Target CI вер. 1.5

РУКОВОДСТВО ПО КИБЕРБЕЗОПАСНОСТИ

Русский

Обновлено: сентябрь 2025 г.

A Sonova Brand

Содержание

1. ВВЕДЕНИЕ

В настоящем документе представлена техническая информация по безопасности и конфиденциальности системы программного обеспечения Target CI вер. 1.5 компании Advanced Bionics, далее именуемой «программным обеспечением для настройки». Программное обеспечение для настройки предназначено для использования квалифицированными специалистами-сурдологами (HCP) с целью настройки слуховых устройств у пациентов, которым установлены кохлеарные импланты компании Advanced Bionics.

В настоящем документе особое внимание уделяется вопросам кибербезопасности и конфиденциальности, которые связаны с использованием программного обеспечения для настройки. Он включает оценку средств управления безопасностью и конфиденциальностью, которые в настоящее время интегрированы в программное обеспечение, а также тех, которые, как ожидается, будут применяться и настраиваться в ИТ-среде, в которой продукт будет использоваться по назначению.

В настоящем документе не содержится техническая информация о безопасности и конфиденциальности относительно:

- предыдущих версий программного обеспечения для настройки AB;
- программного обеспечения AB, отличного от Target CI вер. 1.5;
- веб-сайтов AB;
- мобильных приложений AB;
- слуховых устройств AB.

1.1 ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

Сокращение	Термин
FSW	Программное обеспечение для настройки
HCP	Специалист-сурдолог
SaMD	Программное обеспечение как медицинское устройство
AB	Advanced Bionics
IFU	Инструкция по применению

2. ДРУГИЕ РЕСУРСЫ

2.1 ПОДДЕРЖКА КЛИЕНТОВ

Лицам, находящимся в США и Канаде, компания Advanced Bionics предлагает воспользоваться бесплатной горячей линией для технических консультаций (телефон 877-271-6727); помощь квалифицированных специалистов доступна с понедельника по пятницу, с 5:00 до 17:00 по тихоокеанскому времени.

Лицам, находящимся за пределами США и Канады, техническое обслуживание предоставляется в регионе проживания. Если у вас есть вопросы о программном обеспечении для настройки, соответствующем аппаратном обеспечении или возникли иные вопросы о программировании, обратитесь к представителю AB в вашем регионе.

2.2 ПОРТАЛ AB PRO PORTAL

Программное обеспечение для настройки и соответствующую документацию можно загрузить с сайта https://www.abproportal.com или в веб-клиенте Sonova. Требуется вход в учетную запись. Этот ресурс может быть недоступен в некоторых странах; для получения дополнительной информации обратитесь к представителю AB.

2.3 РАСШИРЕННОЕ РУКОВОДСТВО ПО УСТАНОВКЕ

Расширенное руководство по установке Target CI вер. 1.5 предоставляется по запросу. В руководстве представлена техническая информация о подходящем установщике программного обеспечения для настройки, включая параметры командной строки для тихой и автоматической установки.

2.4 MDS2

Заявление производителя о раскрытии информации о безопасности медицинских устройств (MDS2) — это стандартная для отрасли форма, содержащая ответы на вопросы о безопасности и конфиденциальности программного обеспечения для настройки AB. Форма предоставляется по запросу.

2.5 ИНСТРУКЦИЯ ПО ПРИМЕНЕНИЮ

Инструкция по применению поставляется вместе с установочным носителем программного обеспечения. Для некоторых стран электронная инструкция по применению доступна для загрузки по адресу: www.advancedbionics.com/ifu

Следующие разделы инструкции по применению могут быть важными для ИТ-специалистов:

- Описание продукта
- Минимальные требования к системе и эксплуатационные характеристики
- Указания по информационной безопасности
- Инструкции по установке
- Техническая поддержка

2.6 HIMSA

HIMSA — сторонний поставщик программного обеспечения, выпускающий Noah System 4, систему программного обеспечения, разработанную для отрасли слухопротезирования, которая предоставляет специалистам-сурдологам независимую от поставщика систему для выполнения задач, связанных с клиентом.

Дополнительно в программном обеспечении для настройки можно настроить сохранение данных в Noah System 4 вместо локальной базы данных.

Веб-страница безопасности HIMSA содержит ответы на распространенные вопросы по информационной безопасности, касающиеся Noah System 4.

https://www.himsa.com/support/noah-enterprise-support/security-questionnaire-support/

https://www.himsa.com/support/noah-enterprise-support/security-considerations/

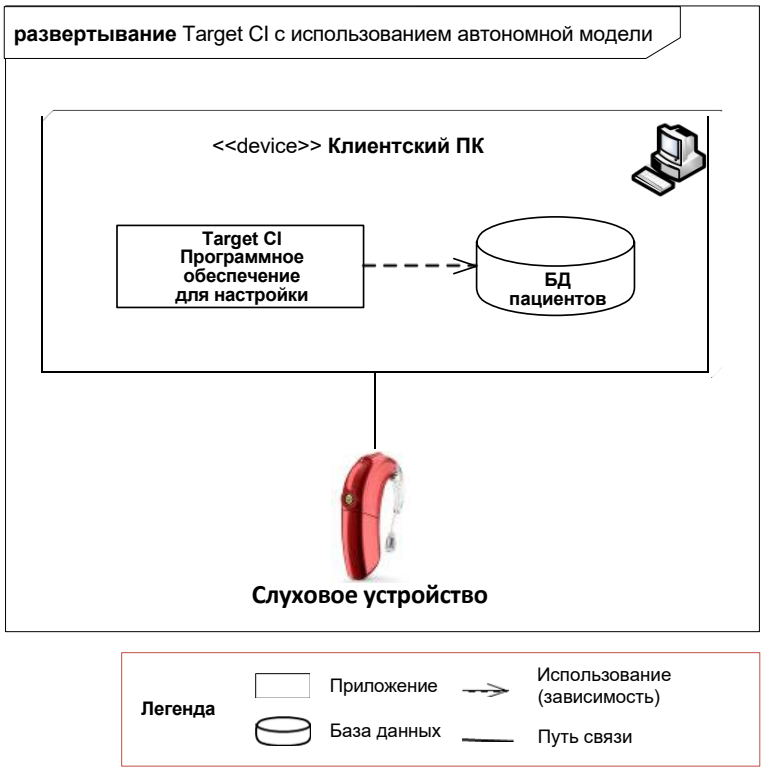
Дополнительную информацию по безопасности см. в разделе «Безопасность» учебного центра HIMSA:
https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/

3. СЕТЕВЫЕ И КОНТЕКСТНЫЕ СХЕМЫ

Поддерживаются две модели развертывания программного обеспечения для настройки, которое представляет собой клиентское приложение (SaMD), устанавливаемое на коммерчески доступный готовый ПК с ОС Microsoft Windows. Программное обеспечение не включает в себя какое-либо аппаратное обеспечение или операционную систему.

