eXpress

Коммуникационная
система для бизнеса

Общие сведения о системе

ООО Анлимитед Продакшен

Москва, Новослободская ул., д.24с1, 127055
+7 903 968 83 34
www.unlimitedtech.ru
sales@unlimitedtech.ru

Содержание данного документа, а также другие материалы, прилагаемые к нему, являются исключительной собственностью ООО «Анлимитед Продакшен»

Оглавление

1. Назначение комплекса 3
2. Основные функции 3
3. Основные компоненты 3
4. Механизмы защиты 5
   4.1. Доступные роли 5
   4.2. Управление контактами 6
5. Архитектура 7
6. Системные требования 11
   6.1. Требования к платформе 11
   6.2. Требования к платформе STUN/TURN 12
   6.3. Требования к ПО 12
   6.4. Требования к DNS 13
   6.5. Требования к сертификату 13
   6.6. Требование к корпоративному каталогу LDAP 13
   6.7. Требование к серверу SMTP 14
   6.8. Требование к сетевым взаимодействиям 14
   6.9. Требования к серверу VoEx 14
   6.10. Требования к DLPS 14

1. Назначение комплекса

Решение Express предназначено для предоставления качественной и непрерывной связи между сотрудниками компании и снижения рисков утечек информации за счет перемещения каналов обмена из публичной сети Интернет в периметр локальных вычислительных сетей Компании.

2. Основные функции

Решение Express реализует следующие основные функции:

- быстрый обмен пользователей текстовыми сообщениями и файлами с помощью мобильных устройств и веб-клиента на ПК в рамках персональных и групповых чатов;
- осуществление персональных и групповых аудио- и видеозвонков;
- обеспечение безопасного хранения и передачи конфиденциальных данных;
- создание копии данных для восстановления работоспособности подсистемы в случае ее повреждения или разрушения;
- оптимизация использования ресурсов.

3. Основные компоненты

Решение Express предусматривает три контура взаимодействия пользователей (которые могут поставляться в трех исполнения):

- публичный (внешний);
- контур предприятия (внутренний контур компании, объединяющий несколько внутренних серверов);
- корпоративный (внутренний).

Публичный (внешний) контур взаимодействия пользователей используется для:

- первичной регистрации пользователей;
- отправки push-уведомлений;
- обмена сообщениями и файлами с пользователями, не подключенными к какому-либо внутреннему контуру;
- совершения звонков пользователям, не подключенных к какому-либо внутреннему контуру;
- маршрутизации сообщений и файлов между внутренними контурами, не имеющими прямых доверенных подключений.

Контур предприятия (внутренний контур компании) используется для:

- регистрации пользователей;
- отправки push-уведомлений;

- маршрутизации сообщений и файлов между корпоративными контурами, не имеющими прямых доверенных подключений.

Корпоративный (внутренний) контур взаимодействия пользователей используется для:

- регистрации корпоративных пользователей;
- обмена сообщениями, файлами и совершения звонков с пользователями компании;
- предоставления корпоративной адресной книги;
- маршрутизации сообщений и файлов между корпоративным контуром компании и корпоративными контурами партнеров с кем установлены доверенные подключения.

Решение Express включает следующие отдельно устанавливаемые компоненты:

- региональный сервер Express (далее — RTS);
- сервер предприятия (далее — ETS)
- корпоративный сервер Express (далее — CTS);
- мобильное приложение;
- десктоп-приложение;
- веб-приложение.

RTS, ETS и CTS являются основными элементами в структуре комплекса. RTS объединяют и обслуживают компьютерные сети внутри одного региона и отвечает за функционирование публичного контура взаимодействия.

ETS объединяют и обслуживают компьютерные сети и корпоративные серверы внутри одной большой компании и отвечает за функционирование контура предприятия. Под ETS выпускается отдельное приложение, которое управляется компанией, использующей ETS. Пользователи CTS, подключенных к ETS, получают СМС и push-уведомления с этого ETS.

