Экземпляр ознакомительный

Проектная документация

«Специализированная Система обеспечения Безопасности информационного взаимодействия»

Пояснительная записка

ООО «НПО «РэйнбовСофт»

Саратов 2012 г.

Оглавление

Цель и назначение Системы

Основной целью разработки и внедрения специализированной системы обеспечения безопасности информационного взаимодействия является удовлетворение требованиям безопасности в процессе автоматизированного взаимодействия специализированных ведомственных информационных систем ГИБДД с другими объектами информационного взаимодействия (сложными, в виде информационных систем других ведомств, средней сложности и элементарными, в зависимости от решаемой задачи). Примерами такого взаимодействия являются такие актуальные задачи:

- взаимодействие с иными ведомствами и организациями с целью эффективного предоставления и получения информации в рамках осуществления служебной деятельности и оказания государственных и иных, требующих эффективной реализации, услуг (ФКРФ, ФССП, ФНС, ФГУП Почта России, операторы платежей и т.д.)
- взаимодействие с сервисами обеспечения государственных и иных услуг населению в электронном виде, включая информирование населения об имеющихся штрафах ГИБДД и состоянии оплаты по ним;

Имеющиеся нормативные документы (ФЗ, ведомственные и иные приказы, указы, указания и распоряжения, инструкции и т. д.) оправданно определяют достаточно строгие требования к обеспечению информационной безопасности в рамках осуществления деятельности государственных органов. Это определяет набор задач по защите и обеспечению безопасности обрабатываемой и хранимой информации, решение которых требует применения современных, соответствующих времени, подходов. При этом даже применение традиционных специализированных систем защиты информации, построенных на шифровании передаваемой информации и управлении доступом к информационным ресурсам и каналам связи, не позволяет в полной степени обеспечить адаптивную защиту в рамках современных моделей угроз, применимых к уже имеющимся на сегодняшний день информационным системам. Именно по этой причине имеются ведомственные требования об ограничении прямого (см. рис. 1), даже защищаемого, соединения между взаимодействующими информационными системами. Наличие таких требований и, вместе с тем, потребности в эффективном и оперативном информационном взаимодействии с иными объектами (в рамках межведомственного взаимодействия, оказания услуг в электронном виде и пр.), определяет задачу поиска соответствующего решения, обеспечивающего информационное взаимодействие без прямого соединения информационных систем и, при этом, обеспечивающего работу в режиме высокой нагрузки и соответствие требованиям по отказоустойчивости.

Говоря простыми словами, прямое соединение использовать нельзя, но информационное взаимодействие реализовать необходимо. Именно для решения данной непростой задачи создана настоящая Система.

Такое решение основывается на архитектуре логического шлюзования данных с применением методов интеллектуальной обработки выполняемых запросов. Именно данная архитектура использована для практического решения задачи обеспечения эффективного и оперативного информационного взаимодействия в рамках построения

гетерогенной информационной системы, объединяющей информационные подсистемы (объекты взаимодействия) различных уровней сложности, включая ведомственные информационные системы. На основании описанного концептуального и архитектурного решения разработана специализированная система обеспечения безопасности информационного взаимодействия. Данная система позволяет успешно решить все обозначенные задачи, обеспечивая соответствие имеющимся требованиям по защите информации. Таким образом, имеется возможность реализации качественно нового технологического уровня обеспечения работы информационной системы ГИБДД, а также возможность ощутимо приблизится к создания эффективно работающего сегмента единого информационного пространства органов государственной власти и общества в целом.

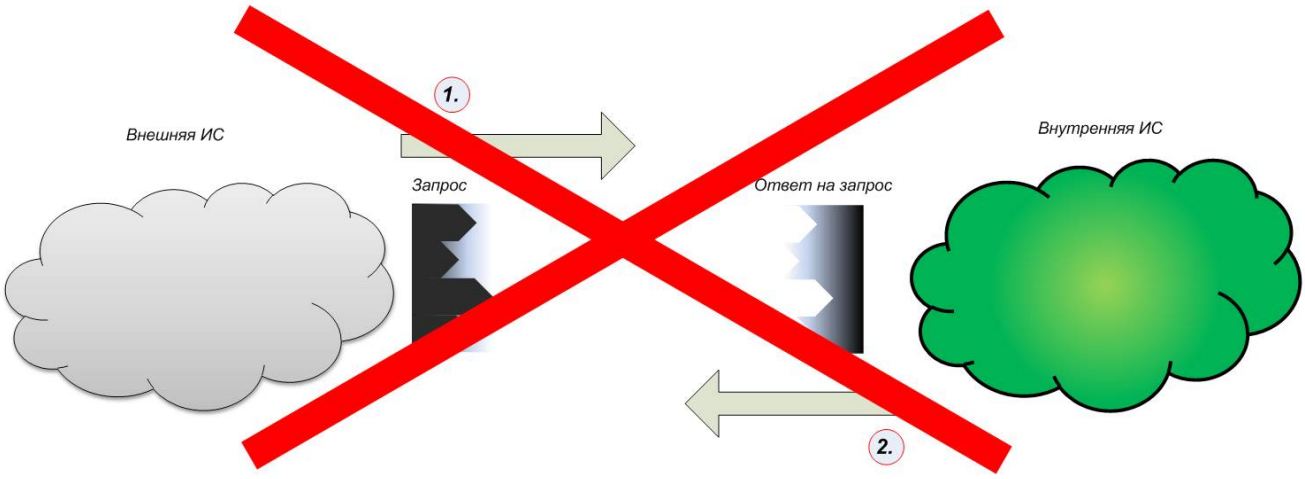


Рисунок 1. Иллюстрация недопустимого решения (с прямым соединением)

Предлагаемая разработка построена и работает на основе системы шлюзования информационных потоков, разработанной компанией ООО НПО “РэйнбовСофт”. Её назначением является объединение в гетерогенную информационную систему разнородных информационных систем. Исключение прямого соединения достигается за счет применения механизма рекомбинации и проверки запросов, реализованного в системе шлюзования (см. рис. 2).

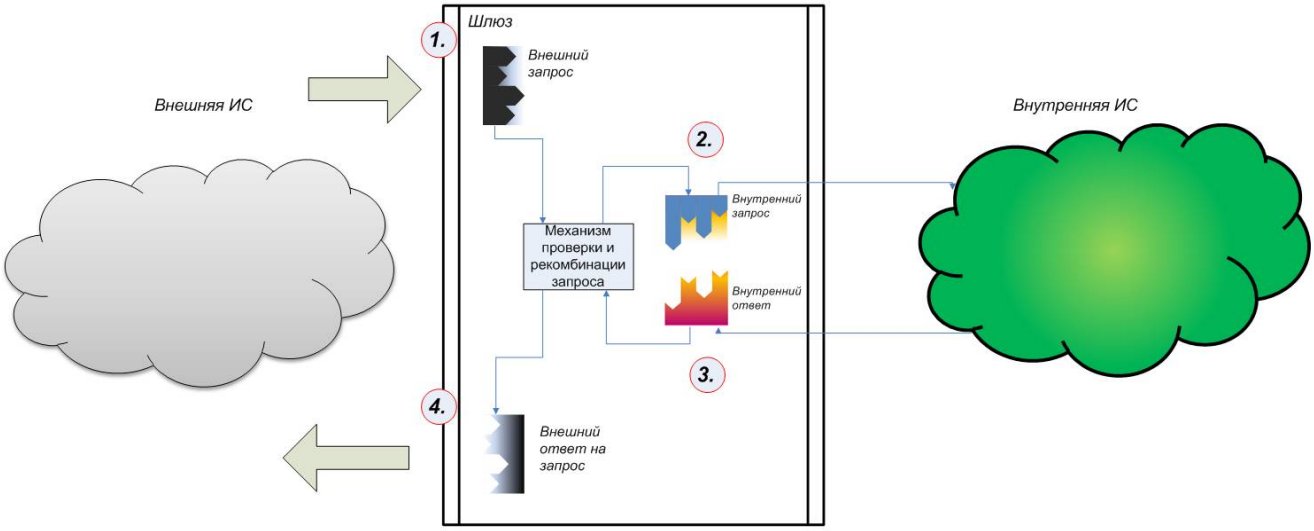


Рисунок 2. Корректное решение в соответствии с действующим законодательством (подключение через шлюз)

В настоящем документе для удобства и краткости обозначения полное наименование специализированной Системы обеспечения безопасности информационного взаимодействия заменяется на термин **Система**. В силу и по причине специфичности концептуальной сущности архитектуры реализации Системы, для грамотного понимания технических подробностей, так же может использоваться специализированный термин Система Шлюзования информации, сокращённо Система Шлюзования.

Часть I. Общее описание Системы

1. Основания разработки и описание системы

В соответствии с Федеральным Законом «Об организации предоставления государственных и муниципальных услуг» № 210-ФЗ от 27.07.2012, поставлена задача реализации государственных и муниципальных услуг в электронном виде.

Распоряжением Правительства Российской Федерации от 25 июня 2009 года № 872р на МВД России возложены задачи оказания государственных услуг по предоставлению сведений гражданам о совершённых ими административных правонарушениях в области БДД с использованием информационных и телекоммуникационных технологий (в том числе по сети общего пользования Интернет). В настоящее время данная функция исполняется с помощью Интернет-ресурса «Электронное Правительство» (портал ГОСУСЛУГИ.РУ) и федеральной информационной системой ГИБДД МВД Российской Федерации.