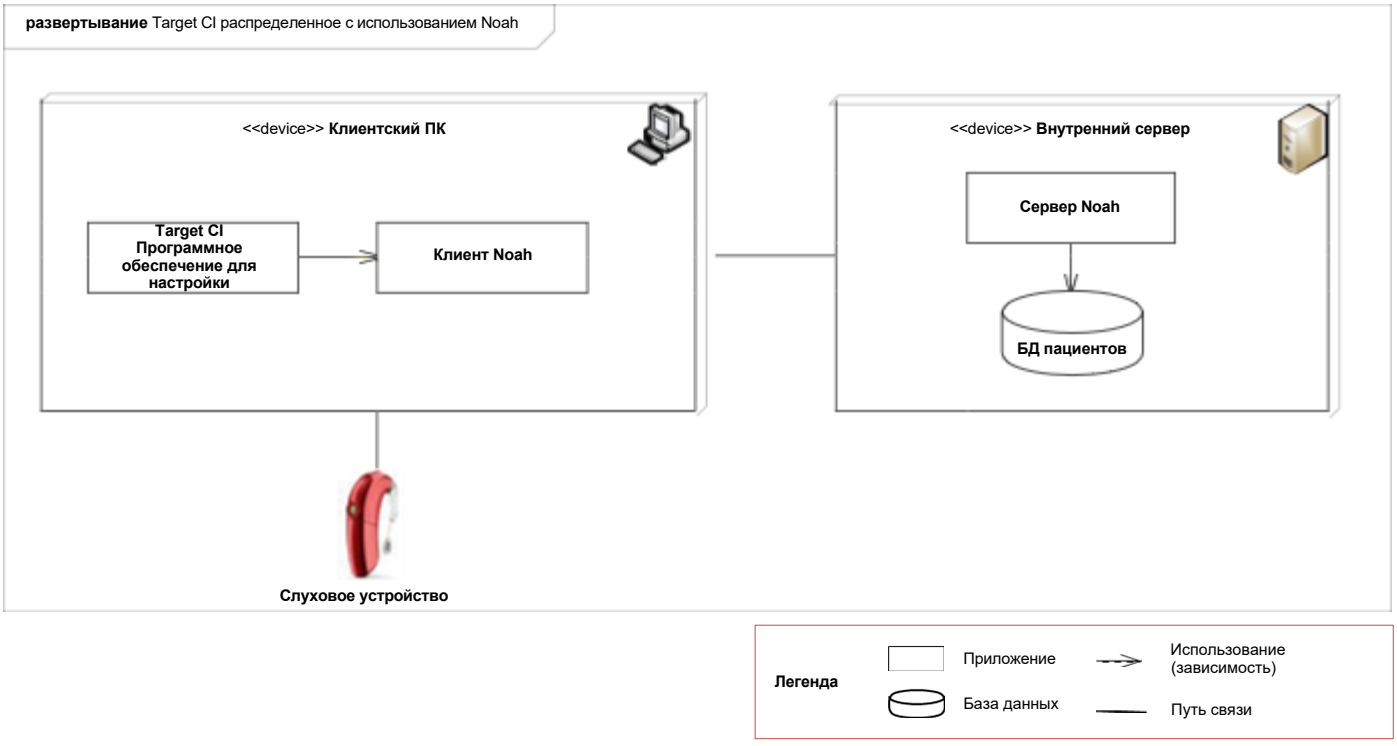
3.1 МОДЕЛЬ РАЗВЕРТЫВАНИЯ 1: АВТОНОМНАЯ

В модели автономного развертывания программное обеспечение для настройки развертывается на клиентском ПК. База данных пациентов хранится на том же ПК и устанавливается вместе с программным обеспечением для настройки.



3.2 МОДЕЛЬ РАЗВЕРТЫВАНИЯ 2: РАСПРЕДЕЛЕННОЕ РАЗВЕРТЫВАНИЕ С ИСПОЛЬЗОВАНИЕМ NOAH

В модели распределенного развертывания с использованием Noah программное обеспечение для настройки развертывается на одном или нескольких клиентских ПК. Сторонняя система управления пациентами Noah развертывается на внутреннем сервере, доступном для клиентских ПК. База данных пациентов хранится на сервере Noah и доступна по сети одному или нескольким клиентским ПК.

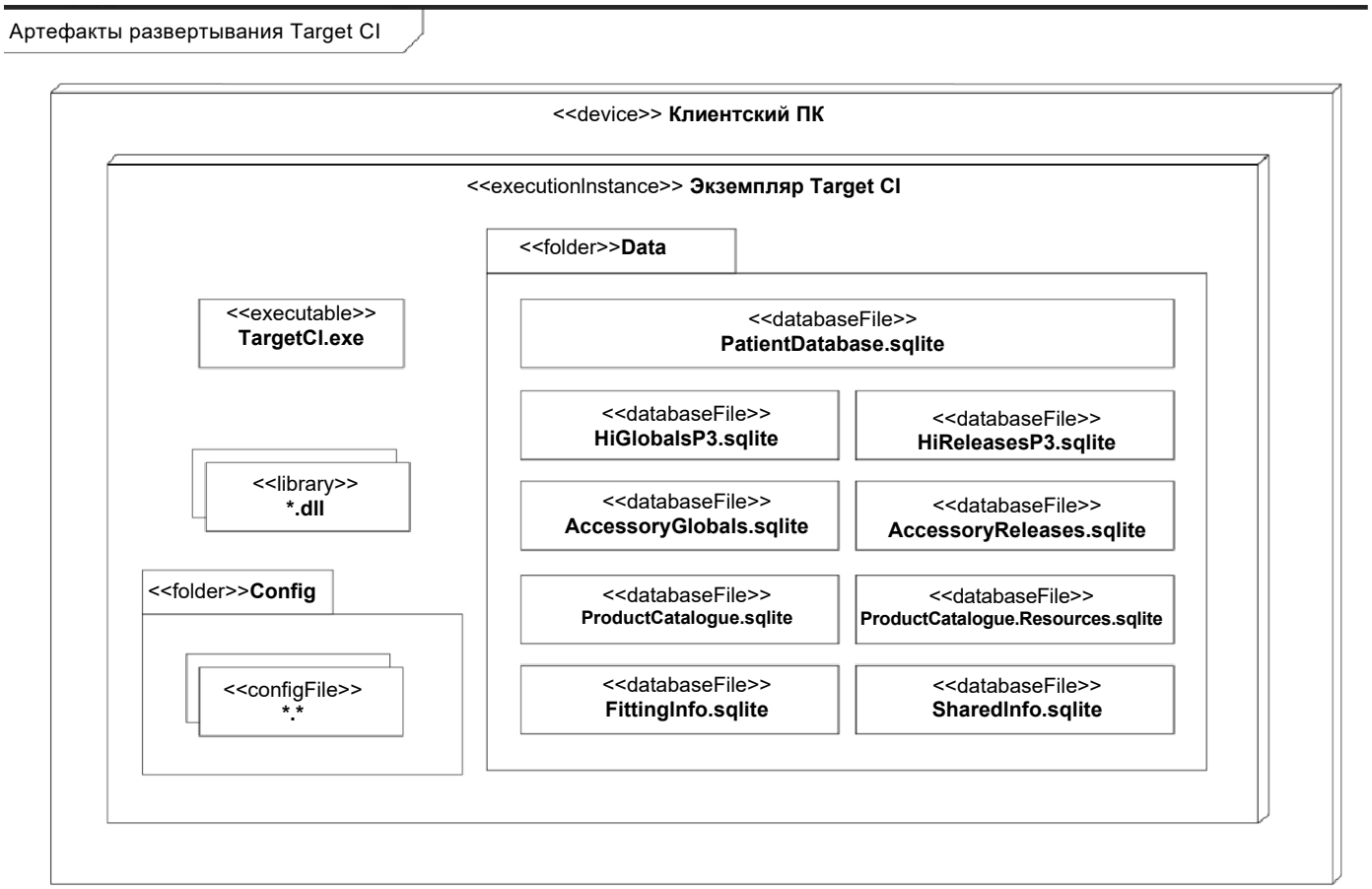


3.3 АРТЕФАКТЫ РАЗВЕРТЫВАНИЯ

Программное обеспечение для настройки устанавливается с исполняемым файлом и набором связанных файлов, включая DLL-файлы компонентов, файлы конфигурации и файлы базы данных SQLite. Файлы конфигурации устанавливаются в папку %ProgramData%\ Advanced Bionics\Target CI\Target CI\Config, файлы базы данных устанавливаются в папку %ProgramData%\Advanced Bionics\Target CI\Target CI\Data. Папка Data (Данные) содержит один файл транзакционной базы данных и несколько файлов информационной базы данных.

