# Рекомендации по обеспечению информационной безопасности при работе с мобильными решениями

В документе описаны механизмы защиты информации, которые используются в мобильных решениях системы Directum RX.

Согласно ГОСТу Р50922-2006 «Защита информации», информация считается защищенной при условии обеспечения ее конфиденциальности, доступности и целостности. Это достигается с помощью использования программно-технических средств.

Защита информации при работе с системой Directum RX в мобильных приложениях обеспечивается с помощью:

- идентификации пользователей в системе;
- применения криптографии для защиты каналов связи;
- применения криптографии при подписании документов электронной подписью;
- ограничения доступа к сервису NOMAD, мобильным приложениям и корпоративным данным, хранящимся на устройстве;
- соблюдения организационных мер по обеспечению безопасности.

Рекомендации, актуальные только для определенной операционной системы или мобильного приложения, отмечены соответствующими тегами:

- Windows и Linux;
- Android и iOS;
- Directum Solo и Directum Jazz.

ВАЖНО. Перечисленные в документе рекомендации актуальны при работе с последними версиями сервиса NOMAD и приложений Directum Solo и Directum Jazz. Подробнее об изменениях версий см. в документации на мобильные решения, входит в комплект поставки Directum RX.

# Общие механизмы защиты информации в мобильных решениях Directum RX

## Аутентификация

В мобильных приложениях Directum Jazz и Directum Solo предусмотрена аутентификация путем ввода логина и пароля и их последующей передачи по каналам связи (внешняя аутентификация, аутентификация по паролю). Для использования этих типов аутентификации рекомендуется обеспечить безопасность каналов связи и устройств пользователей.

## Криптография

При работе с системой Directum RX в мобильных приложениях есть возможность подписывать документы электронной подписью (ЭП).

Подписание документов электронной подписью позволяет заменить традиционные печать и подпись, гарантируя авторство подписи и неизменность текста. После подписания текст документа становится недоступным для изменения.

В системе предусмотрено 2 вида ЭП: простая и усиленная. Усиленная подпись устанавливается уполномоченным сотрудником с использованием зарегистрированного в системе персонального сертификата ЭП. Различают усиленную неквалифицированную ЭП и усиленную квалифицированную ЭП. Их отличие заключается в наличии аккредитации у удостоверяющего центра, выдавшего сертификат ЭП.

# Мобильные приложения

Архитектура мобильных приложений Directum RX представляет собой классическую клиент-серверную архитектуру. Клиентское приложение настроено на определенный адрес сервиса NOMAD. Взаимодействие происходит по протоколу HTTP или HTTPS:


Сплошная линия означает запрос, пунктирная – ответ.

Взаимодействие сервиса NOMAD с клиентскими приложениями рекомендуется организовывать по протоколу HTTPS с использованием порта TCP **443**. Подробнее о настройке протокола см. в разделе «Безопасность передачи данных». При использовании мобильных приложений требуется обеспечить безопасность:

- сервиса NOMAD;
- канала связи;
- устройства пользователя;
- электронной подписи.

# Безопасность сети предприятия

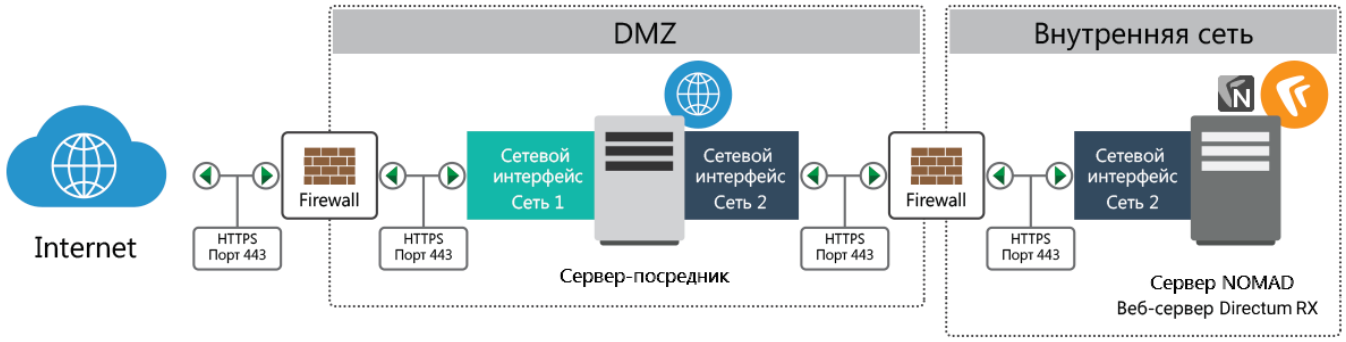
Одним из вариантов обеспечения безопасности сети предприятия является настройка демилитаризованной зоны. Подробнее см. раздел «Использование DMZ и брандмауэров для защиты сервиса NOMAD» и статью «Безопасность: Настройка демилитаризованной зоны» на Directum Club.