В то же время, оказание населению таких государственных услуг как:

- информирование о штрафах ГИБДД;
- предварительная запись с целью регистрации принадлежащих им транспортных средств;
- предварительная запись для получения водительских документов,

может и должно осуществляться также и региональными подразделениями ГИБДД с использованием Интернет-сайтов регионального управления ГИБДД.

Также имеется ещё целый ряд актуальных задач, требующих применения концептуально аналогичного подхода к их решению и, таким образом, можно констатировать очевидную необходимость реализации типового решения указанной задачи на уровне ГИБДД субъекта Российской Федерации, МРЦ ГИБДД и ГУ ОБДД МВД России. Именно решение данной задачи и является основной целью создания, внедрения и эксплуатации настоящей Системы. При этом учитываются все функциональные требования по защите конфиденциальной информации.

2. Требования к Системе

Требования к Системе подразделяются на функциональные требования и требования безопасности.

2.1. Функциональные требования

Система по запросу Внешних объектов (пользователей и (или) других систем) предоставляет определенные наборы данных, содержащихся в информационной системе ГИБДД.

Система поддерживает безопасную передачу запросов из информационной системы ГИБДД Внешним объектам и ответов на них.

Система формирует запросы на основании предоставления Внешними объектами данных:

- идентификатора Внешнего объекта;

- кода действия, выполнение которого запрашивается Внешним объектом у Системы;
- реквизитов запроса.

При обработке данных Пользователя Внешними объектами, алгоритм их работы должен предполагать запрос у Пользователя согласия на обработку персональных данных, когда таковое согласие требуется.

Система имеет возможность внешней интеграции со сторонними сервисами посредством настройки компонентов системы (без изменения принципиальной схемы функционирования системы и внедрения дополнительного оборудования).

2.2 Требования безопасности

Система исключает возможность поступления запросов, не связанных с функционированием Системы, к серверу запросов к источникам данных (во внутреннюю сеть);

Система оборудована программным и(или) аппаратным средством фильтрации поступающий к ней из сети Интернет запросов;

Модули Системы, рассчитанные на предоставление данных по запросам пользователя содержат компонент, предотвращающий массовое получение данных посредством применения автоматических алгоритмов;

Передача персональных данных осуществляется только в зашифрованном виде;

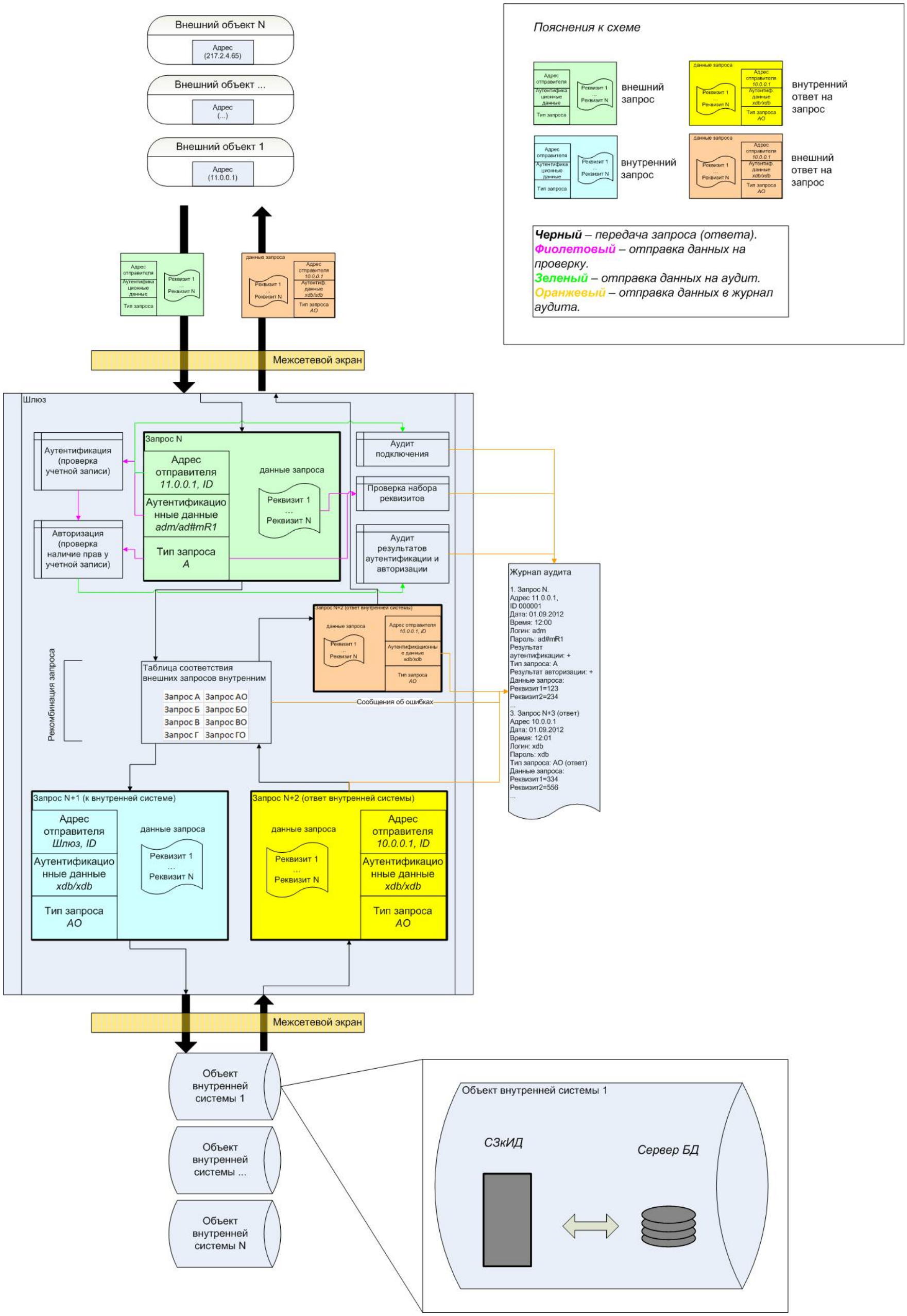
Шифрование информации проводится согласно действующим Государственным стандартам на шифрование.

Система обеспечивает выявление попыток внедрения не регламентированных кодов (с целью неправомерного получения информации или нарушения работоспособности системы) в поступающих запросах.

Интернет-сервис ведет журнал событий, в котором отображаются следующие события:

- факт получения запроса сервисом;
- факт направления сервисом запроса к подсистеме ГИБДД;
- факт получения сервисом ответа от подсистемы ГИБДД;
- факт направления ответа сервисом;
- ошибки взаимодействия.

Время восстановления после отказа, вызванного сбоем электропитания технических средств (иными внешними факторами), не фатальным сбоем (не крахом) операционной системы, не превышает 30-ти минут при условии соблюдения условий эксплуатации технических и программных средств. Время восстановления после отказа, вызванного неисправностью технических средств, фатальным сбоем (крахом) операционной системы, не превышает времени, требуемого на устранение неисправностей технических средств и переустановку программных средств.



Пояснения к схеме

Черный *– передача запроса (ответа).*
Фиолетовый *– отправка данных на проверку.*
Зеленый *– отправка данных на аудит.*
Оранжевый *– отправка данных в журнал аудита.*

Рисунок 3. Схема информационных потоков Системы

3. Описание работы системы

Принцип работы Системы объясняется схемой информационных потоков, представленной на рис.3.

Система состоит из нескольких элементов, каждый из которых выполняет свои определенные функции. Наименования элементов и их функции приведены в табл. 1.

Работа Система по указанной схеме предполагает обмен определённого конкретной задачей набора данных, который может включать в себя как значения реквизитов учёта, так и значение их текущего состояния. Идентификация обменных сообщений взаимодействующих систем осуществляется на основе уникального идентификатора, однозначно определённого во всех взаимодействующих системах. Уникальный идентификатор состоит из:

- кода запрашивающей системы;
- кода запрашиваемой системы;
- кода запрашиваемого действия;
- уникального внутреннего номера сообщения.

Информационное взаимодействие осуществляется следующим образом:

- запрашивающая ИС, с использованием собственных средств формирует необходимое сообщение, включая в него идентификатор сообщения, содержащий код запрашиваемой ИС;
- запрашивающая ИС передаёт сообщение на Шлюз;
- Шлюз, используя уникальный идентификатор сообщения, определяет запрашивающую и запрашиваемую системы, устанавливает наличие прав запрашивающей системы на выполнение действия;
- в случае отсутствия соответствующих прав, Шлюз возвращает запрашивающей ИС отказ в доступе;
- при наличии соответствующих прав, Шлюз через встроенный специализированный web-сервис маршрутизации данных направляет сообщение в запрашиваемую ИС (к СЗкИД);
- СЗкИД выполняет требуемое действие (отправляет запрос на Сервер БД) и и формирует ответ (выборку данных) или сообщение об ошибке;
- запрашиваемая ИС (СЗкИД) передаёт ответ или сообщение об ошибке через специализированный web-сервис маршрутизации данных Шлюза;
- web-сервис маршрутизации данных направляет полученное сообщение по адресу запрашивающей ИС;
- по результатам ответа запрашивающая ИС выполняет необходимые действия собственными средствами.

Система работает и в обратном направлении, т. е. возможно установление соединения, инициатором которого является внутренняя информационная система (ИС ГИБДД).

Техническая реализация схемы информационных потоков основывается на технологиях веб-сервисов и передачи данных по протоколу SOAP и приведена на рисунке 4.