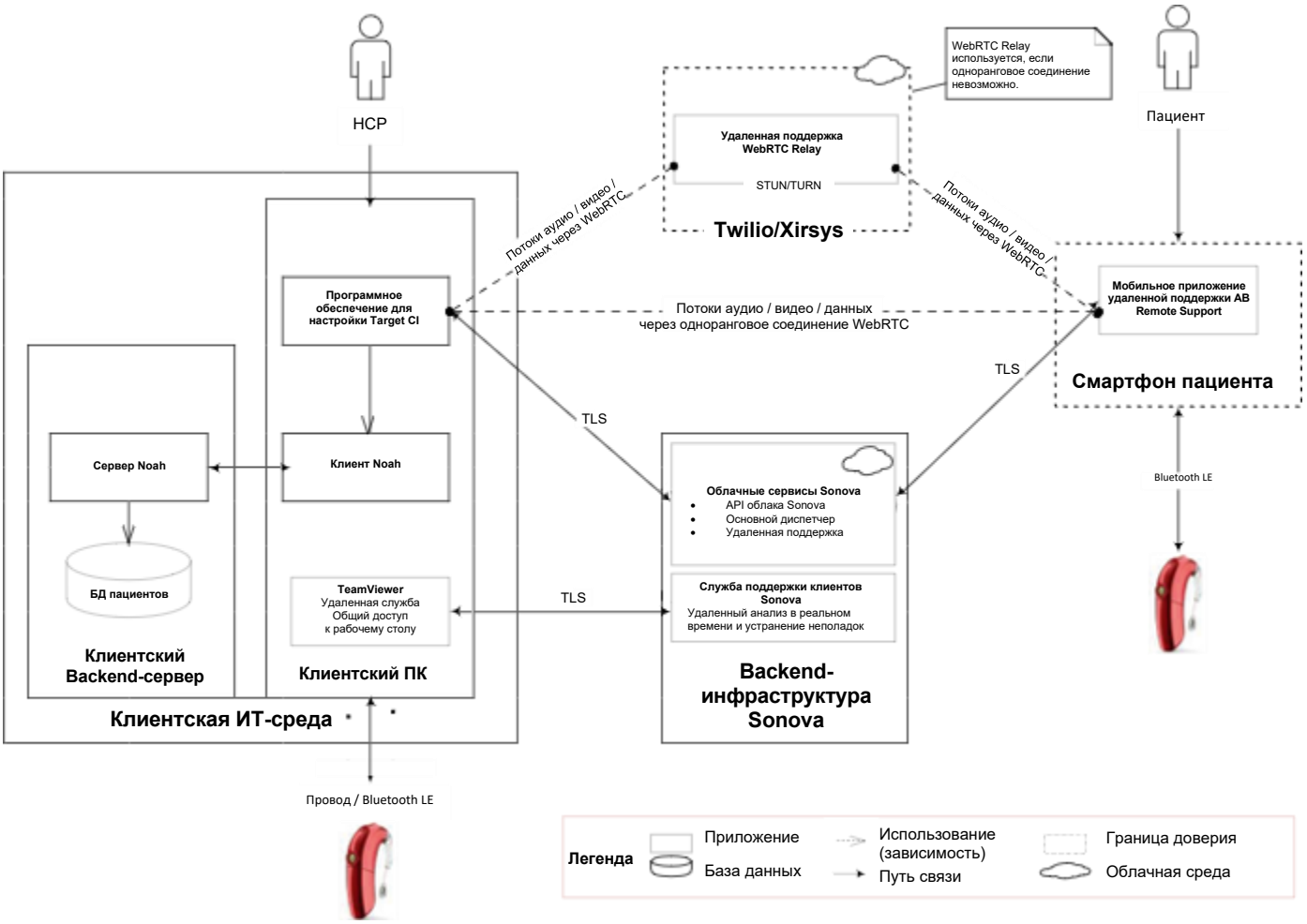
В транзакционной базе данных PatientDatabase.sqlite хранятся демографические данные и данные настройки пациента, она будет установлена только при развертывании программного обеспечения для настройки в автономном режиме.

При развертывании программного обеспечения для настройки в качестве модуля Noah система Noah предоставляет программному обеспечению для настройки необходимые службы для сохранения данных о пациентах. Остальные файлы SQLite являются неотъемлемой частью программного обеспечения для настройки и требуются для всех моделей развертывания.



3.4 ВЗАИМОДЕЙСТВИЕ СИСТЕМ

Приведенные ниже схема и таблица иллюстрируют основные взаимосвязи систем. Как правило, используется только часть имеющихся взаимосвязей.



Источник / место назначения	Служба	Протокол	Порт	Описание
Слуховые устройства	Обмен данными со слуховыми устройствами	Проводное соединение / Bluetooth® с низким энергопотре-блением	Н/П	Используется для обмена данными со слуховыми устройствами для управления, настройки, определения статуса и считывания данных
Noah	Noah 4 ModuleAPI	.NET Remoting	Н/П	Основной интерфейс для модуля, используемого для доступа к программному обеспечению Noah (только в модели распределенного развертывания Noah)
Облачные сервисы Sonova	Sonova Cloud API, основной диспетчер,	SOAP, REST	443	Сервисы Sonova, размещенные в центре обработки данных Microsoft Azure, используются для:

Источник / место назначения	Служба	Протокол	Порт	Описание
	удаленная поддержка			• извлечения данных конфигурации клиента программного обеспечения для настройки из внутреннего хранилища Sonova; • передачи данных журнала и аналитики; • организации сеансов удаленной настройки в режиме реального времени.
Twilio / Xirsys, мобильное приложение AB Remote Support	Удаленная поддержка	WebRTC	Список портов доступен по запросу	Облачные коммуникационные сервисы Twilio размещаются на сторонних облачных платформах, в частности Amazon Web Services (AWS) и Google Cloud Platform (GCP). Эти сервисы используются исключительно функцией удаленной поддержки программного обеспечения для настройки, которая позволяет осуществлять передачу сигналов WebRTC и сеансы удаленной настройки в режиме реального времени.
Служба поддержки клиентов AB	Совместное использование рабочего стола	Проприетарный протокол TeamViewer	5938, 443, 80 См. TeamViewerPorts	Используется для удаленного анализа в реальном времени и устранения неполадок, влияющих на установку программного обеспечения для настройки. Подробную информацию см. в разделе 6.6 УДАЛЕННАЯ СЛУЖБА.

4. СИСТЕМНЫЕ ТРЕБОВАНИЯ

Операционная система	Windows 10 Pro / Enterprise 64-битная версия
.NET Framework	Версия 4.8
Процессор	Intel® Core™ i5 или эквивалент с аналогичной или лучшей производительностью
Оперативная память	4 ГБ или больше
Свободное пространство на жестком диске	3 ГБ или больше
Минимальные требования к дисплею	• Разрешение 1280 x 1024 (максимальное масштабирование 125%) • 24-битный цвет
Драйверы устройств	• Драйвер Noahlink Wireless (при использовании стороннего интерфейса программирования Noahlink Wireless, подключаемого через USB, требуется последняя версия, доступная на сайте HIMSA). • Драйвер CPI-3 (требуется при использовании интерфейса программирования CPI-3, подключенного через USB).
База данных	SQLite или Noah System 4 (версия 4.14 или выше)
Интернет-соединение	Для удаленной поддержки и ведения журнала аналитики требуется подключение к Интернету, см. раздел 3.4 «Взаимодействие систем»; при использовании сетевой версии Noah System 4 требуется интранет.
Сетевые порты	См. раздел 3.4 «Взаимодействие систем»; для портов, используемых системой Noah 4, см. раздел 2. «Другие ресурсы», подраздел «HIMSA».

5. УСТАНОВКА

5.1 ТРЕБОВАНИЯ

Для установки программного обеспечения для настройки требуется учетная запись администратора. После установки программное обеспечение можно запускать без административных или более высоких прав доступа.

Информацию о проверке целостности программного обеспечения перед установкой см. в разделе 8 «Целостность программного обеспечения».

Перед установкой системным администраторам рекомендуется убедиться в следующем:

• устанавливаемая версия программного обеспечения для настройки является новейшей;

• базовая операционная система обновлена.

5.2 ТИПЫ УСТАНОВЩИКОВ

Для установки программного обеспечения для настройки доступны два установщика:

• Стандартный установщик

• Установщик IT Professional

Установщик IT Professional представляет собой один MSI-файл, из которого исключены обязательные компоненты, в остальном он эквивалентен стандартному установщику.

Обязательные компоненты включают Microsoft .NET Framework вер. 4.8 и распространяемые пакеты Microsoft Visual C++.

Оба установщика поддерживают расширенные сценарии установки, включая тихую установку.

Установщик IT Professional следует использовать только в том случае, если вашей организации требуется установка обязательных компонентов и необходимо, чтобы управление ими осуществляла ваша организация, а не установщик программного обеспечения для настройки. Во всех остальных случаях следует использовать стандартный установщик.

Установщик IT Professional можно получить у клинического представителя AB. Установщик IT Professional нельзя использовать для восстановления, переустановки или удаления установок, выполненных с помощью стандартного установщика. Стандартный установщик нельзя использоваться для восстановления, переустановки или удаления установок, выполненных установщиком IT Professional.

6. КОНТРОЛЬ БЕЗОПАСНОСТИ

Программное обеспечение для настройки представляет собой клиентское приложение, устанавливаемое на коммерчески доступный готовый ПК с ОС Microsoft Windows. Программное обеспечение для настройки можно установить как отдельное приложение или как модуль Noah.

6.1 АУТЕНТИФИКАЦИЯ – АВТОНОМНОЕ РАЗВЕРТЫВАНИЕ

Если программное обеспечение для настройки установлено как автономное приложение, оно использует механизмы контроля доступа, предоставляемые операционной системой хоста. IT-персонал заказчика может настроить операционную систему хоста для управления аутентификацией. Программное обеспечение для настройки не имеет такой встроенной функции. Advanced Bionics рекомендует, чтобы каждый пользователь входил в операционную систему хоста, используя уникальную учетную запись.