CTS объединяют и обслуживают клиентские устройства в пределах организации, подключаются к ETS или RTS и выполняют роль посредника между клиентским устройством и ETS/RTS. CTS отвечает за функционирование корпоративного контура. При установленном ETS информационный обмен между корпоративными серверами происходит внутри предприятия, данные с CTS передаются на ETS, ETS осуществляет информационный обмен с внешним контуром.

Клиентское устройство может подключаться как к CTS, так и к ETS или RTS напрямую. Для каждого сервера пользователь регистрирует свой профиль. В зависимости от активного профиля пользователю доступны свои ресурсы в виде чатов, контактов и истории обмена сообщениями. Подключение клиента к CTS возможно после подключения к RTS или ETS. Все сообщения, переданные между корпоративными пользователями, хранятся на CTS в зашифрованном виде и не доступны администраторам сервера. Для обеспечения работы голосовых вызов используется сервер

STUN/TURN (VoEx) который может быть расположен отдельно либо совмещен с CTS., либо расположен на RTS/ETS.

Управление комплексом осуществляется с помощью веб-интерфейса — консоли администратора, которая предоставляет возможности для настройки решения Express и контроля функционирования приложения.

4. Механизмы защиты

Безопасность передачи конфиденциальных данных обеспечивается следующими защитными механизмами, реализуемыми решением Express:

- ролевой метод разграничения доступа;
- многоуровневый метод аутентификации и идентификации пользователей,
  в том числе с использованием дополнительных средств аутентификации;
- использование криптографических средств для защиты каналов связи за пределами контролируемой зоны;
- комплекс решений для резервного копирования и восстановления данных системы.

Реализованы дополнительные механизмы при работе в нестабильных сетях или в сетях с низким качеством:

- локальный доступ к данным на устройстве при отсутствии подключения к сети;
- доступ к локальным копиям ранее отправленных и полученных данных в случае отсутствия связи с сервером, в том числе:
  - просмотр локального списка контактов;
  - просмотр загруженного кэша истории чатов;
  - полнотекстовый поиск по истории переписки;
  - просмотр ранее принятых и отправленных файлов, копия которых
    содержится на данном клиентском устройстве.

4.1. Доступные роли

Управление комплексом осуществляют сотрудники организации, обладающие правами администратора. Административные права системы назначаются
иерархически.

Для безопасной и успешной эксплуатации решения Express определяются
следующие роли:

Роль	Права	Тип учетной записи
Администратор	• назначение ролей; • просмотр журнала безопасности; • управление чатами; • управление учетными записями пользователей; • подключение чат-ботов; • управление настройками системы	Внутренний пользователь
Корпоративный пользователь	• отправка сообщений; • создание чата; • просмотр адресной книги сервера; • подключение к чат-ботам	Внутренний пользователь
Региональный пользователь	• отправка сообщений; • создание чата	Внешний пользователь
Аудитор	• просмотр сообщений в консоли DLP; • просмотр журналов в консоли DLP	Внутренний пользователь

Тип учетной записи зависит от положения сервера, на котором авторизован пользователь. Если в защитном контуре находится RTS, то региональный пользователь становится внутренним.

Решение Express предусматривает создание администраторов с ограниченными правами для решения конкретных задач.

Задачи администраторов:

- установка и управление обновлениями общесистемного и прикладного ПО;
- настройка, поддержка в работоспособном состоянии и мониторинг работы серверного оборудования;
- управление резервным копированием и восстановление данных;
- централизованная настройке приложения;
- управление учетными записями пользователей.

4.2. Управление контактами

Администратор управляет учетными записями пользователей (контактами). Он может:

- добавлять нового пользователя в корпоративный контур и контур предприятия, если настроена авторизация с помощью электронной почты;
- управлять подключением пользователей к корпоративному контуру;
- подключать CTS/ETS к RTS;
- подключать CTS к ETS;
- устанавливать и настраивать трасты между CTS;

- удалять учетные записи пользователей на CTS, если настроена авторизация с помощью электронной почты;
- управлять учетными записями пользователей (создавать, редактировать, удалять) и управлять правами доступа администраторов.