Описание механизма логического шлюзования приведено в разделе 4.1.

Таблица 1. Элементы Системы

Полное наименование элемента		Сокращенное наименование элемента	Функциональное назначение
Внешний объект информационного взаимодействия		Внешний объект	Формирование и отправка запросов Шлюзу; принятие, преобразование и представление данных, полученных от Шлюза Например, такой внешний объект как сервер приложений «Хостинг» системы информирования, выполняет следующие функции: Хранение статических и формирование динамических страниц, предоставляемых пользователю; Обработка запросов пользователя; Формирование запросов Шлюзу; Первичные проверки корректности веденных пользователем данных; Получение данных от Шлюза и преобразование их в Интернет страницу.
Сервер Приложений «Шлюз»		Шлюз	Получение запросов от Внешних объектов и проведение различных проверок над ними; Преобразование запросов от Внешних объектов в запросы к СЗкИД; Получение от СЗкИД ответов на запросы, с последующим преобразованием и отправкой их на Внешние объекты.
Внутренние объекты Информационной системы ГИБДД	Сервер Запросов к Источникам Данных	СЗкИД	Функциональное назначение: Получение запросов от Шлюза и преобразование их в вид, понятный Серверу БД; Отправка запросов Серверу БД; Получение ответов от Сервера БД в виде табличных данных; Преобразование табличных данных в формат сообщений и отправка их Шлюзу;
	Сервер Базы Данных	Сервер БД	Элемент присутствует при необходимости. Хранение и обработка данных; Получение запросов от СЗкИД; Формирование выборки данных при помощи хранимых процедур; Отправка данных СЗкИД.

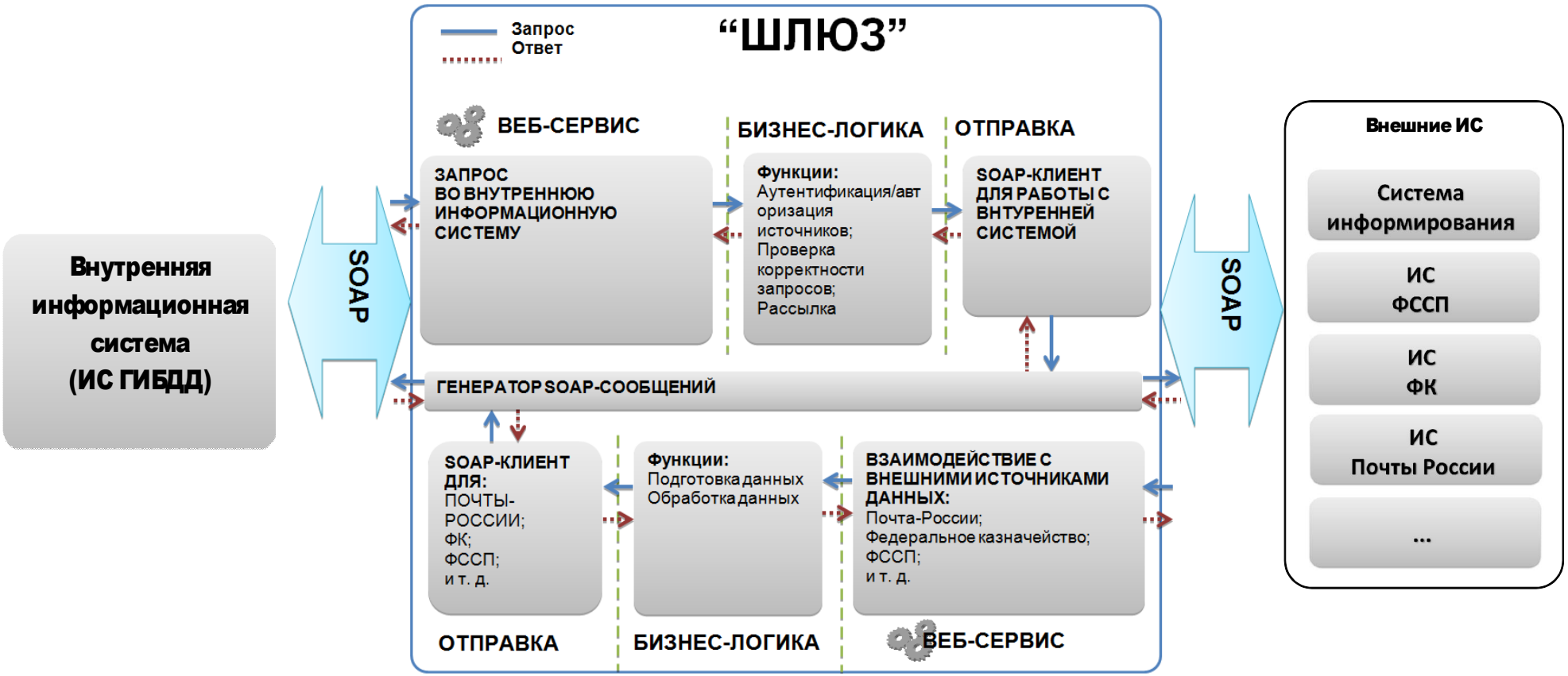


Рисунок 4. Реализация схемы информационных потоков

Реализованная в соответствии с настоящим Проектом Типовая Региональная Система Информирования ГИБДД позволяет расширять набор информационных и иных сервисов в соответствии с проектными дополнениями без ограничений по набору функциональных возможностей. Это достигается за счёт универсальности основного механизма логического шлюзования и применяемой модели безопасности, а так же за счёт компонентно-модульной реализации и возможности интеграции с любыми источниками данных. Для получения более подробной информации обращайтесь в компанию разработчик (ООО НПО “РэйнбовСофт”) настоящей Системы.

4. Уровни обеспечения безопасности информационного взаимодействия

4.1. Уровень логического шлюзования

Безопасность информационного взаимодействия на логическом уровне обеспечивается сервером выполнения логического шлюзования, имеющим созвучное с его логической ролью в Системе краткое рабочее наименование Шлюз. Общая схема внутренней организации работы Шлюза и алгоритм её работы представлены на рис. 5.

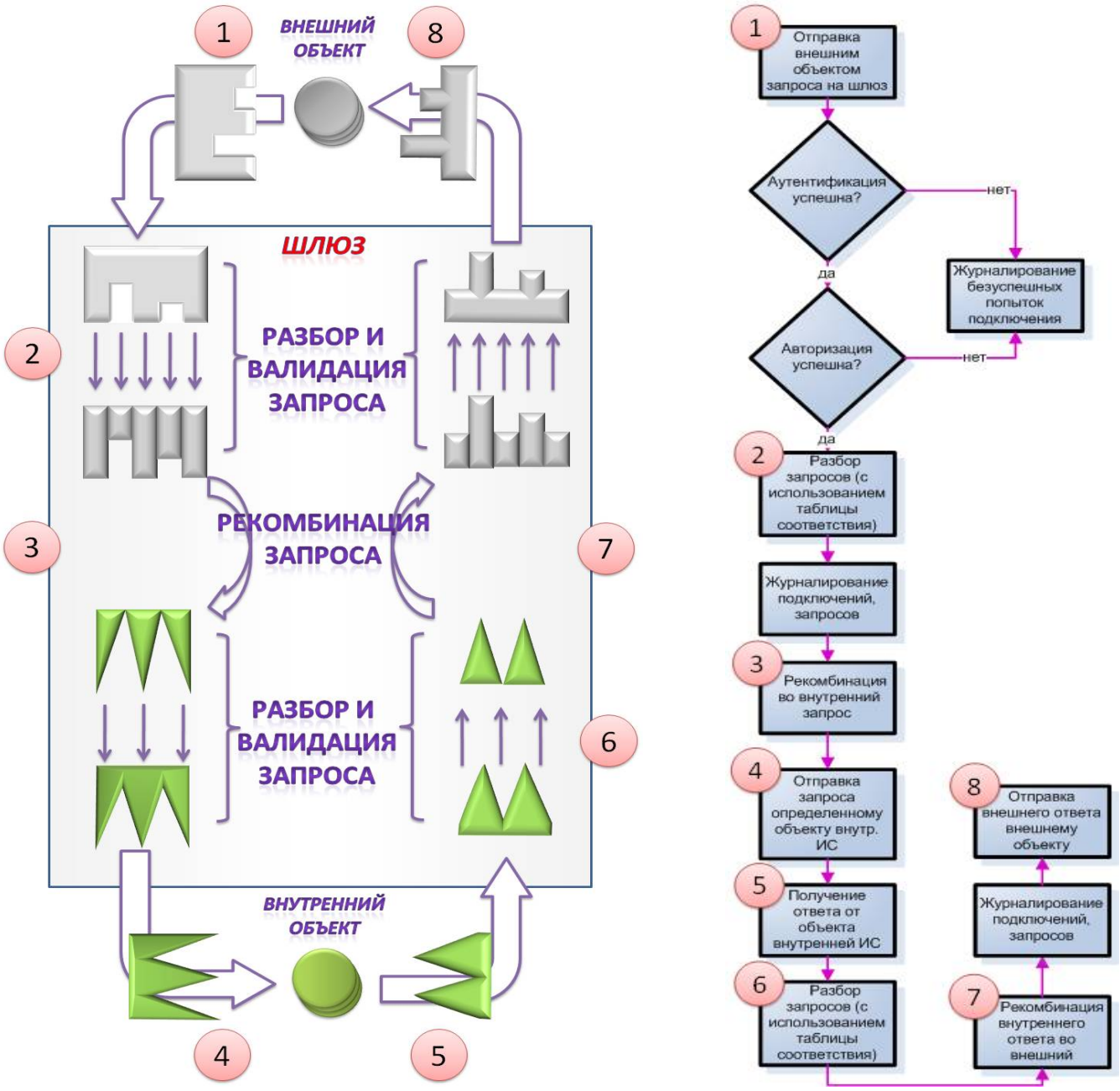


Рисунок 5. Иллюстрация принципа работы и алгоритм работы логического шлюзования

Объекты внешних ИС (внешние объекты) формируют запрос к веб-сервисам Шлюза (внешний запрос). На этом шаге логическое шлюзование может обеспечиваться

собственными механизмами Внешних объектов, например, путём проверки соответствия входных данных на соответствие шаблонам и регулярным выражениям (например, поле «фамилия» может состоять лишь из букв русского алфавита) ещё до формирования внешнего запроса. Таким образом, первый случай логического шлюзования – проверка входных данных на Внешнем объекте (например, Хостинге). Требования к наличию внутренних проверок у Внешних объектов должны быть определены на этапе согласования схемы подключения Внешних объектов к Системе.