6.2 АУТЕНТИФИКАЦИЯ – РАЗВЕРТЫВАНИЕ С ИСПОЛЬЗОВАНИЕМ NOAH

Если программное обеспечение для настройки установлено как модуль Noah, контроль доступа обеспечивается системой Noah System 4. Информацию об элементах аудита, используемых системой Noah System 4, см. на сайте www.HIMSA.com.

6.3 АВТОРИЗАЦИЯ

Программное обеспечение для настройки не ограничивает доступ к своим функциям на основе ролей отдельных пользователей. Программное обеспечение поддерживает одну основную функцию — настройку слуховых устройств пациента — и одну роль специалиста по настройке. Контроль доступа на основе ролей не применяется.

6.4 АУДИТ – АВТОНОМНОЕ РАЗВЕРТЫВАНИЕ

Если программное обеспечение для настройки установлено как автономное приложение, оно использует механизмы аудита, предоставляемые операционной системой хоста. Программное обеспечение для настройки не имеет подобной интегрированной функции. Операционная система хоста может быть настроена ИТ-персоналом заказчика для ведения журнала запусков / выполнения программного обеспечения для настройки и входа пользователей. Advanced Bionics рекомендует, чтобы каждый пользователь входил в операционную систему хоста с уникальной учетной записью для упрощения аудита.

6.5 АУДИТ – РАЗВЕРТЫВАНИЕ С ИСПОЛЬЗОВАНИЕМ NOAH

Если программное обеспечение для настройки установлено как модуль Noah, журналы аудита предоставляются системой Noah. С информацией об элементах аудита, используемых Noah System 4, можно ознакомиться на сайте https://www.himsa.com/.

6.6 УДАЛЕННЫЙ ДОСТУП

Функция общего доступа к рабочему столу позволяет выполнять удаленный анализ в режиме реального времени и устранять неполадки, влияющие на установку программного обеспечения для настройки. Эта функция основана на стороннем инструменте TeamViewer QuickSupport (развертываемом по умолчанию вместе с программным обеспечением для настройки) и позволяет специалистам службы поддержки клиентов AB удаленно подключаться к компьютеру HCP и получать полный контроль над его рабочим столом, включая доступ к базовой операционной и файловой системе.

Для установления сеанса общего доступа к рабочему столу требуется взаимодействие с HCP. Сначала HCP необходимо запустить инструмент TeamViewer QuickSupport (например, с помощью программного обеспечения для настройки Target CI) и сообщить свои учетные данные TeamViewer группе поддержки AB по внеполосному каналу связи (например, по телефону).

Имя члена команды поддержки AB и его идентификатор TeamViewer по умолчанию отображаются на мониторе компьютера HCP во время каждого активного сеанса общего доступа к рабочему столу.

Весь сетевой трафик в режиме общего доступа к рабочему столу защищен с соблюдением или превышением стандартов криптографических протоколов и алгоритмов (обмен открытыми / личными ключами RSA и шифрование сеанса AES 256 бит).

TeamViewer QuickSupport можно удалить вручную, не затрагивая другие функции Target FSW. Программа установки Target FSW поддерживает параметр установки с использованием командной строки, который позволяет выполнить установку Target FSW из командной строки без включения инструмента TeamViewer QuickSupport.

7. ЗАЩИТА ИНФОРМАЦИИ

7.1 ПОЛИТИКА КОНФИДЕНЦИАЛЬНОСТИ ADVANCED BIONICS

Политику конфиденциальности, описывающую, как Advanced Bionics собирает, передает, хранит и использует персональные данные, можно загрузить по ссылке: AdvancedBionics.com/privacy.

Компания Advanced Bionics не размещает, не хранит, не создает резервные копии и не имеет доступа к каким-либо данным, хранящимся в программном обеспечении для настройки или базах данных Noah, если только эти данные явно не передаются Advanced Bionics.

7.2 ФЕДЕРАЛЬНЫЕ СТАНДАРТЫ ОБРАБОТКИ ИНФОРМАЦИИ (FIPS)

Target CI вер. 1.5 соответствует стандартам шифрования FIPS 140-2.

7.3 БЕЗОПАСНОСТЬ ПРИ ПЕРЕДАЧЕ ДАННЫХ

Коммуникационная безопасность обеспечивается и активируется при входящей и исходящей передаче любых данных по сети программным обеспечением для настройки. За исключением функции удаленной поддержки (которая использует протокол WebRTC) и обмена данными со слуховыми устройствами и аксессуарами по Bluetooth, все остальные соединения защищены протоколом Transport Layer Security (TLS), который обеспечивает конфиденциальность, целостность и подлинность информации.

TLS

Конфигурация TLS соответствует современным передовым практикам и рекомендациям по безопасности, изложенным в документе BCP 195 «Рекомендации по безопасному использованию TLS и DTLS», включая следующее:

- Не поддерживаются версии SSL и TLS до 1.2.
- Не поддерживаются наборы шифров, использующие криптографические алгоритмы, обеспечивающие безопасность менее 128 бит.
- Поддержка рекомендуемых расширений TLS BCP 195
- Не поддерживаются небезопасные расширения BCP 195

DTLS

Шифрование является обязательной функцией WebRTC и применяется ко всем потокам мультимедиа, передаваемым через WebRTC. Используемый протокол шифрования зависит от типа канала; потоки данных шифруются с помощью DTLS, а потоки мультимедиа — с помощью безопасного протокола передачи данных в реальном времени (Secure Real-time Transport Protocol, SRTP), который используется, поскольку является более легким вариантом по сравнению с DTLS.

Подробную информацию о настройке безопасности службы удаленной поддержки WebRTC см. по ссылке:

https://developer.liveswitch.io/liveswitch-server/server/security.html

BLE

Соединение со слуховыми устройствами и аксессуарами по Bluetooth с низким энергопотреблением по умолчанию зашифровано, и его целостность защищена (за исключением случаев использования для идентификации и обнаружения). Также время работы режима сопряжения по Bluetooth слухового устройства ограничено по времени. Подробную информацию о безопасности канала связи Bluetooth см. в имеющейся документации к слуховому устройству.

7.4 БЕЗОПАСНОСТЬ В ПОКОЕ

База данных пациентов – модель автономного развертывания

Если программное обеспечение для настройки установлено как автономное приложение, база данных пациентов хранится локально по адресу: C:\ProgramData\Advanced Bionics\Target CI\Target CI\Data

По умолчанию эти записи не шифруются в состоянии покоя. Защищенная медицинская информация (PHI) и Личная идентификационная информация (PII) хранятся в базе данных, которая является внутренней для программного обеспечения для настройки, и не передаются по сети.

В некоторых юрисдикциях нормативные акты могут требовать шифрования всех данных пациентов для исключения потенциальной ответственности в случае потери или кражи данных. Включите BitLocker или эквивалентное полное шифрование диска (на уровне ОС или аппаратного обеспечения), чтобы защитить данные от несанкционированного доступа или копирования, пока они находятся в состоянии покоя.

BitLocker — встроенная функция Windows, которая шифрует весь диск и требует аутентификации для доступа. Перед включением BitLocker обязательно ознакомьтесь с официальными рекомендациями Microsoft и политикой информационной безопасности вашей организации.

Как включить BitLocker

Для управления BitLocker требуются права администратора.

1. Выполните поиск по запросу Manage BitLocker (Управление BitLocker).

   Откройте меню Start (Пуск), введите Manage BitLocker (Управление BitLocker) и выберите его в результатах поиска.

2. Выберите системный диск.

   Для настройки параметров шифрования выберите диск, на котором установлена ОС Windows.

3. Выберите Unlock Method (Метод разблокировки).

   Выберите один из следующих вариантов:

   - только TPM
   - TPM + PIN
   - TPM + USB key (TPM + USB-ключ)

   При выборе метода разблокировки следуйте рекомендациям Microsoft и политике информационной безопасности вашей организации.

4. Создайте резервную копию ключа восстановления.

   Создайте резервную копию ключа восстановления, используя безопасные, одобренные предприятием методы. Рекомендуемые варианты включают:

   - Хранение в Microsoft Entra ID (ранее Azure AD) или Active Directory для устройств, подключенных к домену.

   - Сохранение в безопасном сетевом расположении с контролируемым доступом, шифрованием и ведением журнала аудита.

