ИНФОРМационная БЕЗОПАСНОСТЬ

Обеспечение информационной безопасности

при предоставлении государственных услуг в электронном виде на федеральном и региональном уровнях

ЗАО «Информационная внедренческая компания»
www.ivk.ru
Тел. (495) 221-65-80

Нормативная база

Государственные и муниципальные услуги

- **Федеральный закон от 27 июля 2010 г. №210-ФЗ** «Об организации предоставления государственных и муниципальных услуг»

в части безопасности должны соответствовать

- **Федеральный закон РФ от 27 июля 2006 года №152-ФЗ** «О персональных данных»;
- **Постановление Правительства РФ от 18.05.2009 №424** «Об особенностях подключения федеральных государственных информационных систем к информационно-телекоммуникационным сетям»;
- **Приказ ФСБ РФ N 416, ФСТЭК РФ от 31.08.2010 № 489** «Об утверждении Требований о защите информации, содержащейся в информационных системах общего пользования».

Вопросы, возникающие у гражданина РФ

Куда необходимо обратиться гражданину для получения государственных услуг в электронном виде?

Возможные варианты:

- средства портала Государственных услуг www.gosuslugi.ru
- разрозненные порталы и информационные системы федеральных ведомств и органов исполнительной власти

На региональном и муниципальном уровне вопрос получения региональных и муниципальных услуг остаётся не решённым

Архитектура предлагаемого подхода (1/2)

Информационная территориально-распределенная инфраструктура.

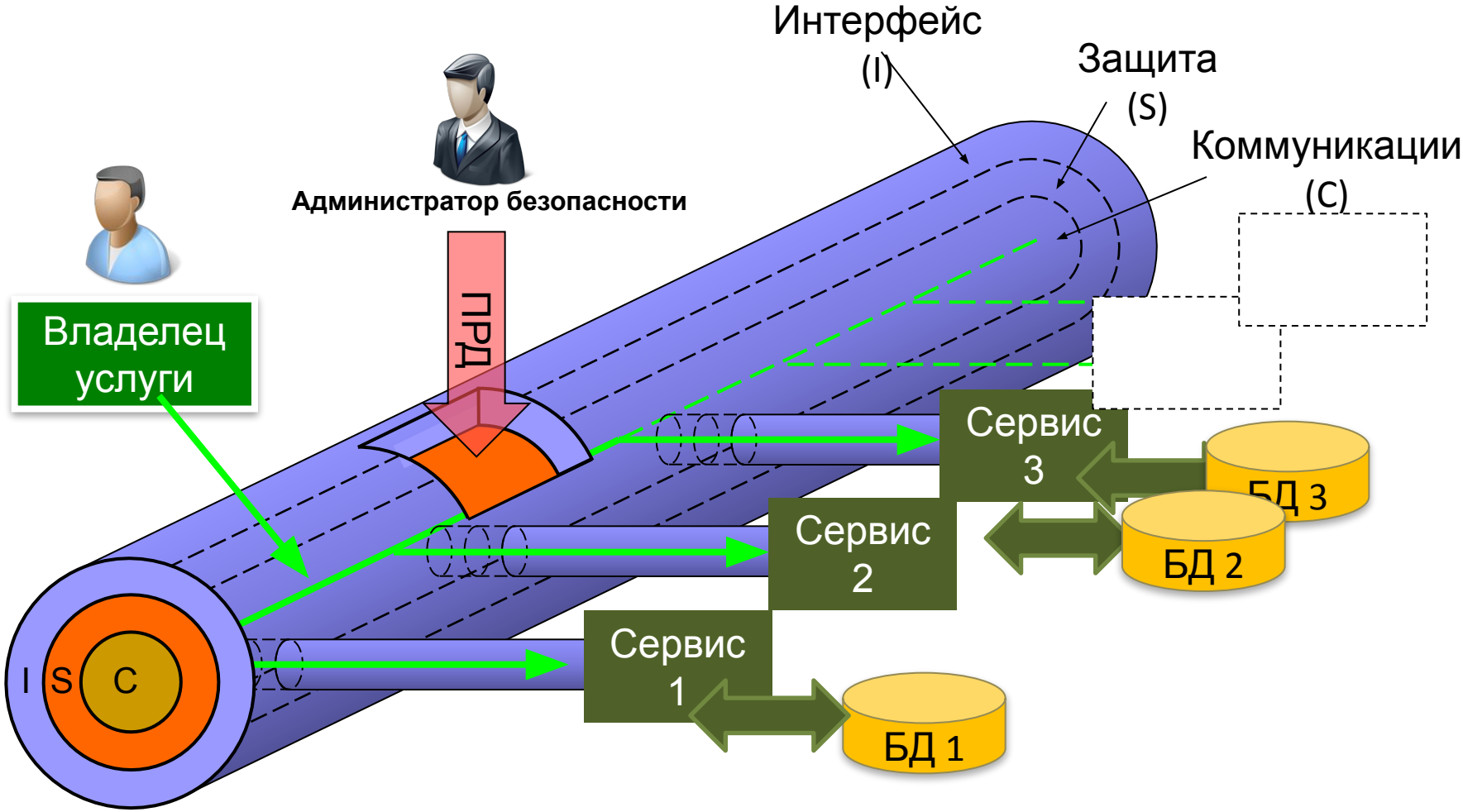
<u>При этом необходимо обеспечить</u>:

- Безопасность информации
- Доступность информации
- Гарантированное доведение информации

<u>Предлагаемые подходы</u>:

1) Распределённая сеть порталов, объединённых в единую защищённую портальную сеть.
2) Узлы находятся в крупных муниципальных образованиях.
3) Зоны ответственности - согласно географии территориального образования.
4) Механизм контроля исполнения запрошенных гражданами услуг.

Виртуальная транспортная магистраль (интеграционная шина)



Создание защищённой наложенной транспортной сети.

Архитектура предлагаемого подхода (2/2)

1. Использование средств защищённой асинхронной передачи данных в сети распределённых порталов.

Это позволит:

- обеспечить гарантированную доставку информации независимо от типов и качества используемых каналов связи.

2. Использование сервис-ориентированной архитектуры.

Это позволит:

- предоставить пользователю единую точку доступа ко всем услугам муниципальных порталов, входящих в региональную портальную сеть и получать доступ к личному кабинету.

- Данный подход не противоречит системн

Проблемы обеспечения безопасности

При получении гражданами РФ услуг в электронном виде, на наш взгляд, возникает три отличительные проблемы обеспечения безопасности информации:

1. Обеспечение гарантированного подтверждения получения согласия от пользователя в соответствии с 152-ФЗ.

2. Обеспечить конфиденциальность и целостность данных в процессе их передачи от клиента к серверу. Например, угрозы перехвата трафика с использованием сниферов или угрозы типа «человек посередине» (man in the middle).

3. Гарантии аутентичности (подлинности) пользователя, регистрирующегося на портале.

Предлагаемое решение обозначенных проблем

1. Процедура регистрации в соответствии с утверждённым регламентом.

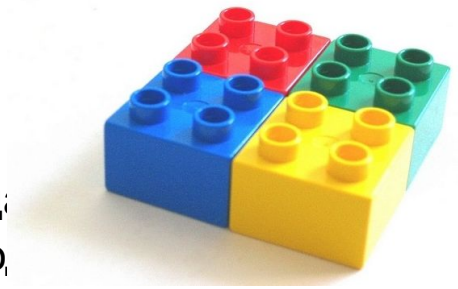
2. Персональные аутентификационные данные выдаются с обязательной проверкой документов при личной явке.

3. Аутентификация по персональному сертификату, с использованием устройств типа token или смарт-карт.

4. Пользователь использует защищённый протокол https, организуемый с помощью сертифицированных средств криптографической защиты информации, реализующих российские криптографические стандарты.

Конструктор услуг

Важным элементом Системы является Конструктор услуг.



1. Конструктор услуг позволяет «собирать» услугу из базовых элементов (шагов услуги) и далее их настраивать.

2. Шагом может быть страница для прикрепления файлов, ввода произвольных данных, вывода логического условия или вывод ознакомительной информации.

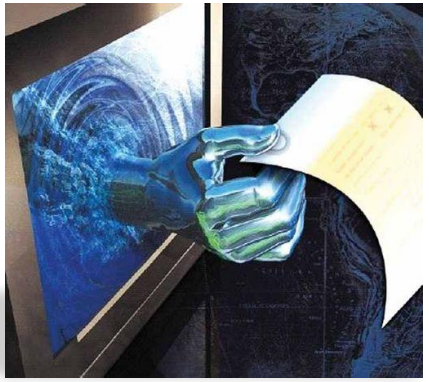
3. Автоматически к реализованной конструктором услуге создаётся административная часть для тонкой её настройки и модерации обращений граждан.

4. Решение о публикации созданной услуги принимает Главный Модератор, проверяющий соответствие услуги требованиям регламента.

5. Контроль категорий и объема собираемой информации (например, ПДн) в рамках оказания той или иной услуги гражданину РФ с целью недопущения несоответствия объемов собираемой информации и целей обработки данной информации при оказании услуги.