# Использование DMZ и брандмауэров для защиты сервиса NOMAD

Чтобы защитить сервис NOMAD от атак из внешних сетей, в организации можно настроить демилитаризованную зону (англ. Demilitarized Zone, DMZ) – конфигурацию сети, направленную на усиление безопасности сети организации. В этой конфигурации открытые для общего доступа сервера находятся в отдельном изолированном сегменте сети. Такая концепция обеспечивает отсутствие контактов между открытыми для общего доступа серверами и другими сегментами сети в случае взлома сервера.

Для этого нужно настроить:

- Windows сервер ARR – физический или виртуальный сервер-посредник, предназначенный для балансировки нагрузки веб-фермы IIS и реализованный с помощью продукта Microsoft Application Request Routing (ARR);
- Linux сервер HAProxy – физический или виртуальный сервер-посредник, предназначенный для балансировки нагрузки TCP и HTTP-приложений;
- сервис NOMAD, который может располагаться на физическом или виртуальном сервере. Он обеспечивает взаимодействие системы Directum RX и мобильных приложений.




## Настройка сервера ARR

Сервер ARR использует два сетевых интерфейса. Пример настройки сетевых интерфейсов сервера ARR и сервера с сервисом NOMAD:

- сетевой интерфейс ARR сети 1 – 210.220.230.240/255.255.255.0;
- сетевой интерфейс ARR сети 2 – 192.168.1.1/255.255.255.0;
- сетевой интерфейс сервера с сервисом NOMAD сети 2 – 192.168.1.2/255.255.255.0.

Благодаря веб-ферме сервер ARR используется как прокси-сервер для веб-запросов из Интернета, адресованных сервису NOMAD. Сам NOMAD при этом располагается во внутреннем изолированном сегменте сети.

Чтобы минимизировать возможные способы доступа к серверу ARR, настройте правила брандмауэра ARR для входящих и исходящих соединений. Для сетевых интерфейсов сетей 1 и 2 разрешите входящие и исходящие соединения только через порт **443**.

### Настройка сервера HAProxy

1. Получите из репозитория или с официального сайта актуальные пакеты HAProxy для используемой версии Linux и установите их. Например, в ОС Ubuntu для этого выполните команды:
   ```
   $ sudo apt-get update
   $ sudo apt-get install haproxy
   ```
2. Настройте работу HAProxy в одном из режимов:
   - проброс TCP-трафика;
   - проброс HTTP(S)-трафика.

Подробнее см. руководство администратора Directum RX, раздел «Настройка HAProxy».

### Настройка сервиса NOMAD

Для дополнительной безопасности рекомендуется ограничить количество потенциальных точек доступа к сервису NOMAD из внутренней сети и разрешить сетевые соединения сервиса NOMAD только с сервером балансировки нагрузки веб-фермы, СУБД и серверами приложений. Для этого настройте правила брандмауэра сервиса NOMAD для входящих и исходящих соединений и разрешите соединения только по необходимым портам.

## Безопасность данных, передаваемых на устройства

Для корректной работы мобильного приложения ознакомьтесь с разделами:

- Особенности передачи данных на устройства;
- Особенности хранения данных на устройствах;
- Способы обеспечения безопасности данных;
- Рекомендации по безопасной работе с устройствами.

# Особенности передачи данных на устройства

Для безопасной передачи данных применяются:

- VPN для подключения к сети организации;
- HTTPS для шифрования трафика.

## VPN

Мобильное устройство можно подключить к VPN как нативными средствами операционной системы, так и с помощью сторонних решений: OpenVPN Connect, ViPNet Client VPN, Checkpoint Capsule.

Для шифрования канала ГОСТ-алгоритмами рекомендуется использовать ViPNet Client VPN.

