПП

Объектом автоматизации является процесс обновления прошивок устройств BVS.

В процессе обновления ПО и прошивок участвуют следующие инфраструктурные единицы:

1. Клиентский персональный компьютер с установленными УЗПО и СПДО;
2. Сервер обновления с двумя виртуальными web-серверами (публичный сервер и сервер обеспечения работы web-АРМ);
3. Компьютер, на котором будет запущен АРМ Администратора.

2 Системные требования

2.1 Программные требования

2.1.1 Программные требования к клиентскому компьютеру

ПО выполняется на клиентском компьютере при наличии следующего базового программного обеспечения:

- ОС Windows XP SP2 и выше;
- компонент «Microsoft XML Parser версии 4.0 SP2 (устанавливается системой развёртывания).

Успешность выполнения развёртывания ПО зависит от наличия административного права пользователя на установку системного сервиса операционной системы.

2.1.2 Программные требования к компьютеру администрирования

ПП функционирует на компьютере администрирования при наличии следующего базового программного обеспечения:

- ОС Windows XP;
- MS .net framework 4.0;
- браузер «Microsoft Internet Explorer версии 8» и выше.

2.1.3 Программные требования к серверу обновления ПО и прошивок устройств

ПП функционирует на сервере обновления при наличии на нём следующего базового программного обеспечения:

- ОС Windows Server 2008 и выше;
- СУБД Microsoft SQL Server 2000;
- Microsoft.Net Framework 4.5 и выше;
- ASP.NET версии 4.0 и выше.

2.2 Аппаратные требования

Аппаратные требования для всех компьютеров не превышают требований для установленного базового ПО (ОС, СУБД).

3 ОПИСАНИЕ СИСТЕМЫ

3.1 Перечень функций, реализуемых системой

Комплекс обновления прошивок устройств BVS выполняет две функции: администрирования сервера обновлений и обновления прошивок.

Административная функция выполняется сервером обновления, управляемого из АРМ Администрирования, запущенного на одном из рабочих мест в КБ ДОРС.

Обновление прошивок устройств BVS осуществляется сервисом проверки доступности обновлений (СПДО), взаимодействующим как с устройствами BVS, так и с сервером обновления. Управление СПДО осуществляется посредством АРМ управления загрузкой программных обновлений (УЗПО).

3.2 Описание принципов функционирования ПО, регламенты и режимы функционирования

Взаимодействие АРМ Администрирования с сервером обновления осуществляется по протоколу https (выполняется взаимная аутентификация и шифрование канала).

Взаимодействие СПДО с сервером обновления осуществляется по http (шифрование канала не выполняется).

Взаимодействие СПДО с устройствами BVS выполняется в соответствии с описанием протокола, приведенного в документе «Сервисный протокол BVS. Внутренняя спецификация».

Схема взаимодействия приведена на рисунке (Рисунок 3.1):

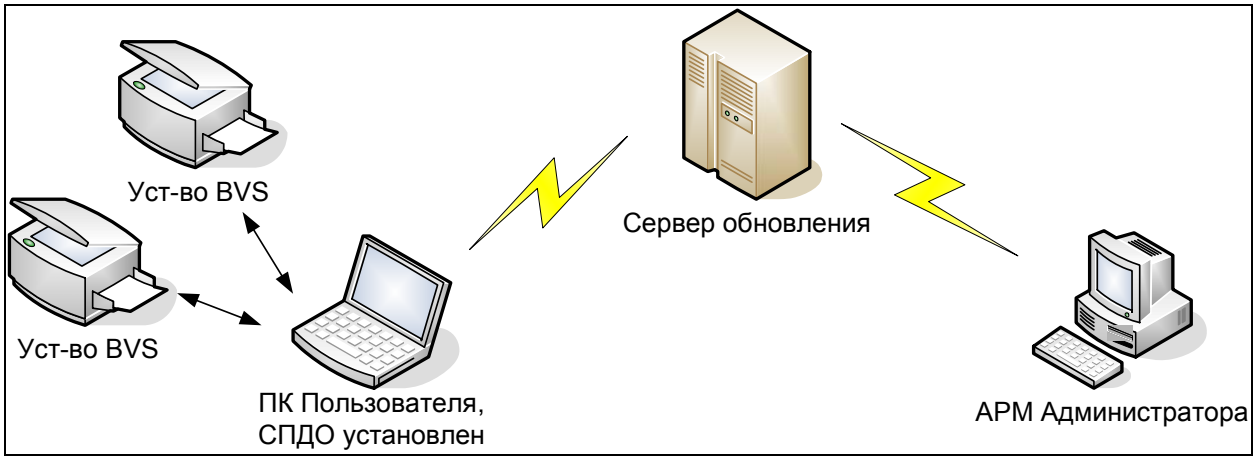

Рисунок 3.1 – Схема взаимодействия

3.3 Описание функциональных подсистем

3.3.1 Сервер обновления

Сервер обновления обеспечивает:

- Хранение данных администраторов системы;
- Хранение и предоставление данных к журналам аудита;
- Управление информацией:
  - о моделях устройств BVS;
  - о наборах бинарных объектов, входящих в прошивки устройств BVS;
  - о партиях выпущенных устройств;
  - о серийных номерах выпущенных устройств.
- Хранение бинарных объектов;
- Передачу СПДО информации об актуальных версиях бинарных объектов для подключенных к СПДО устройств;
- Передачу СПДО актуальных версий бинарных объектов.