Если данные проходят проверку, формируется внешний запрос. Внешний запрос содержит в том числе учетные данные, при помощи которых подвергается как аутентификации, так и авторизации на Шлюзе.

Обе этих процедуры служат как для обеспечения безопасности, так и позволяют, не меняя принципиальной схемы работы, производить поэтапное расширение Системы путём интеграции дополнительных сервисов на Внешний объект или добавления Внешних объектов.

Таким образом, второй и основной этап логического шлюзования состоит в валидации запросов к информационной системе, абстрагировании от внешних запросов инструментами Шлюза.

Логическое шлюзование происходит следующим образом:

1) из полученного запроса извлекаются идентификационные данные (идентификаторы отправителя и получателя, тип запроса);
2) идентификаторы проходят аутентификацию в Системе, т.е. процедуру проверки наличия учетной записи в Системе по учетным данным (имени пользователя и пароля);
3) идентификаторы проходят авторизацию в Системе, т. е. процедуру проверки наличия прав у учетной записи на выполнение запрашиваемых операций (отправка определенных типов запросов);
4) проверка валидности внешних запросов, т. е. проверки:
    4.1) соответствия внешнего запроса правилам формирования (соответствия набора атрибутов запроса его типу);
    4.2) заполненности, логического соответствия значений атрибутов и т.д.;
5) логические проверки безопасности (частота обращений с одного ip-адреса, попытки подключений из доверенной и не доверенных зон сети)
6) используя таблицу соответствия внешних запросов внутренним, формируется внутренний запрос, адрес отправки которого зависит от типа внешнего запроса;
7) реквизиты внешнего запроса определенным образом «перегружаются» во внутренний запрос;
8) внутренний запрос отправляется определенному внутреннему объекту;
9) ответ от внутреннего объекта проходит обратную процедуру (шаги №№7-1), т. е. рекомбинируется во внешний запрос, фиксируется в журналах и уже в рекомбинированном виде отправляется внешнему объекту.

Абстрагирование в данном ключе подразумевает изоляцию внутренней информационной системы по средствам исключения прямого подключения.

Для внешнего объекта, при этом, структура взаимодействия не является очевидной, наоборот, информационное взаимодействие остается «прозрачным», т. е. внешний объект получает ответ на запрос в том же формате, в котором осуществлялась

отправка запроса, промежуточные структурные преобразования этих запросов ни каким образом не выходят за пределы работы Шлюза.

Любые несоответствующие определенным наборам правил запросы отклоняются, а факт их поступления, ровно как и причина несоответствия, фиксируется.

Систематический анализ журнала попыток несоответствующих правил подключения позволяет делать выводы об источниках этих подключений, целях этих подключений, планировать выполнение различных системных действий на основании данных аудита.

Модель аутентификации и авторизации методами веб-сервисов имеет высокую гибкость и позволяет разграничить полномочия различных внешних систем на формирование внутренних запросов к СЗкИД и, как следствие, на получение данных, хранящихся в информационной системе ГИБДД. Такая модель авторизации позволяет создать систему пользователей (соответствующих определенным внешним объектам), каждый из которых будет обладать лишь необходимым набором полномочий и установить соответствие пользователей различным Внешним объектам.

Таким образом, предлагаемая модель логического шлюзования позволяет обеспечить полное системное разграничение взаимодействующих информационных подсистем и ограничить возможность прохождения запросов и ответов на них набором заданных правил соответствия валидности и безопасности.

Пример использования механизма логического шлюзования приведён в описание предполагаемой схемы взаимодействия с сервисом информирования граждан о неоплаченных штрафах в разделе 7.1.

4.2. Сетевой уровень

Для защиты от несанкционированного доступа к данным сервер шлюзования информационных систем должен быть оборудован межсетевыми экраноми. Один межсетевой экран должен обеспечивать фильтрацию данных получаемых Системой от Внешних объектов, другой — получаемых СЗкИД от Шлюза.

Межсетевой экран должен пропускать только разрешенный траффик, иметь встроенную защиту от сканирования портов и анализатор сетевых атак.

Удаленное управление межсетевым экраном должно осуществляться только по защищенным протоколам передачи данных (например, HTTPS).

4.3. Шифрование передаваемых данных

Для защиты передаваемых персональных необходимо использование сертифицированных ФСБ решений системы криптозащиты информации, например, на основе виртуальных частных сетей (VPN).

Весь передаваемый трафик между Внешними объектами и сервером шлюзования информационных систем, а так же между сервером шлюзования информационных систем и сервером приложение в этом случае шифруется.

Это обеспечивает гарантии целостности траффика, неизменности и сокрытия от третьих лиц, не дает возможности получить из него информацию о персональных данных в случае перехвата (например, недобросовестными сотрудниками провайдера).

Подробное описание предлагаемых модулей защиты данных в Системе находятся в Части III (разделы 11.4, 11.5).

5. Дополнительные мероприятия по повышению отказоустойчивости и доступности работы сервисов системы

Для составления мероприятий по повышению отказоустойчивости и доступности сервисов системы необходимо рассмотреть систему как совокупность «точек сбоя» («single point of failure») – то есть элементов, ошибка в работе которых приведет к останову всей системы. Такие элементы сведены в таблицу 2.

Таблица 2. Точки сбоя системы.

№п/п	Наименование
1	Внешний объект
2	Канал связи Хостинга с Шлюзом
3	Шлюз
4	ОС Шлюза
5	Сервис шлюза
6	Канал связи Шлюза с Сервером XML
7	Сервер XML
8	ОС сервера XML
9	Служба сервера XML
10	Канал связи сервера XML с сервером базы данных
11	Сервер базы данных
12	Подсистема хранения сервера БД
13	ОС сервера БД
14	СУБД

Таким образом, среди точек сбоя системы можно выделить несколько групп: аппаратное обеспечение серверов, каналы связи, программное обеспечение серверов.

Под каналами связи следует понимать – сетевые интерфейсы серверов, среды передачи данных (линии связи), коммутационное оборудование.

Выделим ряд возможных причин отказа в работе групп точек сбоя системы:

1. Выход из строя аппаратного обеспечения серверов.
    1.1 Выход из строя вычислительной части оборудования
    1.2 Выход из строя подсистем хранения данных
2. Выход их строя каналов связи.
    2.1 Нарушение линий связи
    2.2 Прекращение работы сетевых интерфейсов

2.3 Выход из строя коммутационного оборудования

3. Отказ в работе ОС и программного обеспечения серверов.

3.1 Повреждение ОС.

3.2 Прекращение работы сервисов.

Существуют следующие методы повышения доступности вычислительных систем:

Дублирование – создание избыточности в количестве критических элементов системы, обеспечивающее быструю замену выходящих из строя элементов.

Наращивание вычислительных мощностей (увеличение оперативной памяти серверов, повышение пропускной способности каналов связи) - для увеличения доступности при большой нагрузке.

Виртуализация – работа операционной системы и сервисов на «виртуальной машине».

Установка дополнительного оборудования – оснащение системы оборудованием, целевым назначением которого является повышение отказоустойчивости.

Дублирование вычислительной части аппаратного обеспечения серверов может быть реализовано при помощи кластеризации.

Кластерные системы традиционно рассматриваются в качестве альтернативы большим и дорогим компьютерам. Преимущества кластеров над большими ЭВМ исходят из самой идеи объединения вычислительных мощностей множества независимых компьютеров в единую систему для решения одной задачи. Кластеры позволяют преодолеть физические ограничения одиночных компьютеров, используя эти компьютеры в качестве «кирпичиков» для построения системы требуемой вычислительной мощности. Объединение недорогих стандартных 2-х или 4-х процессорных компьютеров в кластерную систему дает ощутимый экономический эффект.

В кластере, как правило, каждый узел может выполнять любые задачи, выполняемые любым другим узлом, – такая взаимозаменяемость обеспечивает защиту от системных, аппаратных и программных сбоев. Выход из строя какого-либо из компьютеров не приводит к остановке системы – работа будет продолжена на оставшихся узлах.

Кластеризация сервера базы данных осуществляется при помощи технологии Oracle Real Application Clusters (RAC), которая позволяет системе управления базами данных (СУБД) Oracle выполнять любые приложения на кластере независимых серверов, объединяя их процессорную мощность для обеспечения отказоустойчивости, линейной масштабируемости, высокой доступности и готовности.