## HTTPS

При установке Directum RX администратор выбирает протокол, по которому клиентские приложения взаимодействуют с системой:

- **HTTPS**, который включает в себя несколько криптографических протоколов транспортного уровня. Он является наиболее распространенным способом защиты передаваемых данных в веб-приложениях.

  Для работы по HTTPS на мобильных устройствах требуется установить сертификаты, при этом:

  - если сертификат выдан внешним удостоверяющим центром (УЦ), то дополнительная настройка на устройстве не требуется;
  - если сертификат выдан внутренним УЦ, то необходимо настроить доверие к УЦ. Для этого установите сертификат удостоверяющего центра в соответствующее хранилище устройства.
  - iOS если используется сертификат с алгоритмом SHA-1, с версии iOS 10.3 для работы с ним требуется дополнительная настройка.

    ВАЖНО. Использование алгоритма SHA-1 считается небезопасным.

  При попытке подключения по HTTPS с использованием некорректного сертификата мобильное приложение сообщает пользователю о возможной угрозе безопасности. Дальнейшая работа с системой в этом случае невозможна.
- **HTTP**, открытый небезопасный канал связи. Рекомендуется использовать его только в условиях работы с тестовой средой или демостендом.

# Особенности хранения данных на устройствах

Выделяются следующие виды передаваемых данных:

- аутентификация. Передаются логин и пароль при аутентификации по паролю (SOAP);
- бинарные данные. Передаются тела документов и фотографии сотрудников;
- метаинформация (SOAP). Передаются, например, карточки документов, справочников, заданий, переписка по заданиям.

Особенности хранения данных приложений:

- логин и пароль пользователя, а также сертификаты хранятся в системном хранилище устройства и защищаются средствами ОС:
- iOS используются сервисы KeyChain и шифрование алгоритмом AES-256;
- Android на устройстве хранится пароль. Для хранения сертификатов используются сервисы KeyChain.
- информация системы Directum RX: данные в карточках документов и их содержимое – хранится во внутренней области памяти приложения. Доступ к этим данным другим приложениям, в том числе файловому менеджеру, ограничен.

  Android Если на мобильном устройстве включено резервное копирование данных, информация из приложений Directum Solo и Directum Jazz не копируются в облачные хранилища.

  Чтобы обеспечить безопасное хранение информации из системы Directum RX, которая загружается во внутреннюю память Solo и Jazz, ее рекомендуется зашифровать:

  - iOS при включении блокировки устройства автоматически включается шифрование файлов на диске. Используется шифрование алгоритмом AES-256.

    ВАЖНО. Поскольку графический ключ не является достаточной мерой защиты, рекомендуется настроить снятие блокировки по PIN-коду или Touch ID.
  - Android пользователь может включить шифрование в настройках устройства. Используется шифрование алгоритмом AES-256.

# Способы обеспечения безопасности данных

Безопасность устройств с установленным мобильным приложением обеспечивается с помощью:

- средств защиты по умолчанию:
  - защитой от перебора паролей. После пяти неудачных попыток входа IP-адрес, с которого производится подключение, блокируется на 30 минут.
  - ограниченным временем жизни сессии пользователя при отсутствии его активности. Для поддержания сессии пользователя используется идентификатор сессии, передаваемый в Cookie. По умолчанию продолжительность жизни сессии составляет пять часов с момента последней активности пользователя. Продолжительность жизни сессии настраивается администратором.
- соблюдения рекомендаций для администратора;
- соблюдения рекомендаций для пользователей.

# Рекомендации для администратора

Чтобы обеспечить безопасность данных на мобильном устройстве, необходимо соблюдать следующие рекомендации:

- централизованно управлять мобильными устройствами с помощью MDM-решений. Например, с помощью решения SafePhone администратор может удаленно установить доверенное приложение или запретить его использование;
- подтверждать подключение мобильного устройства пользователя к сервису NOMAD. Выполняется при входе пользователя в приложение. В зависимости от настроек подключение

подтверждает администратор или пользователь. Запрос подтверждения приходит на электронную почту. Без подтверждения подключения данные не будут передаваться с сервиса NOMAD на устройство;

- ограничить доступ пользователей к мобильным приложениям:

  
  
  чтобы сотрудники могли пользоваться мобильным приложением, в системе Directum RX администратор включает их в состав участников предопределенной роли «Пользователи Solo»;

  
  
