Оглавление

[Требования к программному продукту 2](#_Toc72837500)

[Анализ аналогов 2](#_Toc72837501)

[Аппаратно-программный комплекс шифрования “Континент” 2](#_Toc72837502)

[Программный комплекс “Signatura. СпецСвязь” 3](#_Toc72837503)

[Построение VPN сети ТЕЛЕДИСКОНТ 4](#_Toc72837504)

[Аппаратно-программный комплекс ViPNet Custom 5](#_Toc72837505)

[Корпоративный мессенджер “eXpress” 5](#_Toc72837506)

[Омниканальный сервис рассылок “SMS-Uslugi” 6](#_Toc72837507)

[Результаты анализа 7](#_Toc72837508)

# Требования к программному продукту

# Анализ аналогов

Для решения поставленной задачи был изучен рынок сервисов, которые могли бы отвечать требованиям технического задания. Далее будут рассмотрены и проанализированы некоторые из представленных на рынке решений.

## ****Аппаратно-программный комплекс шифрования “Континент”****

<https://www.securitycode.ru/products/apksh_kontinent/?tab=models>

АПКШ «Континент» — аппаратно-программный комплекс, который позволяет обеспечить защиту информационных сетей предприятия от вторжения со стороны внешних сетей (Интернет), а также конфиденциальность во время передачи информации по общедоступным каналам связи, организовать безопасный доступ пользователей виртуальных частных сетей к ресурсам сетей общего пользования, а также защищенное взаимодействие сетей сторонних организаций-партнеров. Комплекс используется как централизованное средство для защиты сетевой инфраструктуры  
и создания VPN-сетей с использованием алгоритмов ГОСТ. “Континент” имеет сертификаты ФСТЭК и ФСБ, а производителем комплекса является компания “Код Безопасности”, которая является одной из лидирующих компаний на Российском рынке средств защиты от информационных угроз.

В арсенал компании “Код Безопасности” входят средства для защиты виртуальных сред (vGate), конечных устройств или точек (Secret Net Studio, Terminal, Соболь), мобильных устройств (Континент АП Мобильный), а также средства по работе с электронными подписями (Jinn Server/Client).

Значительная проблема заключается в стоимости приобретения интересующих нас средств. Цены на различные версии и конфигурации АПКШ “Континент” варьируются и начинаются от 100 000 рублей. Стоит учитывать и то, что на каждую точку подключения необходимо будет установить свой экземпляр средства защиты.

**Плюсы:**

* имеет сертификаты ФСТЭК России на соответствие необходимым классам защищенности и уровням доверия, сертификаты ФСБ России на средство криптографической защиты информации;
* имеет широкий модельный ряд;
* широко известно в сфере информационной безопасности, имеет большую базу пользователей.

**Минусы:**

* требует большую высококвалифицированную команду сопровождения;
* имеет высокую рыночную стоимость.

Аппаратно-программные комплексы давно зарекомендовали себя в качестве первоклассных средств защиты масштабных корпоративных сетей, однако высокая цена и сложность внедрения и содержания не позволяют рассмотреть его как основной вариант решения в нашей работе.

## ****Программный комплекс “Signatura. СпецСвязь”****

<https://www.cryptopro.ru/en/partners/solutions/programmnyi-kompleks-soyuz-spetssvyaz>

<https://cryptex.pro/>

СпецСвязь - система обмена значимой информацией по зашифрованному каналу связи через Интернет от разработчиков кампании ООО “Криптэкс”, связанную с известным производителем и разработчиком в области информационной безопасности компанией Crypto Pro. В основе этого комплекса лежат алгоритмы ГОСТ. В системе реализован механизм “визирования”, то есть возможность последовательного подписания руководителями на разных уровнях. Также в программном комплексе реализовано хранилище совместно используемой и личной информации, которая передается в зашифрованном виде на сервера “Signatura. СпецСвязь”.

СпецСвязь использует необычную модель монетизации: помимо лицензии на подключение компании к сервису (около 15 000 рублей), необходимо также платить за каждое отправленное сообщение или документ (около 8 рублей за штуку), что может вытекать в достаточно большие суммы, учитывая широкий круг получателей и большой поток сообщений.

Данное решение имеет также многоэтапное подтверждение при отправке каждого сообщения и документа, что не является удобным в нашем случае и наиболее подходит для обмена документами, нежели быстрыми сообщениями.

**Плюсы:**

* имеет сертификаты ФСТЭК России на соответствие необходимым классам защищенности и уровням доверия, сертификаты ФСБ России на средство криптографической защиты информации;
* представляет собой веб-ресурс, готовый функционировать без предустановленного программного обеспечения, не считая браузера.

**Минусы:**

* сложный процесс обмена информацией;
* необходимость использования доверенной электронной подписи для пользования сервисом.

“СпецСвязь” могла бы являться одним из фаворитов списка аналогов в связи с удобством использования HTTP/HTTPS-сервисов, абсолютной кросс-платформенностью ввиду широкого использования технологии HTTP, однако чересчур сложный и долгий механизм подтверждения сообщений перевешивает все плюсы сервиса в нашем примере.

## ****Построение VPN сети ТЕЛЕДИСКОНТ****

<https://telediscount.ru/postroenie-vpn/>

Компания ЗАО "Теледисконт" является оператором связи и разработчиком цифровых продуктов IP и SIP телефонии, виртуальных АТС, IT-аутсорсинга. В этой компании в числе прочего можно получить такую услугу, как построение VPN-сети для организации защищенного канала связи на выделенных сетях VPN L2 на основании таких технологий как L2TP-VPN, OPEN VPN, выделенный VPN-сервер и другие.