3.3.2 АРМ Администратора

Предоставляет пользовательский интерфейс для доступа к функциям администрирования сервера обновления.

3.3.3 СПДО

Сервис проверки доступности обновлений обеспечивает:

- Обработку информации о подключаемых к компьютеру устройствах BVS;
- Систематически, запрашивает информацию о доступности обновления прошивок у сервера обновления для всех ранее подключенных устройствах BVS;
- Загружает обновлённые бинарные объекты, доступные на сервере обновления в устройства BVS.

3.3.4 УЗПО

Предоставляет пользовательский интерфейс для управления загрузкой обновлений в устройства BVS.

3.3.4.1 Структура базы данных

Структура базы данных сервера обновлений проектируется исходя из следующих особенностей системы обновления:

1. С уникальным идентификационным номером устройства однозначно связан набор бинарных объектов. Данная связь обозначается в сопутствующих документах как «класс устройства»;

2. Установка на устройство BVS бинарных объектов возможно только в том случае, если устанавливаемая версия имеет номер, отличный от уде установленной версии. Для решения проблемы с публикацией версий бинарных объектов, содержащих критичные ошибки, будет использоваться повторная публикация ранее выпущенных стабильных версий, но с повышением номера версии.

Бинарный объект, входящий в прогрузку устройства BVS, может быть описан следующим набором свойств (ненормализованная база данных):

1. Идентификатор (символическое имя объекта);
2. Версия бинарного объекта;
3. Диапазон серийных номеров, к которым может быть применён объект;
4. Содержимое бинарного файла.
5. Для обеспечения единообразного отображения номеров версии бинарных объектов при их подготовке к публикации принят следующий формат номера:

База валют	EEE	EE.	CCC.	DDD
Не База	AAA.	BBB.	EEE	EE.
	Старший байт			Младший байт

Где:

AAA,BBB,CCC,DDD – 10-ричное число 0…255 без ведущих нулей

EEEEE – 10-ричное число 0….65535 без ведущих нулей

Существующие требования к поисковым запросам позволяют говорить о следующей структуре базы данных:

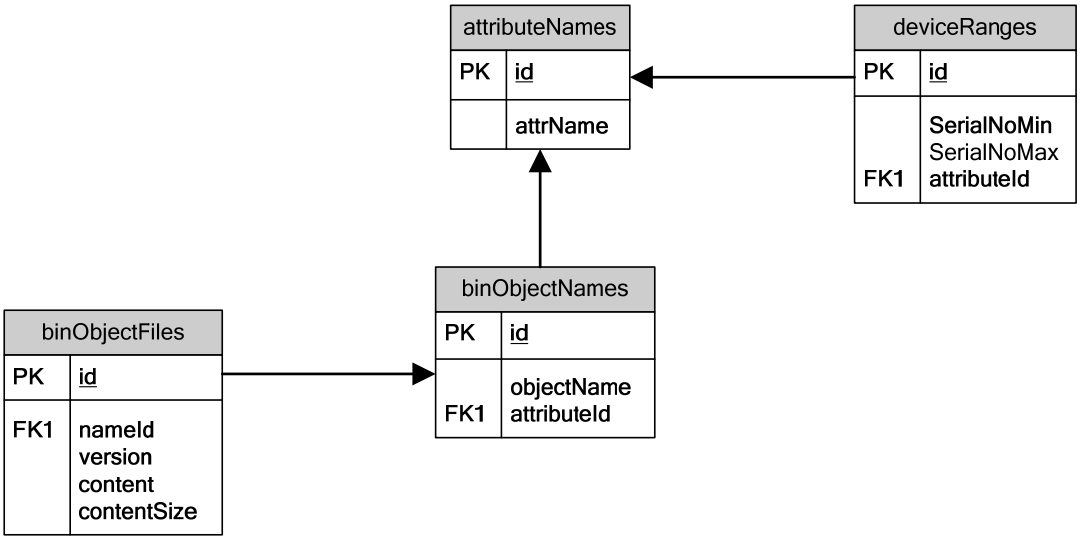

Рисунок 3.2 – Структура базы данных

Определение списка всех доступных бинарных объектов:

```
SELECT binObjectNames.objectName, attributeNames.attrName, binObjectNames.id
FROM binObjectNames
INNER JOIN attributeNames ON attributeNames.id = binObjectNames.attributeId
ORDER BY binObjectNames.objectName DESC
```