Контроль исполнения заявок на оказание услуг

При оказании услуг в электронном виде гражданам РФ обязательным является контроль исполнения полученных заявок ответственными лицами, в частности НЕОТКАЗУЕМОСТЬ принятия решения по данной заявке непосредственно чиновником.



Средствами достижения вышеуказанных требований является:

1. Применение технологии PKI (комплексная система, которая связывает открытые ключи с личностью пользователя посредством удостоверяющего центра (УЦ).
2. Механизм отслеживания изменения заявки.
3. Контроль сроков исполнения заявок на услуги.

Внедрение регионального СМЭВ

Для обеспечения:

- единого межпортального взаимодействия;
- взаимодействия порталов с информационными системами региональных ведомств (РСМЭВ),

должна быть реализована единая политика безопасности межобъектового взаимодействия,

это позволит использовать однотипные сертифицированные программно-технические решения по защите информации в разнородной гетерогенной среде.

При этом мы предлагаем внедрение региональной СМЭВ согласно руководящим документам.

Она соответствует стандартам и интерфейсам, используемым для взаимодействия с федеральной СМЭВ.

Защита сетевого периметра

В рамках реализации единой политики безопасности предлагается использовать классический подход к обеспечению защиты периметра сети и межсетевого взаимодействия с помощью таких средств как межсетевое экранирование и средства обнаружения вторжений.

ИВК ПОРТАЛ. Электронный муниципалитет

- Распределённая защищённая информационная система, позволяющая организовать процесс оказания услуг на региональном и муниципальном уровне.

ПО «ИВК ПОРТАЛ» – система поддержки и управления распределёнными Web-приложениями и информационными ресурсами.
Организация логики и интерфейса решения.

ПО «ИВК ЮПИТЕР» – унифицированные программные средства организации, контроля и управления вычислительным процессом в неоднородных вычислительных сетях в защищенном исполнении.
Транспортная магистраль защищённого гарантированного обмена данными.

ПО «ИВК БюрократЪ» – система защищенного электронного документооборота.
Контроль исполнения заявок граждан.

ПО «ИВК КОЛЬЧУГА» – Межсетевой экран с расширенной функциональностью. Защита серверного сетевого периметра.

ИВК ПОРТАЛ

Основные функции, реализуемые в комплексном решении:

- Предоставление пользовательских интерфейсов.
- Поддержка процесса оказания услуг в электронном виде.
- Обеспечение взаимодействия с гражданином, в части авторизации, приёма и выдачи информации.
- Создание услуг простыми графическими средствами.
- Обеспечение межведомственного и межуровнего взаимодействия.
- Обеспечение контроля и анализа исполнения заявок

ИВК ЮПИТЕР 5.0

Унифицированные программные средства организации, контроля и управления вычислительным процессом в неоднородных вычислительных сетях в защищенном исполнении «ИВК ЮПИТЕР» версии 5.0 – один из немногих российских продуктов, обеспечивающих функции интеграции на уровне данных и обмена сообщениями.

- Сертификация по требованиям ФСТЭК РФ и МО РФ,
- **3-й класс защищенности от НСД**,
- **2-й уровень контроля отсутствия НДВ**,
- обработка информации в АС до 1Б («сс»),
- наличие литеры «О1» (КД и ЭД)

«ИВК Юпитер™» - лауреат национальной премии ЗУБР-2006 и 2008 как «лучшая технология защищенной обработки информации»!

СЭД «ИВК БюрократЪ»

Защищенная система электронного документооборота «ИВК БЮРОКРАТЪ™» предназначена для решения задач организации единого защищенного информационного пространства в части электронного документооборота за счет применения единой технологии обработки и хранения документов.

- Контроль исполнения заявок граждан ответственными лицами реализуется средствами защищённого СЭД ПИ «ИВК БюрократЪ».
- Информация о поступившей заявке поступает непосредственно на рабочее место чиновника, ответственного за данную реализацию услуги в электронном виде.