  можно использовать любую роль, существующую в системе Directum RX, или создать новую. Администратор настраивает разрешение или запрет доступа к мобильному приложению для участников роли;
- защитить конфиденциальную информацию. Для соответствия требованиям законодательства РФ в области хранения и обработки конфиденциальной информации рекомендуется настроить доступ к документам и записям справочников. Доступ настраивается для пользователей, групп пользователей или мобильных приложений. Можно запретить или разрешить загрузку данных на устройство, а также ограничить экспорт конфиденциальных документов в сторонние приложения;
- настроить внешний вид push-уведомлений о получении новых заданий. По умолчанию в уведомлении отображаются: тема задания, инициатор и система, в которой оно было создано. Из соображений конфиденциальности передачу этих данных можно запретить, и в уведомлении будет отображаться только количество новых заданий;
- удалять данные системы Directum RX в случае потери мобильного устройства или при увольнении сотрудника. Администратор может принудительно удалить данные системы Directum RX с телефона или планшета;
- настроить политики блокировки приложения. Администратор настраивает обязательную установку блокировки приложения, задает количество попыток разблокировки, а также включает запрет на использование биометрии для разблокировки на устройствах всех сотрудников, работающих в Directum Solo и Directum Jazz. Добавляемый PIN-код автоматически проверяется на сложность. Если он оказался небезопасным, в приложении отображается сообщение о том, что нужно ввести более надежный PIN-код;
- по требованию службы безопасности компании – запретить подключаться к Directum RX через Directum Solo и Directum Jazz с мобильных устройств на определенной операционной системе. Администратор настраивает запрет для iOS или Android. При попытке сотрудника авторизоваться в Solo и Jazz отображается сообщение о том, что подключение через устройство с этой операционной системой запрещено.

## Рекомендации для пользователей

Чтобы обеспечить безопасность данных на мобильном устройстве, необходимо соблюдать следующие рекомендации:

- настроить блокировку мобильного устройства по PIN-коду или биометрическим данным. Графический ключ или свайп-блокировка не являются достаточными мерами защиты.
- настроить блокировку приложения после 15 минут бездействия. В зависимости от модели и операционной системы устройства поддерживается два варианта снятия такой блокировки: по PIN-коду или биометрическим данным. Добавляемый PIN-код автоматически проверяется на сложность. Если он оказался небезопасным, в приложении отображается сообщение о том, что нужно ввести более надежный PIN-код.

После превышения числа попыток разблокировать устройство ввод PIN-кода или биометрических данных блокируется на некоторое время;

- не использовать устройства с jailbreak и root-доступом, так как это снижает безопасность мобильных приложений и хранящихся на устройстве данных;
- Android включить файловое или полнодисковое шифрование мобильного устройства;
- Android использовать приложения для удаленного управления устройствами, например, Android Device Manager;
- при потере устройства сообщить администратору о необходимости удалить загруженные в приложение данные с помощью служебной страницы сервиса NOMAD.

# Электронная подпись

Мобильные приложения Directum Jazz и Directum Solo используют для подписания механизмы:

- КриптоПро CSP;
- базовые СКЗИ, встроенные в ОС.
- Directum Solo аппаратный ключ (токен).

# КриптоПро CSP

Подписание с использованием КриптоПро CSP поддерживается во всех мобильных приложениях Directum RX. Для подписания требуется клиентская лицензия СКЗИ «КриптоПро CSP».

На компьютере пользователя генерируется контейнер с закрытым ключом. Далее контейнер копируется на мобильное устройство и во внутреннее хранилище КриптоПро CSP. После успешного копирования контейнера псевдоним (алиас) сертификата и его пароль записываются в локальную БД SQLite на мобильном устройстве.

В дальнейшем рекомендуется удалить контейнер с компьютера пользователя. Также для устройств с iOS рекомендуется расценивать устройство как носитель контейнеров и обеспечивать для него надлежащий уровень безопасности.

При запуске мобильного приложения происходит инициализация КриптоПро CSP.

Работа с КриптоПро CSP различается в зависимости от ОС:

Android мобильное приложение регистрируется в ОС как реализация ГОСТ-криптографических алгоритмов. Это позволяет работать с ними, как с любыми другими алгоритмами, используя базовые средства ОС;

iOS КриптоПро CSP встроен в приложение. Настраивается в разделе «Сертификаты» настроек приложения. Использует Microsoft Crypto API, реализуя ГОСТ-алгоритмы. Установка каких-либо дополнительных модулей не требуется.