Решение Express может функционировать совместно с Active Directory. Внесенные изменения в учетные записи пользователей в Active Directory отражаются на соответствующих учетных записях в Express. Авторизация пользователя осуществляется через AD. При функционировании Express без AD авторизация пользователя осуществляется через электронную почту.

5. Архитектура

Решение «Express» состоит из внешнего контура и внутреннего контура. Связь между внешним и внутренним контуром средства в локальной сети осуществляется с помощью специального сервиса – траста. Внешний контур состоит из регионального сервера (RTS), внутренний контур состоит из корпоративного сервера (CTS) или корпоративного сервера и сервера предприятия (ETS), к которому подключаются CTS.

CTS основан на микросервисной архитектуре с использованием контейнеризации на основе Docker. Данное решение позволяет максимально автоматизировать развертывание и обновление серверного ПО Express.

CTS поддерживает 2 вида развертывания:

- единый сервер Express (Single CTS);
- разделенный сервер Express (Front CTS и Back CTS).

Типовая схема развертывания сервера CTS изображена ниже (Рисунок 1).

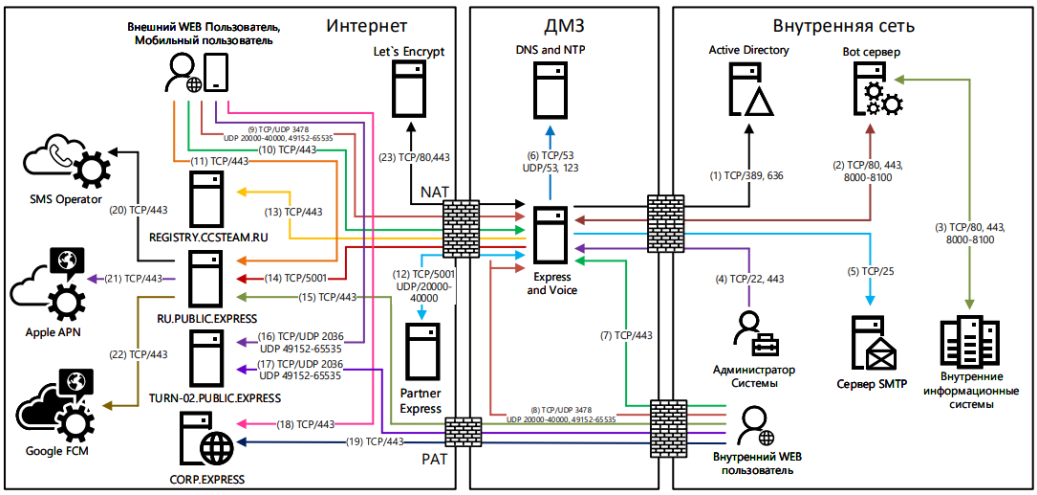

Рисунок 1. Типовая схема развертывания Single CTS

Single CTS размещается в демилитаризированной сетевой зоне компании и содержит в себе следующие контейнеры docker:

- zookeeper (координатор для kafka);
- kafka (диспетчер сообщений между сервисами);
- logstash (отвечает за прием логов от сервисов и загрузку их в elasticsearch);
- elasticsearch (хранилище логов сервисов);
- kibana (сервис просмотра индексов elasticsearch);
- postgres (основная база данных сервисов);
- postgres_exporter (отвечает за снятие метрик с postgres);
- prometheus (отвечает за снятие, обработку и хранение метрик сервисов);
- redis (KV-хранилище);
- nginx (веб-сервер, который принимает подключения извне и отвечает за маршрутизацию подключений);
- ad_integration (интегрируется с Active Directory и другими LDAP-сервисами, отвечает за авторизацию клиента с помощью NTLM и AD);
- admin (интерфейс администратора);
- audit (сервис аудита подключений);
- botx (отвечает за интеграцию с ботами);
- email_notifications (отвечает за рассылку e-mail сообщений с кодом аутентификации);
- file_service (сервис загрузки файлов);
- kdc (хранилище ключей);
- messaging (сервис обмена сообщениями, отвечает за подключение клиентов через протокол websocket);
- phonebook (адресная книга);
- routing_schema (визуализирует схему маршрутизации в чатах);
- settings (отвечает за хранение настроек сервисов);
- trusts (отвечает за обмен событиями между RTS и CTS);
- voex (сервис для совершения аудиовызовов).

