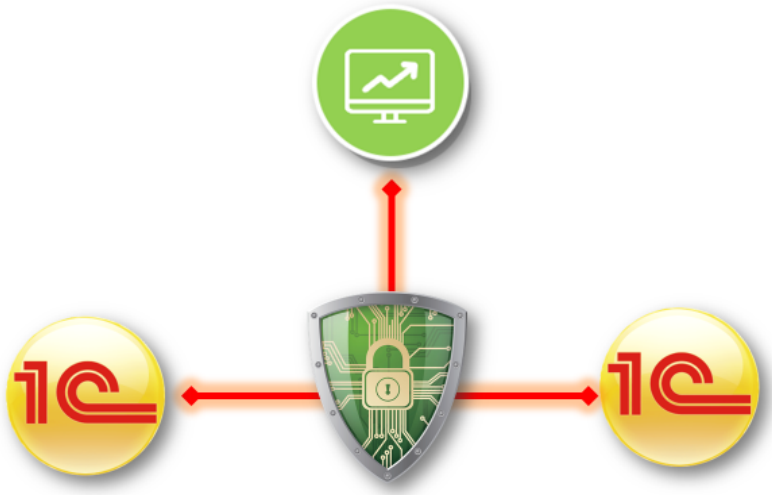
1.11. Обеспечение информационной безопасности

В статье описывается обеспечение информационной безопасности в конфигурации «Агент Плюс: Управление дистрибуцией».

Чтобы обеспечить целостность, доступность и конфиденциальность информации, необходимо защитить ее от несанкционированного доступа, разрушения, незаконного копирования и разглашения. Необходимо организовать комплекс организационных и технических мер, направленных на защиту данных.

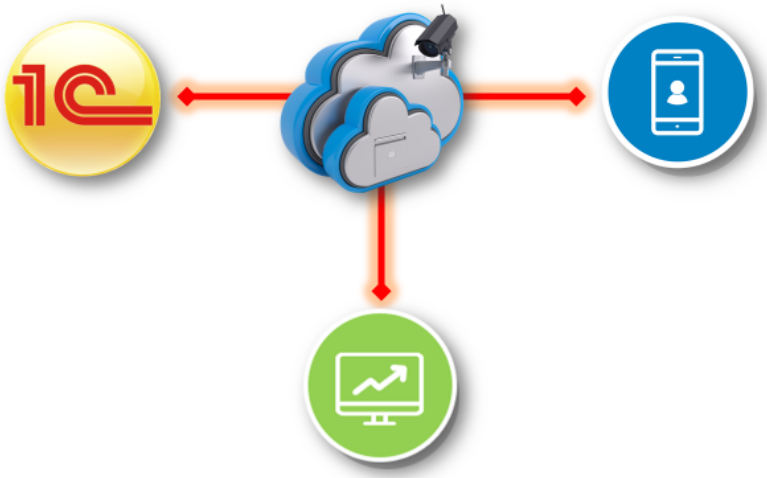
Обмен данными с помощью дополнительных внешних обработок может производиться через защищённое соединение. На сегодняшний день существует множество технологий и сервисов, которые предлагают возможность передавать или принимать данные через своего интернет-провайдера, чтобы быть в полной уверенности, что никто кроме вас не узнает, какие именно манипуляции вы производили со своими файлами. Для обеспечения нужного уровня безопасности необходимо выбрать подходящий вид соединения и протокол передачи данных.

Главным фактором обеспечивающим защиту остается ограничение доступа и наличие надежного пароля.



Для обеспечения безопасности передачи и получения данных в **«Агент Плюс: Управление дистрибуцией»** при помощи облачного сервиса **«Агент Плюс: Т-Обмен»** используется:

- **HTTPS с сертификатом SSL.** Защита данных в HTTPS обеспечивает криптографический протокол SSL/TLS, который шифрует передаваемую информацию. Компьютер пользователя и сервер выбирают общий секретный ключ, с помощью которого и происходит шифрование передаваемой информации. Это ключ уникальный и генерируется для каждого сеанса. Считается, что его подделать невозможно, так как в нем содержится более 100 символов. Во избежание перехвата данных третьим лицом используется цифровой сертификат – это электронный документ, который идентифицирует сервер. Первое, что делает браузер при установке соединения по протоколу HTTPS, это проверку подлинности сертификата, и только в случае успешного ответа начинается обмен данными. Все современные браузеры поддерживают протокол HTTPS. Его не нужно специально настраивать — он автоматически включается в процесс.
- **Токен.** Средство идентификации генерируется системой авторизации в **«Агент Плюс: Личный кабинет»** и привязывается к конкретной конфигурации **«Агент Плюс: Управление дистрибуцией»**. Аналог электронной подписи для доступа к защищенному ресурсу. Токен задействован при каждом запросе на получение данных в ЛК, и в случае несовпадения обмен останавливается. Единственная уязвимость токена — это его кража. Вероятность такого случая может быть уменьшена если:
  - предоставлять каждому сотруднику минимально необходимый уровень доступа к данным — ровно столько, сколько ему нужно для выполнения должностных обязанностей. Этот принцип позволяет избежать многих проблем, таких как утечка конфиденциальных данных, удаление или искажение информации из-за нарушений в работе с ней и т. д;
  - использована технология двухфакторной аутентификации. Для проверки подлинности требуется вводить персональный пароль при входе в Личный кабинет. Доступ к информации на токене открыт только для Администратора.



Авторизация доступа к серверу проводится на основании уникального идентификатора мобильного устройства. В зависимости от выбранного канала обмена данными действуют системы защиты:

- если со службой «Агент Плюс: СОД» попытается связаться мобильное устройство, идентификатор которого не записан в файле настроек службы, то служба прерывает сеанс связи с таким МУ. Допустимые идентификаторы МУ хранятся в XML-файле настроек "config.xml", который находится в корне сетевой папки обмена данными;
- если лицензия мобильного приложения **«Агент Плюс: Мобильная торговля»** дезактивирована в Личном кабинете, то передача как входящих, так и исходящих данных в мобильном устройстве не производится;
- если в МУ установлен пароль для архива с файлом обмена данными на FTP-сервере, то доступ к данным в мобильном приложении **«Агент Плюс: Мобильная торговля»** будет полностью защищен.

На сервере каждому доменному и локальному пользователю, группе и другим объектам безопасности автоматически присваивается уникальный идентификатор — **Security Identifier** или **SID**. Именно SID, а не имя пользователя используется для контроля доступа к различным ресурсам: сетевым папкам, ключам реестра, объектам файловой системы, принтерам и т. д. При обращении к серверу информационная система получает ссылку URL для подтверждения права получения или отправки файла обмена из другого ресурса. Срок действия таких ссылок ограничен по времени в целях безопасности.

Связанные статьи

Разграничение прав доступа в «Агент Плюс: Управление дистрибуцией»

Настройка прав пользователя «Администратор»

Настройки входа пользователей

Активация канала «Т-Обмен» в «Личном кабинете»

Настройка дистрибуции

Настройки пользователей и прав

Общие настройки обмена с мобильными устройствами (МУ)

Синхронизация с АП:Диск. API