Подписание с использованием КриптоПро CSP состоит из этапов:

1. Закрытый ключ загружается из хранилища по известному алиасу сертификата.
2. Подписываемый документ хешируется по указанному в сертификате алгоритму. Хеш формируется:

 средствами ОС с использованием КриптоПро CSP;

 средствами встроенного модуля КриптоПро CSP.

3. Полученный хеш вместе атрибутами, необходимыми для формирования подписи, подписывается в зависимости от ОС аналогично п.2.

# Базовые СКЗИ, встроенные в ОС

Для подписания используются средства, встроенные в ОС. Механизм зависит от используемой операционной системы: Android или iOS.

Поддерживается подписание сертификатами Microsoft CA. Встроенные в ОС поддерживают только RSA-сертификаты.

## Устройства на Android

Для подписания используются базовые средства ОС Android.

ПРИМЕЧАНИЕ. В ОС Android для работы с криптографией используется набор библиотек Spongy Castle из стандартной поставки ОС.

На компьютере пользователя создается контейнер, содержащий закрытый ключ: файл с расширением .pfx или .p12. После этого контейнер копируется на мобильное устройство в папку приложения. После завершения настройки подписания контейнер удаляется из папки на устройстве автоматически. В дальнейшем рекомендуется удалить контейнер с компьютера пользователя.

Сертификат хранится в системном хранилище KeyChain.

Подписание базовыми средствами ОС Android состоит из тех же этапов, что и подписание средствами КриптоПро CSP.

## Устройства на iOS

Подписание реализовано средствами платформы .NET – обертки Microsoft RSACryptoServiceProvider.

ПРИМЕЧАНИЕ. Платформа .NET в мобильных приложениях – это входящая в состав приложения кроссплатформенная реализация платформы .NET Mono.

На компьютере пользователя создается контейнер с закрытым ключом с расширением .pfx. После этого контейнер копируется на мобильное устройство в раздел «Документы» приложения.

Далее в разделе «Настройки» приложения ключ импортируется в закрытое хранилище и автоматически удаляется из открытого раздела «Документы».

Подписание базовыми средствами платформы .NET состоит из тех же этапов, что и подписание средствами КриптоПро CSP.

# Хранение контейнера с закрытым ключом сертификата Microsoft CA на мобильном устройстве

## Устройства на Android

Контейнер с закрытым ключом сертификата Microsoft CA хранится в системном хранилище KeyChain. Приложение разово запрашивает у пользователя доступ к контейнеру и сохраняет полученный алиас в локальную БД SQLite на мобильном устройстве. Последующие обращения к контейнеру происходят по уже известному алиасу без отдельного запроса.

При хранении закрытых ключей в хранилище KeyChain на устройстве должна быть установлена блокировка экрана. Рекомендуется использовать пароль или PIN-код.

### Устройства на iOS

Контейнер с закрытым ключом помещается в файловый каталог приложения и доступен только для процессов, авторизованных на обращение. Контейнер хранится в зашифрованном виде.

Чтобы получить доступ к ключу, мобильное приложение генерирует уникальное имя для каждого сохраняемого контейнера. Приложение сохраняет алиас и пароль для контейнера в системное шифрованное хранилище KeyChain. Доступ к хранилищу запрещен, если устройство заблокировано PIN-кодом или Touch ID.

## Аппаратный ключ (токен)

В Directum Solo поддерживается подписание алгоритмами ГОСТ или RSA. Для взаимодействия с токенами используется интерфейс стандарта PKCS#11. Типы токенов, с помощью которых можно подписывать документы в Directum Solo, см. в руководстве пользователя Directum Solo для iOS и Android.

Если используется токен с копируемым сертификатом, перед использованием его рекомендуется отформатировать и установить использование шифрованного соединения.

Процесс подписания с помощью токена состоит из этапов:

1. Поиск подключенных токенов и формирование соединения с токеном.
2. Сопоставление сертификатов: пользовательского и найденного на токене, и определение того, который требуется использовать.
3. Аутентификация пользователя путем ввода PIN-кода токена.
4. Получение ID закрытого ключа, соответствующего найденному сертификату.
5. Тело подписываемого документа хешируется указанным в сертификате алгоритмом. Хеш формируется средствами ОС. Подробнее см. в разделе «КриптоПро CSP».
6. Полученный хеш передается в токен и подписывается закрытым ключом с указанным ID. При этом закрытый ключ не покидает токен, все криптографические преобразования выполняются аппаратно.