Типовая схема развертывания разделенного сервера CTS (Front CTS и Back CTS) изображена ниже (Рисунок 2).

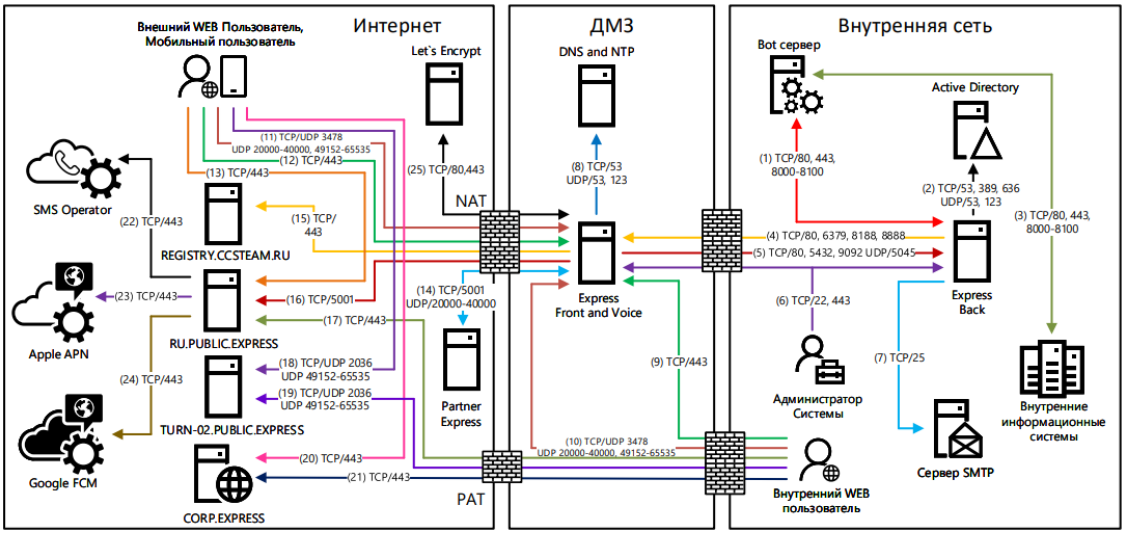

Рисунок 2. Типовая схема развертывания разделенного CTS (Front/Back)

Разделенный сервер состоит из Front CTS и Back CTS сервера.

Front CTS сервер размещается в демилитаризированной сетевой зоне компании и содержит в себе два контейнера и локальный прокси-сервер:

- Trusts (обеспечивает взаимодействие с сервером публичного контура RTS и другими доверенными корпоративными CTS);
- Nginx (обеспечивает подключение пользователей Express);
- Tinyproxy (локальный прокси-сервер, обеспечивает подключение сервера Back CTS к репозиторию образов docker, используемых для установки и обновления изделия).
- Back CTS (сервер размещается в локальной сети компании и содержит в себе следующие контейнеры docker):
  - zookeeper (координатор для kafka);
  - kafka (диспетчер сообщений между сервисами);
  - logstash (отвечает за прием логов от сервисов и загрузку их в elasticsearch);
  - elasticsearch (хранилище логов сервисов);
  - kibana (сервис просмотра индексов elasticsearch);
  - postgres (основная база данных сервисов);
  - postgres_exporter (отвечает за снятие метрик с postgres);
  - prometheus (отвечает за снятие, обработку и хранение метрик сервисов);
  - redis (KV-хранилище);
  - nginx (веб-сервер, который принимает подключения извне и отвечает за маршрутизацию подключений);

- ad_integration (интегрируется с Active Directory и другими LDAP-сервисами, отвечает за авторизацию клиента с помощью NTLM и AD);
- admin (интерфейс администратора);
- audit (сервис аудита подключений);
- botx (отвечает за интеграцию с ботами);
- email_notifications (отвечает за рассылку e-mail сообщений с кодом аутентификации);
- file_service (сервис загрузки файлов);
- kdc (хранилище ключей);
- messaging (сервис обмена сообщениями, отвечает за подключение клиентов через протокол websocket);
- phonebook (адресная книга);
- routing_schema (визуализирует схему маршрутизации в чатах);
- settings (отвечает за хранение настроек сервисов);
- voex (сервис для совершения аудиовызовов).