   - Использование управляемого решения для депонирования ключей, одобренного вашей организацией.

   Избегайте сохранения ключа на локальных дисках, USB-накопителях или его распечатки, если это явно не разрешено политикой. Ключи восстановления должны быть защищены с той же строгостью, что и другие конфиденциальные учетные данные, и немедленно заменены в случае раскрытия.

5. Запустите шифрование.

   Список элементов для выбора:

   - Весь диск — рекомендуется для большинства корпоративных сценариев. Шифрует все сектора, включая неиспользуемое пространство, для предотвращения остаточной информации.

База данных пациентов – модуль распределенного развертывания Noah

При установке программного обеспечения для настройки в качестве модуля Noah личная идентификационная информация пациентов сохраняется в базе данных, размещенной Noah. База данных пациентов, размещенная Noah, может находиться на другом компьютере. Личная идентификационная информация и другие данные пациента сохраняются с помощью программного обеспечения Noah, шифрование данных пациента в состоянии покоя обеспечивается системой Noah. Программное обеспечение для настройки может отправлять / принимать личную идентификационную информацию с помощью проводного или беспроводного сетевого соединения, если база данных Noah настроена для сетевого доступа.

Личная идентификационная информация, хранящаяся в сетевой базе данных Noah, будет видна другим пользователям устройств на разных ПК, у которых имеются разрешения на доступ к той же сетевой базе данных. Базу данных Noah также можно настроить для несетевого доступа и установить на том же ПК, что и программное обеспечение для настройки.

Noah блокирует доступ программного обеспечения для настройки к базе данных записей пациентов. Когда пользователь открывает запись пациента в программном обеспечении для настройки через клиент Noah, программное обеспечение для настройки может только читать и записывать данные в текущую открытую запись пациента и не может получить доступ к другим записям пациентов в базе данных Noah.

Стандарты шифрования, используемые Noah System 4, см. в разделе www.HIMSA.com.

Файлы экспорта RMA

Программное обеспечение для настройки позволяет экспортировать информацию о клиенте в файл. Файл RMA можно отправить Advanced Bionics для решения вопросов RMA или связанных с поддержкой.

Файл RMA асимметрично зашифрован RSA с использованием ключа длиной 512 бит. Программное обеспечение для настройки не имеет возможности расшифровать файл RMA.

Анонимизированные файлы экспорта

Программное обеспечение для настройки позволяет экспортировать информацию о клиенте в анонимизированный файл. Личная идентификационная информация клиента, в частности дата рождения и имя, заменяются общими значениями. Шифрование файла не осуществляется, и его можно импортировать в тот же или другой экземпляр программного обеспечения для настройки.

Стандартные файлы экспорта

Программное обеспечение для настройки позволяет экспортировать информацию клиента в стандартный файл экспорта. Файл использует фирменный двоичный формат без шифрования. Файл можно импортировать в тот же или другой экземпляр программного обеспечения для настройки. При использовании этой функции пользователи программного обеспечения для настройки должны убедиться, что стандартные файлы экспорта обрабатываются в соответствии с их локальными ИТ-политиками по управлению незашифрованной личной идентификационной информацией.

Слуховое устройство

Программное обеспечение для настройки сохраняет информацию о клиенте на его слуховом устройстве. Личная идентификационная информация, в частности имя и дата рождения клиента, не сохраняется в слуховом устройстве. Остальная информация, не относящаяся к личной идентификационной информации, сохраняется с использованием шифрования PBKDF2 со 128-битным ключом.

Программное обеспечение для настройки может отправлять / принимать информацию о клиенте, не являющуюся личной идентификационной информацией, в слуховой аппарат / от слухового аппарата через фирменное проводное устройство (например, CPI-3), мобильное приложение AB Remote Support или устройство NoahLink Wireless. Устройство NoahLink Wireless подключается к слуховому устройству с помощью технологии Bluetooth с низким энергопотреблением (BLE) по стандартному каналу BLE с шифрованием 128 бит AES.

8. ЦЕЛОСТНОСТЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

8.1 ПРОВЕРКА ЗАГРУЖЕННОГО УСТАНОВОЧНОГО НОСИТЕЛЯ

Установочный носитель программного обеспечения для настройки Target CI можно загрузить в некоторых регионах с портала Pro Portal компании Advanced Bionics или в веб-клиенте Sonova Web Client. Загруженный установочный носитель можно аутентифицировать с помощью любого надежного инструмента хеширования SHA-256.

Хеш SHA256 для стандартного установочного zip-файла:
A42B8F41A5A4111D1CDF67394FFBBFBCDF2FB6215EC2696DB310B3AED6D4DD83

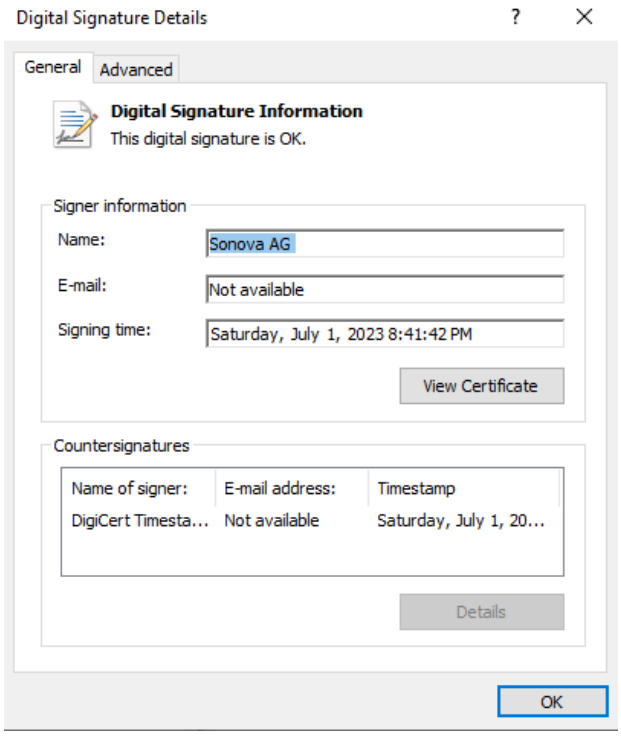
Хеш SHA256 для установочного zip-файла IT Professional:
DDAD362CC3213EFEA702D9F4A61740B34EDF794FE997811B6B2C908CE754B25F

8.2 РУЧНАЯ ПРОВЕРКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ НАСТРОЙКИ ПЕРЕД УСТАНОВКОЙ

Пользователи могут выполнить следующие действия для проверки целостности и подлинности программного обеспечения для настройки перед установкой:

1. Откройте проводник Windows и перейдите в корневую папку установочного носителя программного обеспечения для настройки. Если ваш установочный носитель — это флэш-накопитель, вставьте его в USB-порт и перейдите в его корень. Если ваш установочный носитель представляет собой zip-файл, распакуйте его в папку и перейдите в эту папку.

2. Щелкните правой кнопкой мыши по файлу SonovaVerify.exe и выберите в контекстном меню пункт Properties (Свойства).
3. Выберите вкладку Digital Signatures (Цифровые подписи).
4. Дважды щелкните подпись SHA256 «Sonova AG».
5. Проверьте правильность элементов подписи. В частности, убедитесь, что в верхней части отображается сообщение «The digital signature is OK» (Цифровая подпись в порядке), а имя и время подписания соответствуют следующему изображению:



1. Закройте всплывающие диалоговые окна и дважды щелкните файл SonovaVerify.exe.
2. Убедитесь, что отображается сообщение «NO ERRORS DETECTED.» (ОШИБОК НЕ ОБНАРУЖЕНО.), как показано на следующем рисунке:

На изображении показано, что программа SonovaVerify выполнила аутентификацию и проверку цифровых подписей всех файлов на установочном носителе, включая установщик. Это подтверждает, что установочный носитель не был подделан, поврежден или иным образом скомпрометирован. SonovaVerify выведет предупреждения или сообщения об ошибках, если файлы или папки отсутствуют или на установочный носитель были добавлены непредвиденные файлы или папки.