Решение задач повышения отказоустойчивости и доступности Внешних объектов лежит на организациях, их эксплуатирующих.

В случае, когда Внешним объектом по отношению к системе является сервер приложений информирования граждан о наличии неоплаченных штрафов при помощи типового сайта областного ГИБДД (Хостинг), повышение его отказоустойчивости и доступности также рекомендуется производить в соответствии с концепциями, изложенными в данном разделе. Существует возможность кластеризации серверов приложений (таких как Хостинг), эта возможность поддерживается в сервере приложений GlassFish, начиная с версии 2.0, а также в серверах приложений WebLogic.

Общие характеристики кластерных систем.

1. Высокая степень готовности системы.

Выход из строя одного сервера или его программного обеспечения не должен приводит к выходу из строя всей системы в целом. При сбое в узле база данных остается открытой, и приложения продолжают иметь доступ к данным через другие работающие узлы и экземпляры.

2. Масштабируемость.

По мере возрастания требований к ресурсам увеличение мощности всей системы в целом производится за счет замены устаревшего узла, либо добавлением в кластер нового сервера. Замена или добавление новых серверов в кластер не должно вызывать прерывания в обслуживании, а новые мощности должны быть готовы к использованию сразу после их подключения.

3. Непрерывность (бесперебойность) функционирования.

Непрерывное функционирование, как при сбоях, так и при выполнении запланированных сервисных работ. Большинство сервисных должно быть выполнено без остановки в обслуживании и прозрачно для пользователя либо выполняться на узлах кластера поочередно.

Дублирование подсистемы хранения данных сервера БД обеспечивается использованием дискового массива хранения данных с применением технологии RAID 60.

Дисковый массив, основанный на технологии RAID 60 представляет собой чередование (RAID 0) записи на два массива RAID 6. RAID 6 в свою очередь представляет из себя массив минимум из четырёх дисков, при этом под контрольные суммы выделяется ёмкость 2-х дисков, рассчитываются 2 суммы по разным алгоритмам. Таким образом, технологией RAID 60 обеспечивается защита при одновременном выходе из строя до двух дисков включительно в каждой из RAID 0 групп.

Аналогично, но с применением менее затратных технологий RAID (использующих меньшее количество дисков, например RAID 1) может быть организовано повышение отказоустойчивости подсистемы хранения данных серверов приложений.

Повышение отказоустойчивости каналов связи может быть осуществлено при помощи прокладки дублирующих линий связи с объединением их в транк. При этом обеспечивается одновременная передача данных по всем объединенным в транк средам передачи. И если в одной из линий происходит обрыв, то это никак не сказывается на доступности остальных линий.

Технология виртуализации представляет собой организацию работы серверов приложений в среде виртуальной машины, что позволяет абстрагироваться от конкретных аппаратных и программных конфигураций.

Этот способ позволяет сократить время восстановления как после критического сбоя операционной системы, так и после сбоя оборудования до минимума.

Время восстановления после критического сбоя операционной системы сокращается за счет восстановления образа рабочей операционной системы из так называемого «снимка» («snapshot»).

Время восстановления после критического сбоя оборудования сокращается за счет возможности разворачивания сервера на конфигурации аппаратного обеспечения, отличной от конфигурации, вышедшей из строя.

Однако, технология виртуализации имеет свои недостатки:

1. Необходимо дополнительное место для хранения снимков.
2. Меньшая производительность в среде виртуальной машины вследствие потребления ресурсов гостевой операционной системой.

Поэтому внедрение технологий виртуализации требует проведение дополнительного анализа и оценки повышения эффективности перед внедрением.

Установка дополнительного оборудования представляет собой дополнение системы такими устройствами как Источники Бесперебойного Питания, которые позволяют осуществить корректное завершение работы серверов, необходимое для избежания потери данных, в случае долгосрочного отключения электроэнергии, либо работу серверов и коммутационного оборудования от аккумуляторов ИБП в случае краткосрочного отключения электроэнергии.

Таким образом, такие решения как кластеризация, организация RAID-массивов и создание транков являются вариантом наращивания вычислительных мощностей методом дублирования.

Возможно также применение таких технологий как кластеризация виртуальных машин (например, на основе Microsoft HyperV), объединяющая в себе положительные стороны обоих этих методов.

Часть II. Направления использования Системы

6. Взаимодействие с ОАСУ РПО ФГУП «Почта России»

Информационное взаимодействие с ОАСУ РПО ФГУП «Почта России» осуществляется с целью контроля прохождения почтовый отправлений формируемых подразделениями ГИБДД и корректного применения дат административного и исполнительного производства.

Постановления по делам об административных правонарушениях, возбужденных в связи с выявлением нарушения ПДД средствами фото-видео фиксации нарушений ПДД, работающими в автоматизированном режиме, направляются подразделением ГИБДД собственнику транспортного средства почтовым отправлением ФГУП «Почта России».

Уникальным идентификатором почтового отправления является специализированный код ФГУП «Почты России» (бар-код). Бар-код присваивается каждому сформированному почтовому отправлению подсистемой ГИБДД в автоматизированном режиме.

С целью определения состояния конкретного почтового отправления подсистема ГИБДД формирует запрос в ОАСУ РПО, содержащий бар-код интересующего почтового отправления, уникальный идентификатор запроса, состоящий из кода, описывающего запрос как запрос к ОАСУ РПО, его уникального номера.

Подсистема ГИБДД направляет запрос специализированному web-сервису Системы.

Специализированный web-сервис, на основе уникального идентификатора запроса определят адресата запроса, исключает из состава запроса уникальный идентификатор (приводит формат запроса к формату регламента информационного взаимодействия с ОАСУ РПО), направляет запрос в ОАСУ РПО. Однозначное определение запроса после удаления уникального идентификатора осуществляется с использованием бар-кода.

Система, через заданные промежутки времени, опрашивает ОАСУ РПО о готовности ответа на запрос с заданным бар-кодом. По готовности ответа (сообщения об ошибке) Система получает ответ, направляет его соответствующей службе подсистемы ГИБДД.

Подсистема ГИБДД получает ответ, сохраняет статус состояния почтового отправления для принятия дальнейших решений.

7. Взаимодействие с сервисами информирования граждан о наличии неоплаченных штрафов

7.1. Описание взаимодействия с типовым сайтом областного ГИБДД

При взаимодействии с сервисом информирования граждан при помощи типового сайта областного ГИБДД внешним объектом по отношению к Шлюзу становится система, состоящая из сервера приложений «Хостинг» и Пользователей (граждан), подключающихся к нему посредством сети Интернет (Рисунок 6).

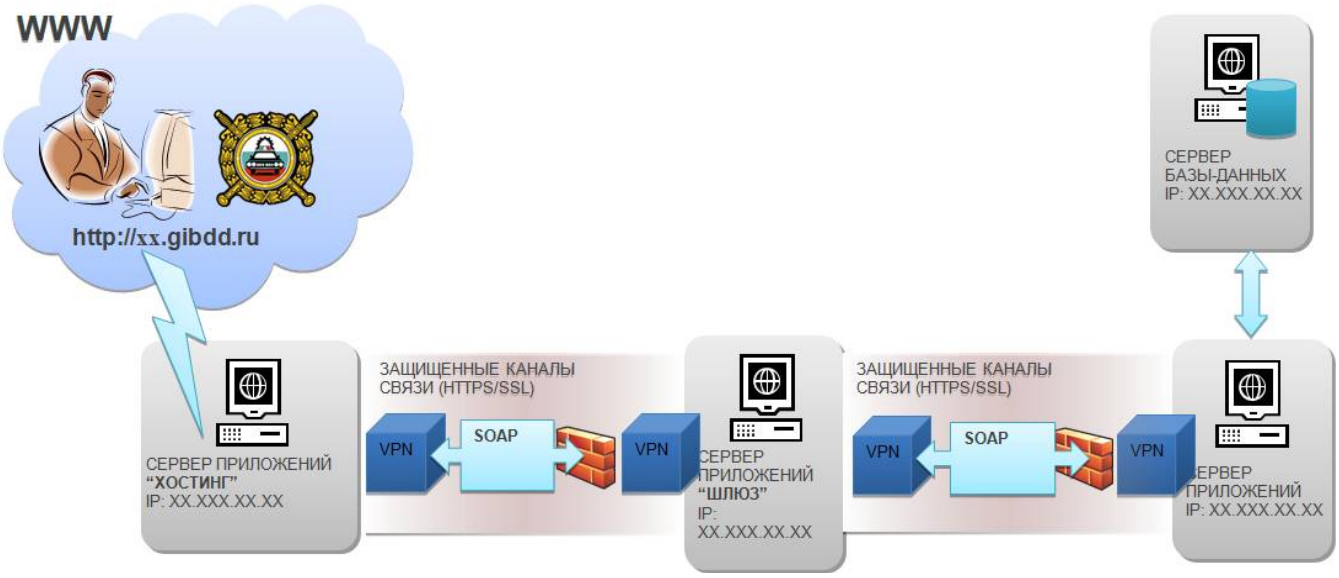


Рисунок 6. Схема системы информирования граждан при помощи типового сайта областного ГИБДД

1. Пользователь при помощи какого либо устройства, позволяющего осуществлять подключение к сети Интернет и просмотр веб-сайтов (персональный компьютер, коммуникатор, смартфон) осуществляет в веб-браузере устройства переход на страницу сайта областного ГИБДД (например, введя в адресную строку браузера «64.gibdd.ru»).
2. Хостинг, на котором размещается этот сайт, предоставляет веб-браузеру пользователя страницу, на которой имеется ссылка «Просмотр неоплаченных штрафов».
3. Пользователь, осуществляя переход по указанной ссылке попадает на страницу выбора типа запроса (по номеру водительского удостоверения и фамилии, имени, отчетсва, по номеру свидетельства о регистрации и государственному регистрационному знаку автомобиля или по номеру протокола (постановления)). Выбрав тип запроса, пользователь вводит исходные данные (реквизиты запроса).
4. Хостинг, выполнив ряд первичных проверок данных, введенных пользователем (например, фамилия, имя должны состоять только из букв русского алфавита), формирует специальный запрос к Шлюзу.
5. Шлюз выполняет следующие проверки:

- запрос данных осуществляется пользователем или автоматическим алгоритмом (на основании частоты запросов с одного адреса, результате прохождения теста Тьюринга);
- заполнены ли все поля, соответствуют ли они шаблонам.