VoEx сервер размещается в сети Интернет либо в демилитаризированной сетевой зоне компании. При размещении в сети Интернет, VoEx располагается на выделенном сервере. При размещении в демилитаризированной сетевой зоне компании, VoEx может располагаться на выделенном сервере либо на сервер Single CTS или Front CTS.

Типовая схема развертывания ETS и единого сервера CTS (Front CTS) изображена ниже (Рисунок 3).

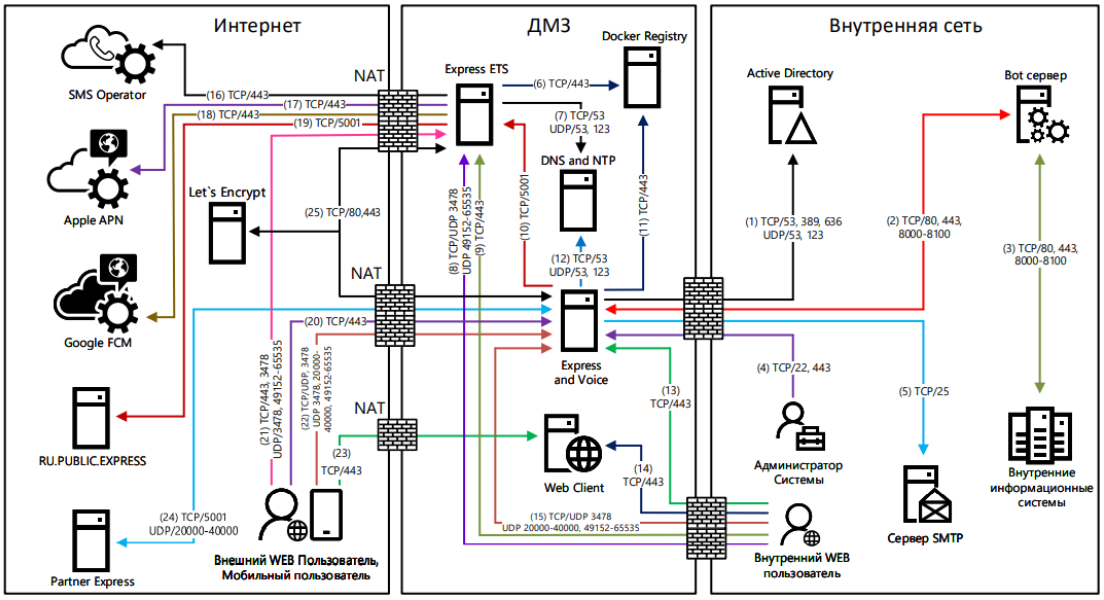

Рисунок 3. Типовая схема развертывания ETS и Single CTS

Типовая схема развертывания ETS и разделенного сервера CTS (Front CTS и Back CTS) изображена ниже (Рисунок 4).