Определение списка зарегистрированных партий устройств:

```
SELECT attributeNames.attrName, deviceRanges.SerialNoMin, deviceRanges.SerialNoMax
FROM attributeNames
INNER JOIN deviceRanges ON deviceRanges.attributeId = attributeNames.id
ORDER BY attributeNames.attrName DESC
```

Получение списка всех модификаций бинарных объектов для устройства:

```
SELECT binObjectNames.objectName, binObjectFiles.version, binObjectFiles.content_size,
binObjectFiles.id FROM binObjectNames

INNER JOIN deviceRanges ON deviceRanges.attributeId = binObjectNames.attributeId

INNER JOIN binObjectFiles ON binObjectFiles.nameId = binObjectNames.Id

WHERE CAST(deviceRanges.SerialNoMin as bigint) <= @DeviceId AND CAST(deviceRanges.SerialNoMax
as bigint) >= @DeviceId

ORDER BY binObjectFiles.version DESC
```

Последний запрос вернёт все доступные модификации бинарных объектов в порядке уменьшения номера версии. С целью оптимизации производительности, в таблице binObjectFiles можно хранить не все версии бинарных объектов, а только наиболее актуальные.

Скрипт создания базы данных может быть приблизительно следующим:

```
CREATE TABLE [attributeNames] (
        [id] [int] IDENTITY (1, 1) NOT NULL ,
        [attrName] [nvarchar] (50) COLLATE Cyrillic_General_CI_AS NULL ,
        CONSTRAINT [PK_attributeNames] PRIMARY KEY  CLUSTERED
        (
                [id]
        )  ON [PRIMARY]
) ON [PRIMARY]
GO

CREATE TABLE [binObjectFiles] (
        [id] [int] IDENTITY (1, 1) NOT NULL ,
        [nameId] [int] NOT NULL ,
        [version] [int] NOT NULL ,
        [content] [image] NOT NULL ,
```

```
	[content_size] [int] NOT NULL ,
	[content_type] [nvarchar] (50) COLLATE Cyrillic_General_CI_AS NOT NULL ,
	CONSTRAINT [PK_binObjectFiles] PRIMARY KEY  CLUSTERED
	(
		[id]
	)  ON [PRIMARY]
) ON [PRIMARY] TEXTIMAGE_ON [PRIMARY]
GO

CREATE TABLE [binObjectNames] (
	[id] [int] IDENTITY (1, 1) NOT NULL ,
	[objectName] [nvarchar] (50) COLLATE Cyrillic_General_CI_AS NOT NULL ,
	[attributeId] [int] NOT NULL ,
	CONSTRAINT [PK_binObjectNames] PRIMARY KEY  CLUSTERED
	(
		[id]
	)  ON [PRIMARY]
) ON [PRIMARY]
GO

CREATE TABLE [deviceRanges] (
	[id] [int] IDENTITY (1, 1) NOT NULL ,
	[SerialNoMin] [nvarchar] (50) COLLATE Cyrillic_General_CI_AS NOT NULL ,
	[SerialNoMax] [nvarchar] (50) COLLATE Cyrillic_General_CI_AS NOT NULL ,
	[attributeId] [int] NOT NULL ,
	CONSTRAINT [PK_deviceRanges] PRIMARY KEY  CLUSTERED
	(
```

[id]

) ON [PRIMARY]

) ON [PRIMARY]

GO

3.4 Модель безопасности

Модель безопасности подробно описана в документе «Описание модели информационной безопасности комплекса удалённого обновления прошивок устройств BVS». Основными угрозами, решаемыми комплексом удалённого обновления прошивок устройств BVS, являются:

1. Помещение злоумышленниками на сайт сторонних данных под видом бинарых объектов BVS;
2. Перехват аутентификационных данных пользователями АРМа Администратора (web-АРМ) с использованием фишинг-сервера.

Для обеспечения защиты комплекса от различного вида атак трафик шифруется с использованием SSL, используется двухсторонняя аутентификация сервера обновления и пользовательского приложения (web-браузер), а также обязательная аутентификация пользователя и разграничение прав доступа на основе реляционной модели.

Следует заметить, что осуществляется защита соединения «сервер обновления – АРМ Администратора», тогда как соединения «СПДО – сервер обновления» никак не защищаются. Причина состоит в том, что сервер обновления не принимает от СПДО каких-либо данных, способных повлиять на работоспособность комплекса, тогда как АРМ Администратора загружает на сервер обновления бинарные объекты, а также позволяет его настроить.