Если эти проверки успешно пройдены, формируется запрос к СЗкИД;

6. СЗкИД, получив запрос от Шлюза, выполняет запрос к хранимым процедурам Сервера БД.
7. Сервер БД отвечает на запрос СЗкИД выводом данных в табличном формате.
8. СЗкИД, получая от Сервера БД табличные данные, преобразовывает их в формат сообщений и передает на Шлюз.
9. Шлюз преобразовывает эти сообщения в формат, понятный Хостингу и отправляет их.
10. Хостинг в свою очередь преобразовывает данные, получаемые от Шлюза в Интернет страницу, которую способен отобразить веб-браузер устройства пользователя.
11. Веб-браузер устройства пользователя выводит на экран следующие данные:
    - дата нарушения;
    - место нарушения;
    - статья;
    - сумма штрафа;
    - описание нарушения;
    - номер постановления;
    - дата вступления постановления в законную силу;
    - подразделение, принявшее решение о назначении наказания за совершение административного правонарушения;
    - информация о способах оплаты.

Предлагаемый набор данных является примерным. Реальный набор данных должен быть определен на этапе согласования проекта внедрения системы информирования.

Подробное описание логики взаимодействия, её программной реализации и пользовательских интерфейсов находятся в Части III.

7.2. Описание взаимодействия с информационными киосками

При взаимодействии с сервисом информирования граждан при помощи информационных киосков, внешним объектом по отношению к Шлюзу может являться как специальный сервер взаимодействия с информационными киосками, так и каждый единичный киоск, в зависимости от выбора схемы реализации.

Алгоритм получения информации при использовании информационных киосков аналогичен таковому для сайта. Но помимо функции информирования, информационный киоск, расширенный набором устройств для приема платежей дает удобный и доступный способ оплаты взысканий (штрафов) по административным нарушениям непосредственно после получения информации о них.

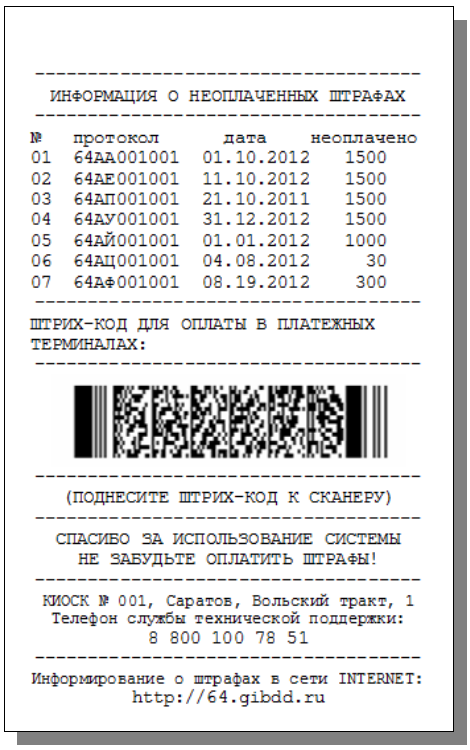
Такой способ оплаты обладает рядом ключевых преимуществ перед

традиционными средствами и способами оплаты штрафов (используемыми платежными системами на данный момент):

- нет необходимости иметь при себе постановления-квитанции (протоколы), достаточно данных с документов, которые водители, как правило, постоянно имеют при себе;
- не нужно вводить реквизиты платежей (ошибки при вводе этих данных зачастую приводят к тому, что платеж может быть проведен по некорректным реквизитам, следовательно штраф так и останется неоплаченным), все эти данные хранятся в системе;
- оперативное обновление статусов платежей («Не оплачен», «В оплате», «Платеж проведен») в базе данныхподсистемы «АдмПрактика», что является основой исключения возможности необоснованного привлечения к ответственности за неоплату административного штрафа в срок;
- поддержка сканирования двумерных штрих-кодов водительских удостоверений нового образца;
- оформление SMS и/или e-mail подписки.

Информационный киоск, не оборудованный набором устройств для приема платежей, тем не менее имеет функцию вывода на печать информации о выбранных неоплаченных штрафах. Помимо номеров постановлений (протоколов), дат их оформления и сумм, которые необходимо оплатить, на печатную форму помещается также унифицированный штрих-код, при помощи которого возможно произвести оплату постановлений, номера которых размещены на печатной форме в ближайшем платежном терминале, оборудованном сканером штрих-кодов.

Пример печатной формы представлен на рисунке 7.



ИНФОРМАЦИЯ О НЕОПЛАЧЕННЫХ ШТРАФАХ

№	протокол	дата	неоплачено
01	64АА001001	01.10.2012	1500
02	64АЕ001001	11.10.2012	1500
03	64АП001001	21.10.2011	1500
04	64АУ001001	31.12.2012	1500
05	64АЙ001001	01.01.2012	1000
06	64АЦ001001	04.08.2012	30
07	64АФ001001	08.19.2012	300

ШТРИХ-КОД ДЛЯ ОПЛАТЫ В ПЛАТЕЖНЫХ ТЕРМИНАЛАХ:

(ПОДНЕСИТЕ ШТРИХ-КОД К СКАНЕРУ)

СПАСИБО ЗА ИСПОЛЬЗОВАНИЕ СИСТЕМЫ
НЕ ЗАБУДЬТЕ ОПЛАТИТЬ ШТРАФЫ!

КИОСК № 001, Саратов, Вольский тракт, 1
Телефон службы технической поддержки:
8 800 100 78 51

Информирование о штрафах в сети INTERNET:
http://64.gibdd.ru

Рисунок 7. Пример печатной формы информационного киоска

7.3. Описание взаимодействия с системами уведомления

В рамках реализации проекта системы информирования можно выделить ряд событий, при наступлении которых могут быть инициированы уведомления. Доведение уведомлений до сведения граждан предлагается осуществлять по средствам систем уведомлений. Такими событиям могут быть:

- оформление постановлений ЦАФАП;
- вступление постановлений об административном правонарушении в законную силу (в случае отсутствия опротестования);
- изменение статуса оплаты штрафа;
- приближение окончания допустимого срока оплаты;
- факт передачи постановления ФССП (по окончанию допустимого срока оплаты).

Отправка уведомлений осуществляется с согласия Пользователя и по электронному адресу (номеру телефона), указанному им при использовании системы. Для получения уведомлений Пользователю необходимо будет подписаться на услугу по предоставлению ему сведений об изменении состояния дел административного производства, возбужденных на его имя.

В таком случае, система уведомления формирует и направляет соответствующей службе подсистемы ГИБДД запрос, содержащий уникальные идентификаторы водителя и запроса. Подсистема ГИБДД, по уникальному идентификатору водителя, обеспечивает формирование и направление системе уведомления информации об изменениях статуса административных правонарушений, допущенных водителем.

К средствам связи для отправки уведомлений относятся:

- письмо по электронной почте;
- sms-сообщение;
- интерфейс личного кабинета системы информирования.

Возможна комбинация различных средств уведомления. Например, в случае фотовидеофиксации факта административного правонарушения, пользователю последовательно отправляется следующее:

- sms или email уведомление о факте фотовидефиксации нарушения, совершенного с использованием транспортного средства, принадлежащего Пользователю;
- постановление-квитанция заказным письмом;
- sms или email уведомление о вступлении постановления в законную силу (в случае отсутствия опротестования);
- sms или email уведомление о приближении окончания допустимого срока оплаты штрафа;
- sms или email уведомление об изменении статуса платежа (после оплаты);
- уведомление о передаче дела ФССП (в случае отсутствия оплаты).

8. Взаимодействие с системами предварительной записи и подготовки данных

Данный тип взаимодействия рассмотрен вследствие необходимости автоматизации и информатизации оказания гражданам услуг по предварительной записи и подготовке данных.

Взаимодействие предполагает ускоренную подготовку документов-заявлений на совершение регистрационных действий путем применения сторонних зарегистрированных Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) сервисов.

Технология ускоренной подготовки основывается на отсутствии необходимости вносить в сервис, используемый Пользователем, полного набора значений всех, необходимых для подачи заявления, реквизитов.

В качестве примера, в таблицу 3 сведен полный набор данных, необходимых для совершения регистрационного действия с транспортным средством.

Таблица 3. Перечень реквизитов, необходимых для совершения регистрационного действия с транспортным средством.