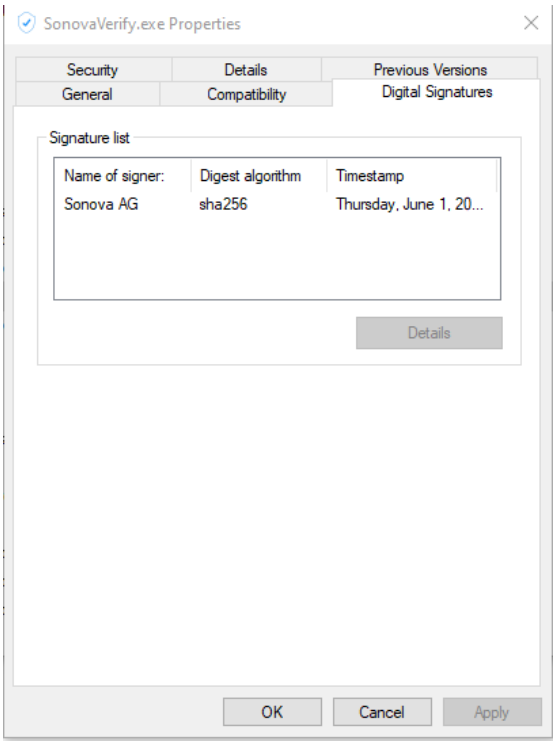
8.3 АВТОМАТИЧЕСКАЯ ПРОВЕРКА ЦЕЛОСТНОСТИ УСТАНОВЛЕННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ НАСТРОЙКИ

SonovaVerify интегрирована с программным обеспечением для настройки и запускается при каждом запуске приложения для проверки целостности программных файлов программного обеспечения для настройки. Программные файлы имеют цифровую подпись с использованием стандартных отраслевых методов и сертификатов, выданных доверенным центром сертификации. Если какие-либо программные файлы скомпрометированы, программное обеспечение уведомляет пользователя посредством предупреждающих сообщений.

8.4 РУЧНАЯ ПРОВЕРКА ЦЕЛОСТНОСТИ УСТАНОВЛЕННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ НАСТРОЙКИ

Пользователи могут выполнить следующие шаги для проверки целостности и подлинности установленного программного обеспечения для настройки в любое время без запуска программного обеспечения для настройки:

1. Откройте проводник Windows и перейдите к исполняемой папке программного обеспечения для настройки, которая обычно располагается в: C:\Program Files (x86)\Advanced Bionics\Target CI\
2. Щелкните правой кнопкой мыши по файлу SonovaVerify.exe и выберите в контекстном меню пункт Properties (Свойства).
3. Выберите вкладку Digital Signatures (Цифровые подписи).
4. Дважды щелкните подпись SHA256 «Sonova AG».
5. Проверьте правильность элементов подписи, в частности, убедитесь, что в верхней части отображается сообщение «The digital signature is OK» (Цифровая подпись в порядке), а имя и время подписания соответствуют следующему изображению:



1. Закройте всплывающие диалоговые окна и дважды щелкните файл SonovaVerify.exe.
2. Убедитесь, что отображается сообщение «NO ERRORS DETECTED.» (ОШИБОК НЕ ОБНАРУЖЕНО.), как показано на следующем рисунке:

На изображении показано, что программа SonovaVerify проверила и выполнила аутентификацию цифровых подписей всех установленных программных файлов. Это подтверждает, что программное обеспечение для настройки не был подделано, повреждено или иным образом скомпрометировано. SonovaVerify выведет предупреждения или сообщения об ошибках, если файлы или папки отсутствуют или в папку с программными файлами добавлены непредвиденные файлы или папки.

9. ИСПРАВЛЕНИЯ И ОБНОВЛЕНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Автоматические обновления не поддерживаются.

10. УПРАВЛЕНИЕ ДАННЫМИ

10.1 БАЗЫ ДАННЫХ

Программное обеспечение для настройки использует транзакционную базу данных для хранения данных пациентов и набор информационных баз данных, которые предоставляют конфигурации метаданных, необходимые приложению.

Подробный список всех баз данных, развернутых программным обеспечением для настройки, см. в разделе 3. «Сетевые и контекстные схемы — Артефакты развертывания».

Если программное обеспечение для настройки установлено как автономное приложение, база данных пациентов является внутренней по отношению к программному обеспечению для настройки. База данных пациентов, хранящаяся в файле PatientDatabase.sqlite, находится на том же компьютере, что и программное обеспечение для настройки, и обеспечивает хранилище данных пациентов. Для резервного копирования данных приложения при развертывании Target CI в качестве автономного приложения создайте резервную копию всей папки, расположенной по адресу: %ProgramData%\Advanced Bionics\Target CI\Target CI\Data. Защитите резервные копии данных не только от потери данных, но и от кражи. При установке программного обеспечения для настройки в качестве модуля Noah данные пациентов сохраняются в базе данных, предоставляемой системой Noah. База данных Noah может быть настроена для сетевого доступа. Базу данных Noah также можно настроить для несетевого доступа и установить на том же ПК, что и программное обеспечение для настройки. Настройте шифрование базы данных Noah для защиты данных (см. документацию HIMSA).

Для режима распределенного развертывания Noah обратитесь к следующей ссылке для получения инструкций по резервному копированию и восстановлению базы данных пациентов Noah:

https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/backing-up-and-restoring-the-data-in-your-noah-database/

10.2 МИГРАЦИЯ ДАННЫХ

Программное обеспечение для настройки позволяет пользователям переносить записи пациентов из предыдущего программного обеспечения для настройки компании AB — SoundWave 3.2. Для переноса записи пациентов должны быть доступны в установленной программе SoundWave 3.2 на том же компьютере, что и Target CI.

10.3 КОНФИГУРАЦИИ СЛУХОВЫХ УСТРОЙСТВ

Программное обеспечение для настройки позволяет экспортировать и импортировать конфигурацию и настройки устройства.

10.4 УДАЛЕНИЕ ДАННЫХ

С инструкциями по удалению данных можно ознакомиться в Инструкции по применению (IFU) или на следующем сайте по развертыванию Noah: https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/deleting-patient-records/

11. БЕЗОПАСНАЯ СРЕДА – СОВМЕСТНАЯ ОТВЕТСТВЕННОСТЬ

Программное обеспечение для настройки разработано для предполагаемого использования, в рамках которого управление рисками кибербезопасности считается общей ответственностью заинтересованных сторон во всей экосистеме слухопротезирования, включающей, помимо прочего, пользователей слуховых устройств, родителей или законных опекунов детей, являющихся пользователями слуховых устройств, HCP, ИТ-администраторов, учреждения и поставщиков услуг по слухопротезированию, поставщиков слуховых устройств и оборудования для программирования.

Ниже представлен список рекомендаций по передовой практике и методов обеспечения безопасности для среды, в которой будет использоваться программное обеспечение для настройки:

Уровень ОС

- Применяйте контроль доступа на уровне ОС, например:
  - Удаляйте учетные записи гостей.
  - Активируйте вход пользователя Windows.
  - Ведите список уполномоченных операторов для контроля доступа к системе.
  - Настройте индивидуальных пользователей и роли.
  - Применяйте требования к надежным паролям и держите учетные данные в тайне.
- Применяйте элементы аудита на уровне ОС.
- Регулярно обновляйте операционную систему.
- Регулярно обновляйте установленную версию программного обеспечения для настройки.
- Включите современную защиту от вредоносных программ и вирусов.
- Включите белый список приложений.

Защита данных

- Для защиты всех данных зашифруйте данные пациента с помощью сторонних инструментов или элементов управления на уровне ОС, например, с помощью шифрования диска (например, бесплатного приложения Microsoft BitLocker). При развертывании в качестве модуля Noah рассмотрите возможность использования шифрования базы данных Noah.
- Внешние носители, содержащие данные, экспортированные из программного обеспечения для настройки, включая отчеты и журналы, должны быть защищены. Если данные больше не используются, их следует стереть безопасным способом, и (или) следует удалить носитель безопасным способом.
- Используйте USB-носители информации со встроенными функциями безопасности, например зашифрованные USB-накопители со встроенной клавиатурой.
- Обязательно обеспечивайте безопасность данных:
  - При передаче данных по небезопасным каналам отправляйте данные анонимно или шифруйте их.
  - Защитите резервные копии данных не только от потери данных, но и от кражи.
  - Удалите все данные с носителя, который больше не используется или должен быть утилизирован.
- Пользователи должны использовать утвержденные процедуры и инструменты для безопасного удаления данных, хранящихся на съемных носителях, в соответствии с применимыми правилами и рекомендациями по обработке информации пациентов / личной идентификационной информации (PII) / защищенной медицинской информации (PHI).

ИТ-инфраструктура

Используйте программное обеспечение для настройки в безопасной сетевой среде, защищенной от несанкционированного вторжения. Существуют различные эффективные методы изоляции и защиты медицинских информационных систем, включая использование брандмауэров, демилитаризованных зон (DMZ), виртуальных локальных сетей (VLAN) и сетевых анклавов. Поддерживайте активное сетевое подключение для получения обновлений операционной системы.