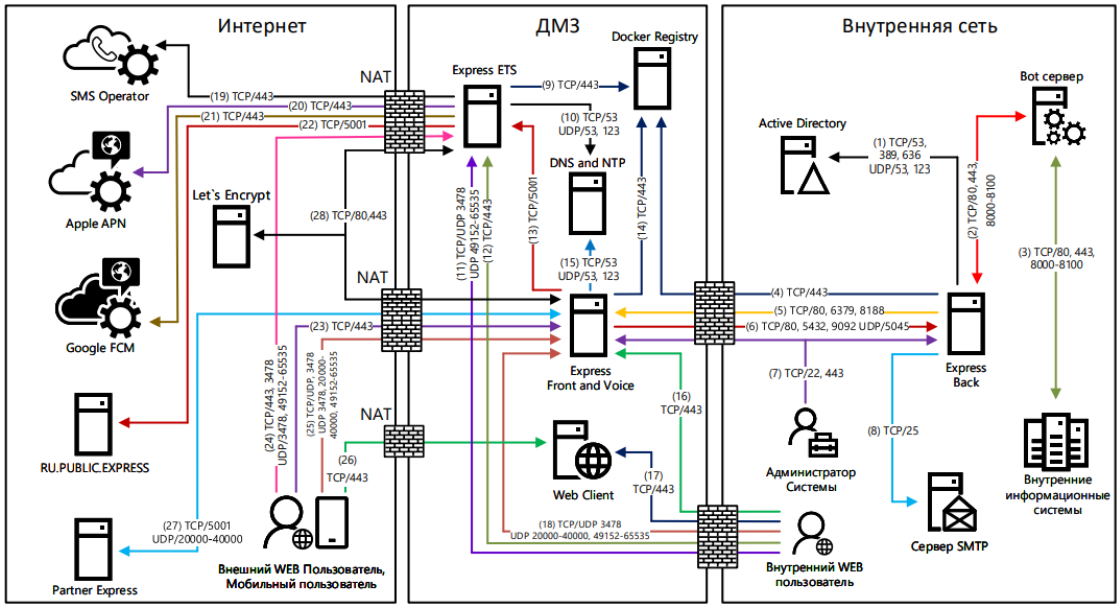

Рисунок 4. Типовая схема развертывания ETS, Front CTS и Back CTS

6. Системные требования

6.1. Требования к платформе

CTS может быть развернут на аппаратной платформе или в среде виртуализации.

Минимальные системные требования к аппаратной платформе Single CTS либо сервер Back CTS в зависимости от количества пользователей:

Кол-во пользователей	vCPU/CPU Core	RAM Гб	HDD Гб
10	4	8	70
25	4	8	145
50	6	10	270
100	6	12	520
200	8	16	1020
500	12	24	2520
1000	16	32	5020
2000	16	36	10020
5000	24	52	25020
10000	32	64	50020

Примечание. Объем HDD взят из расчета глубины хранения журналов (1 Гб) и пользовательских данных (4 Гб) за 4 года. Данные по требуемому месту могут значительно отличаться от расчетных при более активном использовании изделия.

Минимальные системные требования к серверу Front CTS при использовании разделенного CTS в зависимости от количества пользователей:

Кол-во пользователей	vCPU/CPU Core	RAM Гб	HDD Гб
50	2	4	42
100	2	4	42
200	2	4	42
500	4	8	42
1000	4	8	42

6.2. Требования к платформе STUN/TURN

Сервер STUN/TURN может быть развернут на аппаратном сервер или в среде виртуализации. Требования к аппаратной платформе сервера STUN/TURN в зависимости от количества пользователей:

Кол-во пользователей	vCPU/CPU Core	RAM Гб	HDD Гб
10	2	1	42
25	4	2	42
50	4	2	42
100	8	4	42
200	10	5	42
500	12	6	42
1000	16	8	42
2000	18	9	42
5000	32	16	42
10000	64	32	42

При развертывании сервера STUN/TURN на сервер Single CTS требования суммируются.

6.3. Требования к ПО

Требование к операционной системе: Сервер CTS поддерживает любую ОС семейства Linux, на который устанавливается Docker 18.03.0-ce и выше. Рекомендуется Ubuntu 20.04 LTS.

Требование к ПО контейнеризации: Docker: 18.03.0-ce и выше (настоятельно рекомендуется установка из репозитория docker, https://docs.docker.com/install/linux/docker-ce/ubuntu/).

Требование к синхронизации времени: Необходим установленный и настроенный локальный сервер NTP с уровнем stratum не ниже 15.