№ п/п	Наименование
1	Адрес места жительства
2	Тип заявителя (собственник или представитель собственника)
3	Фамилия собственника (представителя)
4	Имя собственника (представителя)
5	Отчество собственника (представителя)
6	Дата рождения собственника (представителя)
7	Тип документа, удостоверяющего личность
8	Номер документа, удостоверяющего личность
9	Гражданство
10	Телефонный номер
11	Тип регистрационной операции
12	Вносится ли изменение в текущий ПТС или требуется выдать новый
13	Номер государственного регистрационного знака ТС
14	В отношении какого объекта осуществляется регистрационная операция (автомобиль/ автобус/ прицеп/ прочие ТС)
15	Год выпуска ТС
16	VIN ТС
17	Марка ТС
18	Модель ТС
19	Тип двигателя
20	Категория ТС
21	Фотокопии документов*
*по желанию Пользователя	

Определенный набор данных является ключевым. При помощи запроса, содержащего ключевые данные, Внешний объект запрашивает у Системы остальную информацию.

Набор ключевых реквизитов вариативный и определяется на стадии проработки проекта подключения систем предварительной записи и подготовки данных.

Сервис предварительной записи также работает в режиме двунаправленного обмена данными через Систему и предполагает получение следующих данных от Пользователя (помимо указанных в таблице 3):

1. Место совершения регистрационного действия.
2. Дата и время совершения регистрационного действия.

При этом осуществление предварительной записи может производиться по следующему алгоритму:

1. От Пользователя на соответствующий сервис системы поступает запрос, содержащий ключевой набор данных, место совершения и предпочитаемый диапазон дат совершения регистрационного действия.
2. Сервис проверяет данные, указанные Пользователем и в случае, если они корректны, формирует ответ, содержащий остальные данные (не ключевые) и таблицу с информацией о наличии, либо отсутствии свободного времени для записи на совершение регистрационного действия в указанном диапазоне дат.
3. Пользователь проверят полученные от Системы данные, при необходимости вносит корректировки и выбирает удобное для него время совершения регистрационного действия согласно полученному расписанию. Эти данные передаются в Систему и хранятся в ней.
4. Инспектор, пользуясь специальным интерфейсом, осуществляет проверку данных и выносит предварительное заключение об одобрении, либо отклонении запрашиваемого Пользователем регистрационного действия.

При необходимости, возможна организация оповещения пользователей о таких событиях как вынесение предварительного заключения Гос. Инспектором, напоминание о приближении даты (времени), на которое записан пользователь, либо причина отказа от выполнения указанного действия в желаемое Пользователем время, например посредством электронной почты. Более полный перечень предполагаемых сообщений системы уведомления Пользователей приведен в соответствующей главе «Взаимодействие с ОАСУ РПО ФГУП «Почта России».

9. Взаимодействие с сервисом поиска собственника АМТС

9.1. Концепция сервиса поиска собственника

Один из перспективных направлений мировой практики использования современных информационных технологий в сфере регулирования и обеспечения безопасности дорожного движения является разработка систем, функционирование которых направлено на установление собственника транспортного средства и отправки ему информационного сообщения. Развитие этого направления обусловлено требованиями к повышению ответственности владельцев транспортных средств, оставленных ими с нарушением действующих ПДД, т.е. ненадлежащим образом припаркованным на проезжей части, находящимся в местах, либо в местах, где планируется проведение различных работ (монтаж, демонтаж бордюров, ремонт асфальтового покрытия, уборка снега и льда), либо культурно-массовых мероприятий.

Таким образом, возможна попытка устранения причины нарушения до вызова службы эвакуации путём оповещения собственника АМТС.

Одновременно с этим, функционирование таких систем должно гарантировано не допускать не только утечек персональной информации, но и нарушения конституционных прав человека и гражданина в отношении сведений, затрагивающих его личную жизнь.

Эффективное, а главное, соответствующее указанным в предыдущем абзаце требованиям, создание такой системы также возможно произвести с использованием технологии Шлюзования, предложенной в данном проекте.

Концепция такой системы с применением технологии Шлюзования представлена на рисунке 8.

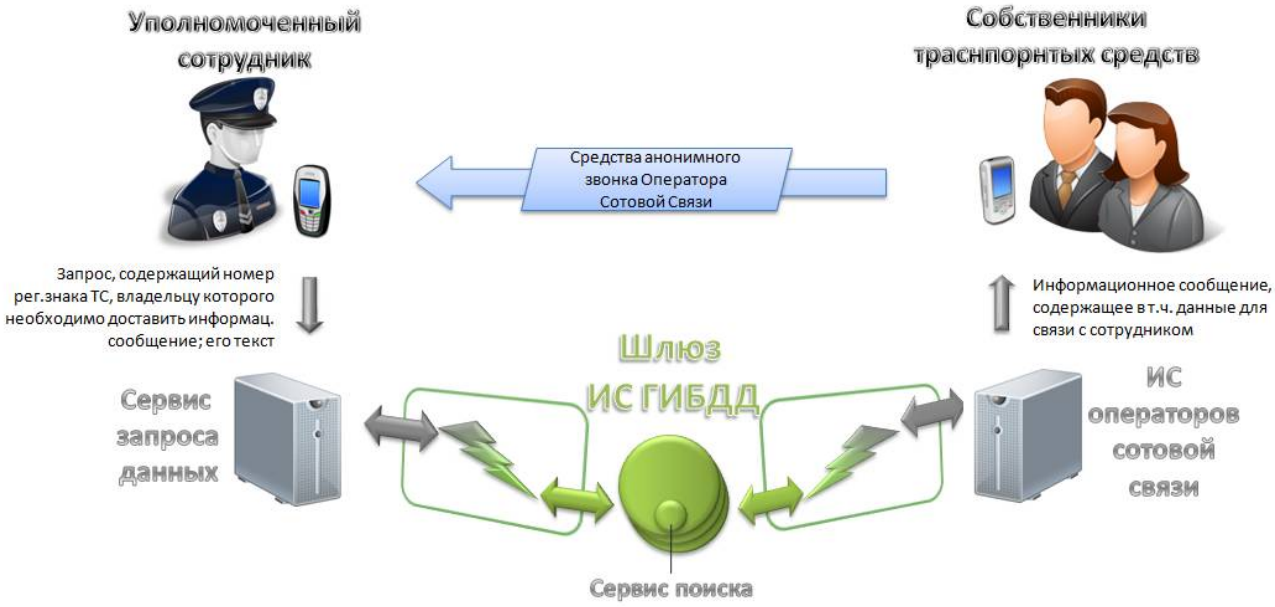


Рисунок 8. Концепция системы поиска собственника

Уполномоченный сотрудник в специальном приложении (либо посредством

определенным образом форматированного sms-сообщения) формирует запрос собственнику транспортного средства и отправляет это сообщение на сервис запросов. Сервис запросов осуществляет ряд первичных проверок поступившей информации и отправляет данные о запросе поиска владельца на Шлюз. Шлюз, выполнив анализ, проверки и рекомбинацию запроса, передает данные внутреннему сервису поиска владельца. Сервис поиска подключается к базе данных АМТС и осуществляет поиск данных о собственнике. Эти данные передаются на Шлюз для последующей их отправки специальному сервису операторов сотовой связи. Если в ИС операторов по указанным данным найден номер мобильного телефона, то этот сервис формирует sms-сообщение и отправляет его на найденный номер. Таким образом, собственник транспортного средства получает информационное сообщение, и, в случае необходимости, может связаться с Уполномоченным сотрудником по находящимся в сообщении реквизитам, в том числе с использованием средств анонимизации вызывающего абонента.

9.2. Информационные потоки сервиса поиска

Наиболее важным аспектом проектирования данной системы является составление корректной схемы информационных потоков. Именно на этом этапе осуществляется планирование состава передаваемых на каждом этапе реквизитов. Для каждого этапа передачи этот состав должен быть необходимым и достаточным для функционирования системы, при этот состав этих данных должен быть минимален, то есть получение узлами системы избыточных данных, не связанных непосредственно с их функционированием, должно быть исключено.

В рамках данного проекта предлагается, представленная на рисунке 9 предварительная схема информационных потоков, основанная на концепции, изложенной в предыдущем разделе.