Физический уровень

- Рабочая станция, на которой установлено программное обеспечение для настройки, должна быть физически защищена способом, исключающим доступ непредусмотренных пользователей.
- Исключите возможность несанкционированного вмешательства в работу системы.
- Доступ к принтерам, подключенным к рабочей станции, должен контролироваться.
- Монитор рабочей станции, на которой установлено программное обеспечение для настройки, должен быть расположен способом, ограничивающим видимость содержимого экрана только пользователю.

Организационный уровень

- Эксплуатировать систему разрешено только профессионально обученному, полностью квалифицированному персоналу. Прежде чем разрешить кому-либо управлять системой, следует убедиться, что данное лицо прочитало и полностью поняло инструкции по эксплуатации, прилагаемые к программному обеспечению для настройки.
- Если вы заметили какую-либо подозрительную активность в учетных записях вашего программного обеспечения для настройки или какую-либо непредвиденную операцию, свяжитесь с Advanced Bionics. Подробности см. в разделе 2.1.

Для получения дополнительной информации о совместной ответственности и более подробного списка рекомендаций по передовой практике и методов обеспечения безопасности для среды на разных уровнях, в которой будет использоваться программное обеспечение для настройки, см.:

- Белая книга EHIMA «Рекомендации по безопасной настройке слуховых устройств», EHIMAWhitePaper

12. ПРОЦЕСС ПРОИЗВОДСТВА И РАЗРАБОТКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Кибербезопасность учитывается на протяжении всего процесса разработки программного обеспечения. Программное обеспечение для настройки разработано в соответствии со стандартами IEC 62304 и IEC 82304.

В ходе производственного процесса программное обеспечение для настройки проверяется на наличие вирусов и вредоносных программ.

Уязвимости в сторонних компонентах, перечисленные в Национальной базе данных уязвимостей (NVD) Национального института стандартов и технологий (NIST), оцениваются и устраняются в процессе разработки, а также отслеживаются после выпуска программного обеспечения для настройки.

13. КОМПОНЕНТЫ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И СПЕЦИФИКАЦИЯ МАТЕРИАЛОВ

В состав программного обеспечения для настройки входят некоторые коммерчески доступные готовые программные компоненты.

В следующей таблице перечислены все SOUP (программное обеспечение неизвестного происхождения), распространяемые вместе с программным обеспечением для настройки.

НАИМЕНОВАНИЕ SOUP	ОПИСАНИЕ ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ	ИЗГОТОВИТЕЛЬ	ВЕРСИЯ
API SharpBITS	SharpBITS.NET — это .NET-оболочка API BITS и небольшое приложение Windows UI для быстрого доступа к отправке и получению данных BITS.	perpetualKid	2.1.0.0
ciAD Hearingloss Simulator	Библиотека симулятора потери слуха для медиаплеера	ciAD (Jurg Haubold)	1.0.0.1
CredentialManagement	Пакет управления учетными данными — это оболочка для Windows Credential Management API	iLya Lozovyy	1.0.2
CSharpAnalytics	Используется для Google Analytics.	Attack Pattern	1.6.1
Dapper	Объектно-реляционное отображение	Sam Saffron,Marc Gravell,Nick Craver	2.0.78
Destructurama.Attributed	Используется библиотеками Nephele.	Участники Serilog	3.0
DirectShow 2005	Обеспечивает доступ к функциям Microsoft DirectShow из приложений .NET.	Microsoft	2.0
DSL4	DSL 4 Fitting formula library	Национальный центр аудиологии, Канада	4.2
DSL5	DSL 5 Fitting formula library	Национальный центр аудиологии, Канада	5.0.34
GNOtometrics.Aurical	GNOtometrics.Aurical переиздан для Sonova	GNOtometrics	2.0.1.9
IceLink	Используется для интеграции аудио- / видеоконференции WebRTC	FM (Frozen Mountain)	3.8.0.22151
IdentityModel	OpenID Connect и клиентская библиотека OAuth 2.0, используемая компонентом Kona.CommonServices.Authentication для аутентификации OAuth 2.	Dominick Baier, Brock Allen	5.0.1
IMCInterfaces	Библиотека интерфейса межмодульной связи Noah	HIMSA II K/S	4.4.0.2266
LibGit2Sharp	Используется библиотеками Sonova для взаимодействия с Git	Участники LibGit2Sharp	0.26.1
Mapster	Используется для объектного отображения в коде.	chaowlert,eric_swann	7.2.0.0
MathNet.Numerics	Используется для алгоритмов настройки (путь сигнала, сопоставление целей и т. д.)	Christoph Ruegg, Marcus Cuda, Jurgen Van Gael и соавторы	4.11.0
Microsoft.Bcl.AsyncInterfaces	Предоставляет IAsyncEnumerable<T> и интерфейсы IAsyncDisposable, а также вспомогательные типы для .NET Standard 2.0.	Microsoft	5.0.0
Microsoft.CodeAnalysis.Common	Используется библиотеками из Sonova.HardwareAbstraction. Palio.Trafo	Microsoft	3.9
Microsoft.CodeAnalysis.CSharp	Используется библиотеками из Sonova.HardwareAbstraction. Palio.Trafo	Microsoft	3.9

НАИМЕНОВАНИЕ SOUP	ОПИСАНИЕ ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ	ИЗГОТОВИТЕЛЬ	ВЕРСИЯ
Microsoft.Identity.Client	Библиотека MSAL для .NET является частью платформы идентификации Microsoft для разработчиков (ранее известной как Azure AD) версии 2.0. Она позволяет получать токены безопасности для вызова защищённых API. Использует отраслевой стандарт OAuth2 и OpenID Connect.	Microsoft	4.38.0.0
Microsoft.Identity.Client.Extensions .Msal	Безопасный кроссплатформенный кэш токенов для клиентских приложений MSAL общего пользования.	Microsoft	2.19.3.0
Microsoft.IdentityModel. JsonWebTokens	Включает типы, обеспечивающие поддержку создания, сериализации и проверки Веб-токены JSON. Используется компонентами, взаимодействующими с внутренними службами, которые используют JSON Web Tokens для аутентификации.	Microsoft	6.8.0
Microsoft.IdentityModel.Logging	Зависимость Microsoft.IdentityModel.Tokens	Microsoft	6.8.0
Microsoft.IdentityModel.Tokens	Зависимость SOUP Microsoft.IdentityModel.JsonWebTokens	Microsoft	6.8.0
Microsoft.Win32.TaskScheduler.dll	Используется для инструмента резервного копирования FSW (автоматизированное резервное копирование).	David Hall	2.5.11.0
Microsoft.Xaml.Behaviors.Wpf	XAML Behaviors — простое в использовании средство добавления общей и повторно используемой интерактивности в ваши приложения WPF с минимальным кодом.	xamlexperiencesteam, Microsoft	1.0.1
NAL-NL1	NAL-NL1 Fitting formula library	Australian Hearing	1.1.0.0
NAL-NL2	NAL-NL2 Fitting formula library	Australian Hearing	2.0.11
NAudio.dll	Используется для регулировки громкости и воспроизведения звуковых файлов.	Открытое программное обеспечение	1.9
.NET Framework	Среда выполнения .NET Framework	Microsoft	4.8.3928.0
Newtonsoft.Json	Используется для сериализации и десериализации JSON.	James Newton-King	12.0.3
Nibelung	Библиотеки настройки NoahLink Wireless	GN ReSound	1.3.16.1
Nlog	Зависимость HIMSA Nibelung.CPD (Noahlink Wireless)	Kim Christensen	4.4.0
NoahLink	Драйвер настраиваемого устройства NoahLink	HIMSA	1.55.6.166