Для организации VPN-сети компания "Теледисконт" предлагает к приобретению сетевое оборудование компании MikroTik, которое будет установлено в каждой точке подключения к сети.

Компания предоставляет широкий выбор тарифов и условий, с которыми можно гибко подобрать подходящий под нужды компании подходящий тариф. Средняя цена ежемесячного тарифа – 6 000 рублей. К этому необходимо прибавить цену на сетевое оборудования по количеству точек подключения (в среднем 6 000 – 10 000 рублей).

**Плюсы:**

* возможность в кратчайшие сроки развернуть VPN-сеть с местами подключения в любой точке России, а также масштабировать уже существующую сеть;
* возможность выбора необходимого алгоритма шифрования, в том числе ГОСТ.

**Минусы:**

* необходимость установки сетевого оборудования в каждой точке подключения;
* возможность использования VPN-сети только в области действия ближайшей точки подключения.

Весьма удобно иметь у себя в арсенале VPN-сеть из зарекомендовавших себя универсальных в плане настройки устройств от латвийского производителя, однако необходимости постоянно находиться возле точки доступа не очень вяжется с концепцией, которую мы стремимся построить.

## ****Аппаратно-программный комплекс ViPNet Custom****

<https://www.astral-rd.ru/pir/produkty-vipnet-custom/kompleks-vipnet-custom>

ViPNet **Custom** – это средство, которое позволяет организовывать защиту информации в крупных сетях (от нескольких десятков до десятков тысяч сетевых узлов — рабочих станций, серверов и мобильных компьютеров) и нацелено на решение различных задач информационной безопасности. Наиболее интересующей нас в этом случае задачей является создание защищенной, доверенной среды передачи информации ограниченного доступа с использованием публичных и выделенных каналов связи (Интернет, телефонные и беспроводные линии связи) путем организации виртуальной частной сети (VPN) с одним или несколькими центрами управления.

**Плюсы:**

* имеет сертификаты ФСТЭК России на соответствие необходимым классам защищенности и уровням доверия, сертификаты ФСБ России на средство криптографической защиты информации;
* широко известно в сфере информационной безопасности, имеет большую базу пользователей.

**Минусы:**

* требует большую высококвалифицированную команду сопровождения;
* высокая рыночная стоимость.

В использовании аппаратно-программного комплекса достаточно плюсов, чтобы рассмотреть его как вариант, однако, как и в случае с АПКШ “Континент” минусы значительно перебивают плюсы в рамках, поставленных для решения задач.

## Корпоративный мессенджер “eXpress”

<https://www.express.ms/>

Мессенджер eXpress – это средство для безопасного корпоративного общения внутри компании, а также для коммуникации с бизнес-партнерами и внешними пользователями. Его основная функция – организация быстрой корпоративной коммуникации без рисков. Организованная инфраструктура позволяет совершать защищенную коммуникацию между серверами и работниками разных компаний.

**Плюсы:**

* включен в Единый реестр российских программ для ЭВМ и баз данных Минкомсвязи РФ;
* имеет возможность размещения выделенных серверов во внутренней сети;
* имеет решения, как для мобильных устройств, так и для персональных компьютеров;
* содержит комплексное шифрование, а также имеет возможность управления ключами шифрования.

**Минусы:**

* содержит большое количество перегружающего функционала, выходящего за рамки технического задания (поддержка видеоконференций, агрегации справочников и контактов и др.);
* отсутствуют инструменты управления возможностями сервиса.

Вариант радует универсальностью использования, сравнительно невысокой ценой и простотой во внедрении, однако главным его минусом можно посчитать неконтролируемый, перегруженный функционалом клиент, а также невозможность скорректировать под себя необходимые инструменты.

## Омниканальный сервис рассылок “SMS-Uslugi”

<https://sms-uslugi.ru/>

SMS-Uslugi — онлайн-сервис, который позволяет настроить персональную массовую рассылку в различных каналах — SMS, Viber, Вконтакте, Одноклассниках и Голосовые рассылки.

Регистрация в самом сервисе бесплатна, оплата осуществляется только за каждое отдельное сообщение или звонок (в среднем 3 рубля за каждое отправленное сообщение каждому адресату).

Не смотря на сравнительную дешевизну использования, сервис не подходит для использования в нашем примере, так как отправляемые сообщения никак не шифруются, кроме внутреннего шифрования отдельно каждого сервиса, о благонадежности которого мы можем только мечтать. Ни о какой конфиденциальности в данном варианте речи идти не может.

**Плюсы:**

* имеет удобные механизмы взаимодействия и управления возможностями сервиса;
* соответствует федеральным законам № 152-ФЗ и № 242-ФЗ.

**Минусы:**

* не входит в Единый реестр российских программ;
* использует только сторонние сервисы для передачи сообщений, не давая получить гарантию полной конфиденциальности передаваемых сообщений.

Как бы не был хорош сервис в сфере цифрового общения и коммуникаций, под наши изначальные цели он подходит меньше всего из всего списка перечисленных аналогов ввиду отсутствия главного фактора выбора – контролируемого нами шифрования.

# Результаты анализа

В ходе анализа существующих для решения поставленной задачи средств была выявлена необходимость в разработке узконаправленного продукта, отвечающего всем требованиям технического задания, так как ни одно из рассмотренных средств не отвечает в полной мере заявленным требованиям.

**Сравнительная таблица**