6.4. Требования к DNS

Требуется DNS-имя для сервера CTS, разрешаемое в сети Интернет и ссылающиеся на внешний IP-адрес публикации сервера Single CTS или Front CTS. Рекомендуется имя третьего уровня express.mydomain.tld.

Во внутренней сети компании DNS-имя должно разрешаться во внутренний IPадрес сервера Single CTS.

Требования к DNS имени STUN/TURN сервера аналогичны требованиям к DNS имени сервера CTS.

6.5. Требования к сертификату

Для работы изделия требуется оформить сертификат на внешнее имя сервиса Express (FQDN или wildcard), выпущенный публичным доверенным центром сертификации, удовлетворяющий следующим требованиям:

- версия 3 и не ниже TLS 1.2;
- длина ключа не меньше 2048 бит;
- алгоритм подписи SHA 256;
- версия синтаксиса X.509 3;
- незашифрованный закрытый ключ.

Файл должен содержать в себе сертификат сервера, сертификаты промежуточного центра сертификации и корневого центра сертификации. Формат сертификатов должен соответствовать кодировке Base64. Файл закрытого ключа должен содержать нешифрованный закрытый ключ кодировки Base64.

Примерная структура файла сертификата изображена на рисунке ниже
(Рисунок 5).

```
-----BEGIN CERTIFICATE-----
Base64 server certificate
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Base64 intermediate ca
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Base64 root ca
-----END CERTIFICATE-----
```

Рисунок 5

Поддерживается использование бесплатного сертификата от компании Let`s Encrypt.

6.6. Требование к корпоративному каталогу LDAP

При интеграции Express с корпоративным каталогом на базе Microsoft Active Directory требуется создание учетной записи с правами «Domain Users» и контейнера «deleted objects»

(https://support.microsoft.com/enus/help/892806/how-to-let-non-administrators-view-the-active-directory-deletedobject).

Стандартной практикой предоставление доступа пользователей к Express является создание группы пользователей Express в Active Directory. Тип группы — «Security», видимость группы — «Universal».

При интеграции Express с корпоративным каталогом на базе LDAP совместимого сервера требуется создание учетной записи с правами чтения каталога.

6.7. Требование к серверу SMTP

Для возможности отправки ПИН-кодов аутентификации устройства пользователя требуется создание на почтовом сервер учетной записи, под которой будет производиться отправка электронной почты.

6.8. Требование к сетевым взаимодействиям

Требования к сетевым взаимодействиям описаны в Руководстве администратора.

6.9. Требования к серверу VoEx

Сервер VoEx может быть развернут на аппаратном сервер либо в среде виртуализации. Минимальные системные требования серверу VoEx в зависимости от количества пользователей:

Кол-во пользователей	vCPU/CPU Core	RAM Гб	HDD Гб
10	2	1	42
25	4	2	42
50	4	2	42
100	8	4	42
200	10	5	42
500	12	6	42
1000	16	8	42
2000	18	9	42
5000	32	16	42
10000	64	32	42

Примечание. При развертывании сервера VoEx на сервер Single CTS либо Front CTS требования суммируются.

6.10. Требования к DLPS

Для функционирования DLPS необходимо выполнение следующих требований:

- доступ к подсистеме kafka на получение событий топиков «admin-events» и «system-events»;
- доступ к API подсистем kdc (БД ключей безопасности) и messaging (БД сообщений);

- доступ к базам данных messaging (БД сообщений) и DLPS;
- доступ к LDAP-серверу при авторизации по LDAP;
- доступ к скачиванию файлов.

Требования к сетевой инфраструктуре входящих соединений:

Модуль/сервис	Протокол	Порт
Веб-клиент	TCP	80, 443

Требования к сетевой инфраструктуре исходящих соединений:

Модуль/сервис	Протокол	Порт
Kafka	TCP/UDP	9092/9093
Zookeeper	TCP	2182
Postgresql	TCP	5432
CTS-app	TCP	80, 443

Требования к объему памяти

Параметр	Значение
Процессор	8 ядер
Оперативная память	8 Гб
Жесткий диск	40 Гб
Пропускная способность сети	1 Гбит/с