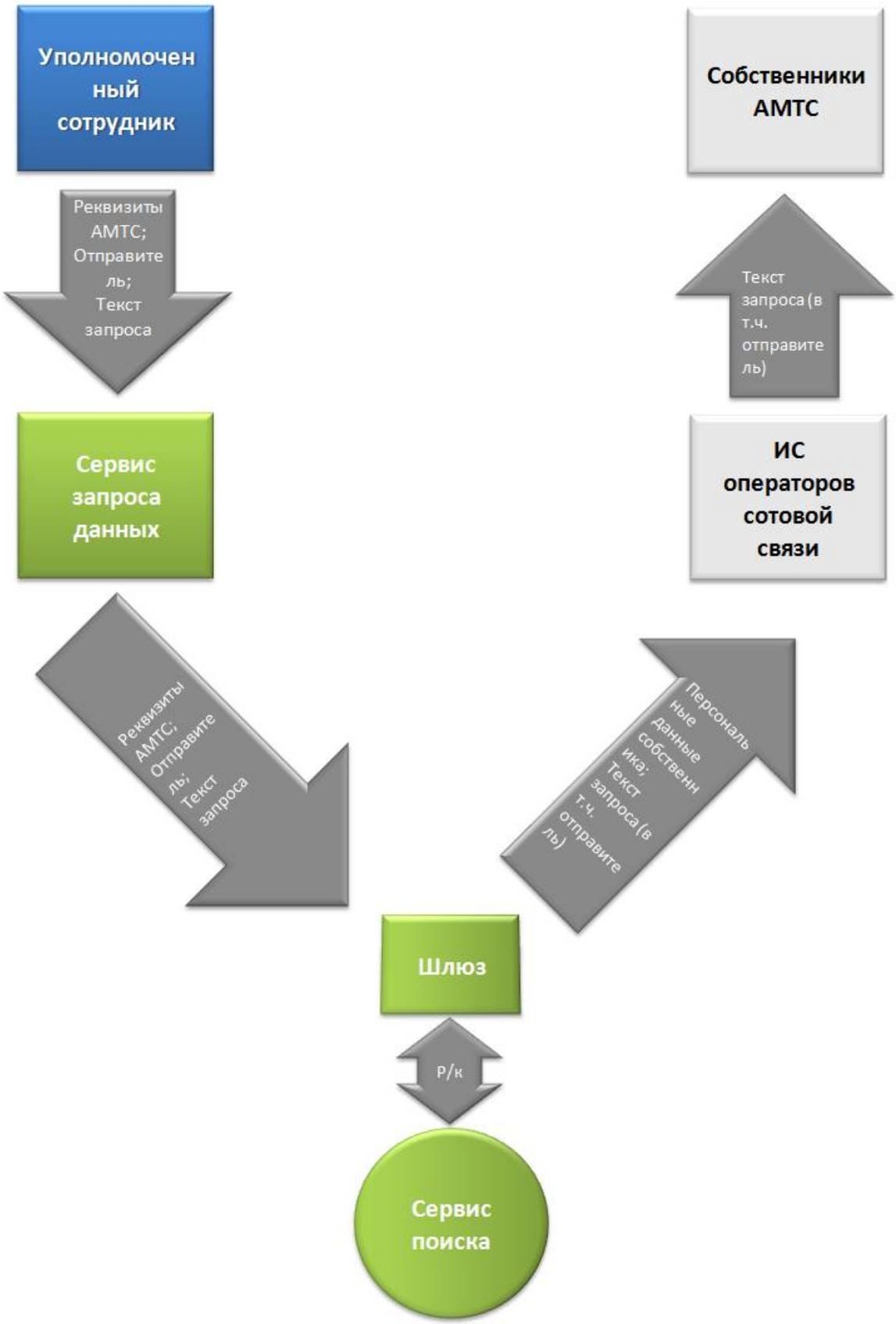


Рисунок 9. Концепция системы поиска собственника (На рис. «Р/к» — рекомбинированные запросы)

Уполномоченный сотрудник в специальном приложении (либо посредством определенным образом форматированного sms-сообщения) формирует запрос собственнику транспортного средства и отправляет это сообщение на сервис запросов.

Таким образом, от сотрудника к сервису запросов передаются следующие данные:

1. Номер государственного регистрационного знака АМТС, по которому производится запрос.
2. Текст информационного сообщения.
3. Обратные координаты связи с сотрудником.

Пример sms-сообщения сервису:

На номер: +79010010101

Текст сообщения:

А001АА34 /Т/ В зоне, где припаркован Ваш автомобиль планируется проведение общественных мероприятий. Во избежании принудительной эвакуации, просим до 13:00 убрать автомобиль из указанной зоны. /П/ Гос.инспектор Крылов А.А. ГАИ г.Фролово, контактный тел. 3-12-34, 8-902-123-45-67.

Сервис запросов осуществляет ряд первичных проверок поступившей информации и отправляет данные о запросе поиска владельца на Шлюз.

К таким проверкам могут относиться:

1. Соответствие номера отправителя запроса списку допустимых номеров отправителей.
2. Соответствие номера государственного регистрационного знака или иных реквизитов АМТС шаблонам, хранящимся в сервисе запросов.
3. Прочие проверки.

В случае, если отправка запроса осуществлялась не с помощью специального приложения, а путём отправки sms-сообщения, сервис дополнительно производит его разбор (т. н. «парсинг»).

Помимо указанного, сервис запросов может осуществлять дополнительный (основной осуществляется Шлюзом) аудит запросов.

Шлюз, выполнив анализ, проверки и рекомбинацию запроса, передает данные внутреннему сервису поиска владельца.

Шлюз выполняет своё функциональное назначение в соответствии с указанным в первой части настоящего документа алгоритмом. На сервис поиска передается следующая информация:

1. Реквизиты АМТС (номер государственного регистрационного знака, или иные).
2. Текст запроса.

Сервис поиска подключается к базе данных АМТС и осуществляет поиск данных о собственнике. Эти данные передаются на Шлюз для последующей их отправки специальному сервису операторов сотовой связи.

По указанным реквизитам АМТС определяется собственник. Данные о собственнике, совместно с текстом запроса отправляются на Шлюз и передаются специальному сервису (сервисам) оператора (операторов) сотовой связи. Реквизиты АМТС в данном запросе не содержатся, либо частично скрыты.

Если в ИС операторов по указанным данным найден номер мобильного телефона, то этот сервис формирует sms-сообщение и отправляет его на

найденный номер. Таким образом, собственник транспортного средства получает информационное сообщение, и, в случае необходимости, может связаться с Уполномоченным сотрудником по находящимся в сообщении реквизитам, в том числе с использованием средств анонимизации вызывающего абонента.

Пример sms-сообщения собственнику:

От: СервисИнформированияСобственниковАМТС

Текст сообщения:

Запрос на автомобиль (н/з *001***4) «В зоне, где припаркован Ваш автомобиль планируется проведение общественных мероприятий. Во избежании принудительной эвакуации, просим до 13:00 убрать автомобиль из указанной зоны». ОТ «Гос.инспектор Крылов А.А. ГАИ г.Фролово, контактный тел. 3-12-34, 8-902-123-45-67». Вы можете воспользоваться услугой анонимного вызова. Информация об услуге *111#.

Преимущества указанной схемы информационных потоков:

1. Обмен ограниченными наборами данных обеспечивает минимизацию ущерба в случае их утечки:
2. Циркуляция информации, содержащей персональные данные, осуществляется только в ИС ГИБДД и ИС операторов сотовой связи.
3. В ИС операторов сотовой связи передаются только данные о владельце, данные о ТС не передаются, либо передаются частично скрытыми (достаточно для идентификации собственником АМТС определенного транспортно средства, но недостаточно для использования в корыстных целях в случае утечки данных от оператора сотовой связи).
4. Персональные данные о собственнике транспортного средства, а также номер мобильного телефона собственника, остается неизвестным даже для уполномоченного сотрудника, что исключает еще один возможный путь утечки персональных данных (все же в случае необходимости получения таких данных, сотрудник может воспользоваться иными сервисами системы, при наличии на это достаточных полномочий в этих сервисах).

При наличии таких жестких ограничений, возможна реализация сервисов, направленных на отправку запросов не только уполномоченными сотрудниками, но и любыми другими заинтересованными лицами, вплоть до рядовых граждан, однако, это требует дополнительной концептуальной проработки системы.

Часть III. Примеры использования Системы

Для демонстрации возможностей применения и практической реализации системы обращайтесь к компании-разработчику - ООО НПО «РэйнбовСофт».

Список использованных сокращений

HTTPS	Hypertext Transfer Protocol Secure (Безопасный протокол передачи гипертекстовых данных)
IP	Internet Protocol (Протокол сети Интернет)
QoS	Quality of Service (качество обслуживания) - показаталь соответствия качества связи ранее определенному
RAC	Real Application Cluster (программное обеспечение для кластеризации и повышения доступности для Oracle Database)
RAID	Redundant Array of Independent Disks (избыточный массив независимых жёстких дисков)
SMS	Short Message Service (сервис коротких сообщений)
SNMP	Simple Network Transfer Protocol (простой протокол сетевого управления)
SOAP	Simple Object Access Protocol (простой протокол доступа к объектам)
SQL	Structured Query Language (язык структурированных запросов)
SSH	Secure SHell (безопасная оболочка)
SSL	Secure Sockets Layer (уровень защищённых сокетов)
TCP	Transmission Control Protocol (протокол управления передачей)
VPN	Virtual Private Network (виртуальная частная сеть)

WSDL	Web Service Description Language (язык описания веб сервисов)
XML	eXtensible Markup Language (расширяемый язык разметки)
АМТС	Авто Мото Транспортные Средства
БД	База Данных
ГОСТ	ГОсударственный СТандарт
ГУ	Главное Управление
ИБП	Источник Бесперебойного Питания
ИС	Информационная Система
КоАП	Кодекс об Административных Правонарушениях
МВД	Министерство Внутренних Дел
МРЦ	МежРегиональный Центр
НПО	Научно-Производственная Организация
ОАО	Открытое Акционерное Общество
ОАСУ РПО	Общероссийской автоматизированной системы учета и контроля за прохождением регистрируемых почтовых отправлений
ОБДД	Обеспечение Безопасности Дорожного Движения
ООО	Общество с Ограниченной Ответственностью

ОС	Операционная Система
ПДД	Правила Дорожного Движения
ПС	Платежная Система
РФ	Российская Федерация
РПО	Регистрируемое Почтовое Отправление
СЗкИД	Сервер Запросов к Источникам Данных
СУБД	Система Управления Базой Данных
ТС	Транспортное Средство
ФГУП	Федеральное Государственное Унитарное Предприятие
ФК	Федеральный Клиент
ФКРФ	Федеральное Казначейство Российской Федерации
ФСБ	Федеральная Служба Безопасности
ФССП	Федеральная Служба Судебных Приставов
ФСТЭК	Федеральная Служба по Техническому и Экспортному Контролю
ЦАФАП	Центр Автоматизированной Фиксации Административных Правонарушений