Межсетевой экран «ИВК Кольчуга»

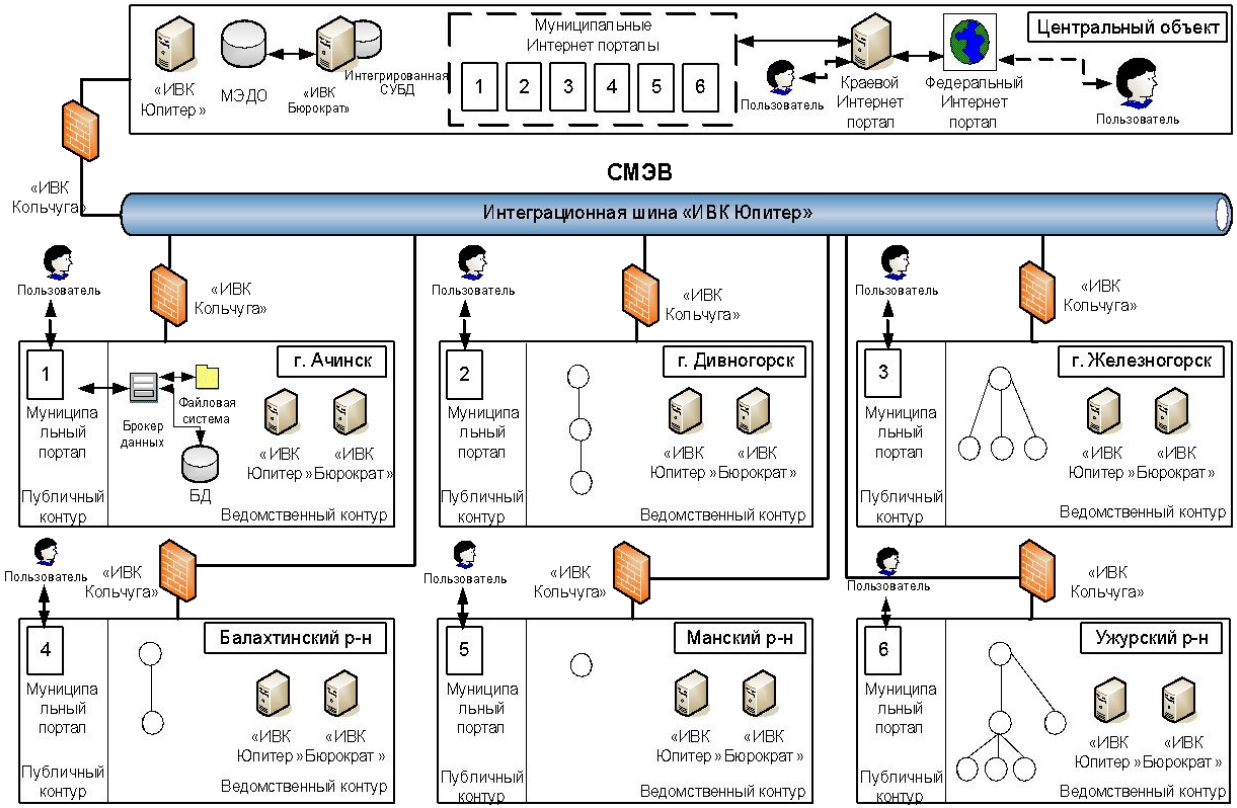
1. Обеспечение конфиденциальности, целостности и доступности информации на объектах автоматизации АС;
2. Защита периметра и организация доступа в открытую сеть Интернет объектов автоматизации территориально-распределенной АС;
3. Организация Интранет-ресурсов на объектах АС;
4. Возможность удаленного администрирования, построение централизованной системы управления телематическими сервисами АС;
5. Собственная безопасность и защита от «внешних и внутренних» нарушителей;
6. Непротиворечивое взаимодействие с объектовыми средствами защиты (в том числе СКЗИ);
7. Доступность организациям любого масштаба;
8. Простота администрирования как решение острой кадровой проблемы.

МЭ «ИВК Кольчуга™» сертифицирован ФСТЭК РФ по 4-му и 2-му классам защищенности от НСД (для МЭ) и 2-му уровню контроля НДВ.

МЭ «ИВК Кольчуга™» предлагается в двух вариантах исполнения

Решение вводится в опытную эксплуатацию

На площадке **Красноярского края** протестировано комплексное программно-аппаратное решение, позволяющее предоставлять муниципальные услуги в электронном виде.



Решение «Под ключ»

Компания ЗАО «ИВК» представляет
комплексное решение «под ключ»:

- Аппаратные и программные решения.
- Разработка организационно-нормативных документов.
  (модель нарушителя и угроз, политики безопасности, руководства и инструкции)
- Обеспечение взаимодействия с федеральным уровнем на основе нормативной, методологической и технической базы.
- Обучение персонала на местах.

Спасибо за внимание!

Контактная информация:

Руководитель проектов
ЗАО «ИВК»
Буйлов Михаил Борисович
тел. (495) 221-65-80, доб. 1157

E-mail: buylov@*ivk.ru*
www.ivk.ru