НАИМЕНОВАНИЕ SOUP	ОПИСАНИЕ ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ	ИЗГОТОВИТЕЛЬ	ВЕРСИЯ
NoahLink Wireless	Драйвер настраиваемого устройства Noahlink Wireless	HIMSA	2.0.0.68
Otometrics.HiPro2	Коммуникационные библиотеки HiPro	GNOtometrics	2.0.0.4
Otometrics.REMaccess	Уровень абстракции Otometrics над библиотекой межмодульного интерфейса связи Noah	GN Otometrics	1.0.0.10
PDFium.Net.SDK	Библиотека C# PDF для создания и редактирования PDF-документов в приложениях .Net.	Patagames.com	4.54.2704.0
Polly	Библиотека, позволяющая разработчикам излагать политики отказоустойчивости и обработки нерегулярных отказов, в частности политики в области обработки повторных попыток, автоматического выключения, изоляции от каскадных сбоев и использования резервных ресурсов, свободным потокобезопасным способом.	Приложение vNext	7.2.1
Polly.Contrib.WaitAndRetry	Библиотека для Polly, содержащая вспомогательные методы для различных стратегий ожидания и повторения попыток.	Grant Dickinson, приложение vNext	1.1.1
Polly.Extensions.Http	Библиотека, содержащая продуманные и удобные методы настройки политик Polly для обработки нерегулярных отказов, типичных для вызовов через HttpClient.	Приложение vNext	3.0
Portable.BouncyCastle	Зависимость HIMSA Nibelung.CPD (Noahlink Wirlesss)	BouncyCastle.Crypto	1.8.10.0
protobuf-net.dll	Фреймворк сериализации, используемый для blob-объекта RC.	Открытое программное обеспечение	2.0.0.668
Security.Cryptography	Расширения для API безопасности, поставляемые с .NET Framework	Microsoft	1.7.2
Serilog	Компонент журналов, который используется для всего приложения Chinook.	Участники Serilog	2.10.0
Serilog.Enrichers.Thread	Пополнение событий Serilog информацией о свойствах из текущего потока	Участники Serilog	3.1
Serilog.Expressions	Фильтрация событий на основе выражений для Serilog.	Участники Serilog	2.0
Serilog.Settings.AppSettings	Конфигурация XML (System.Configuration <appSettings>) поддержка Serilog.	Участники Serilog	2.2.2
Serilog.Sinks.Console	Приемник Serilog, который записывает события журнала в консоль / терминал.	Участники Serilog	4.0.0.0
Serilog.Sinks.Debug	Приемник Serilog, который записывает события журнала в окно вывода отладки.	Участники Serilog	2.0

НАИМЕНОВАНИЕ SOUP	ОПИСАНИЕ ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ	ИЗГОТОВИТЕЛЬ	ВЕРСИЯ
Serilog.Sinks.File	Запись событий Serilog в текстовые файлы в обычном формате или формате JSON.	Участники Serilog	4.1
Serilog.Sinks.Trace	Приемник диагностических сообщений системы отслеживания для Serilog.	Участники Serilog	2.1
SharpZipLib	#ziplib (SharpZipLib, ранее NzipLib) — это библиотека Zip, Gzip, Tar и Bzip2, полностью написанная на C# для платформы .NET. Эта библиотека обеспечивает функцию сжатия (zip, unzip, потоковое сжатие и т. д.). Мы используем его в приложении Firmware Update.	Открытое программное обеспечение	1.1.0.145
SQLite.Interop	SQLite — это программная библиотека, предоставляющая систему управления реляционными базами данных. Под «Lite» в SQLite понимается простота настройки, администрирования базы данных и требуемых ресурсов. SQLite обладает следующими примечательными особенностями: автономность, бессерверность, нулевая конфигурация, транзакционность. Это база данных (SQLite 3.32.1) для хранения информации о пациенте (в автономном режиме), ресурсах нашего каталога продукции и метаданных для настройки, аксессуаров и CA.	Команда разработчиков SQLite	1.0.113
Superpower	Библиотека парсер-комбинатора для C#	Datalust, участники Superpower, участники Sprache	2.3
System.Buffers	Обеспечивает объединение ресурсов любого типа для критически важных для производительности приложений, которые часто выделяют и освобождают объекты.	23rogramma,dotnetframework	4.5.1
System.Collections.Immutable	Используется библиотеками из Sonova.HardwareAbstraction. Palio.Trafo	Microsoft	5.0
System.ComponentModel. Annotations	Предоставляет атрибуты, которые используются для определения метаданных объектов, используемых в качестве источников данных.	23rogramma,dotnetframework	4.7
System.Configuration. Configuration Manager	Предоставляет типы, поддерживающие использование файлов конфигурации.	Microsoft	5.0
System.Data.SQLite.Core	Используется библиотеками из Sonova.HardwareAbstraction. Palio.Trafo	Команда разработчиков SQLite	1.0.113.7
System.Drawing.Common	Обеспечивает доступ к графическим функциям GDI+.	Microsoft	5.0.1

НАИМЕНОВАНИЕ SOUP	ОПИСАНИЕ ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ	ИЗГОТОВИТЕЛЬ	ВЕРСИЯ
System.IdentityModel.Tokens.Jwt	Включает типы, обеспечивающие поддержку создания, сериализации и проверки веб-токенов JSON. Используется компонентами, взаимодействующими с внутренними службами, которые используют JSON Web Tokens для аутентификации.	Microsoft	6.8.0
System.IO.Abstractions	Набор абстракций, помогающих тестировать взаимодействие файловых систем.	Tatham Oddie и друзья	12.0.10
System.Memory	Предоставляет типы для эффективного представления и объединения управляемых, стековых и собственных сегментов памяти и последовательностей таких сегментов, а также примитивы для анализа и форматирования текста в кодировке UTF-8, хранящегося в этих сегментах памяти.	24rogramma, dotnetframework	4.5.4
System.Numerics.Vectors	Предоставляет аппаратно ускоренные числовые типы, подходящие для высокопроизводительных вычислительных и графических приложений.	24rogramma, dotnetframework	4.5
System.Reactive. Интерфейсы	Реактивные расширения (Rx) для .NET	.NET Foundation	3.1.1
System.Reactive.Core	Реактивные расширения (Rx) для .NET	.NET Foundation	3.1.1
System.Reactive.Linq	Реактивные расширения (Rx) для .NET	.NET Foundation	3.1.1
System.Reactive.PlatformServices	Реактивные расширения (Rx) для .NET	.NET Foundation	3.1.1
System.Reactive.Windows. Threading	Реактивные расширения (Rx) для .NET	.NET Foundation	3.1.1
System.Reflection.DispatchProxy	Предоставляет класс для динамического создания замещающих типов, которые реализуют указанный интерфейс и являются производными от указанного типа DispatchProxy. Вызовы методов на сгенерированном proxyinstance отправляются в базовый тип DispatchProxy.	Microsoft	4.7.1
System.Reflection.Metadata	Этот пакет предоставляет низкоуровневые средства чтения и записи метаданных .NET (ECMA-335). Он ориентирован на улучшение производительности и идеально подходит для создания библиотек более высокого уровня, которые предназначены для предоставления собственной объектной модели, например, компиляторов.	Microsoft	5.0

НАИМЕНОВАНИЕ SOUP	ОПИСАНИЕ ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ	ИЗГОТОВИТЕЛЬ	ВЕРСИЯ
System.Runtime.CompilerServices.Unsafe	Предоставляет System.Runtime. Класс CompilerServices.Unsafe, который предоставляет универсальную низкоуровневую функциональность для манипулирования указателями.	24rogramma,dotn etfra me work	5.0
System.Security.AccessControl	Предоставляет базовые классы, позволяющие управлять списками контроля доступа и аудита для защищаемых объектов.	Microsoft	5.0
System.Security.Permissions	Предоставляет типы, поддерживающие управление доступом для кода (CAS).	Microsoft	5.0
System.Security.Principal.Windows	Предоставляет классы для получения текущего пользователя Windows и взаимодействия с пользователями и группами Windows.	Microsoft	5.0
System.Text.Encoding.CodePages	Обеспечивает поддержку кодировок на основе кодовых страниц, включая Windows-1252, Shift-JIS и GB2312.	Microsoft	5.0
System.Text.Encodings.Web	Предоставляет типы для кодирования и изолирования строк для использования в JavaScript, языке разметки гипертекста (HTML) и унифицированных адресов ресурсов (URL). Является зависимостью SOUP IdentityModel	24rogramma, dotnetframework	5.0
System.Text.Json	Предоставляет высокопроизводительные и требующие малого выделения памяти типы данных, которые сериализуют объекты в текст JavaScript Object Notation (JSON) и десериализуют текст JSON в объекты со встроенной поддержкой UTF-8. Также предоставляет типы для чтения и записи текста JSON в кодировке UTF-8 и для создания объектной модели документа (DOM) в памяти, доступной только для чтения, для произвольного доступа к элементам JSON в структурированном представлении данных.	Microsoft	5.0.1
System.Threading.Tasks.Extensions	Предоставляет дополнительные типы, упрощающие написание многопоточного и асинхронного кода.	25rogramma,dotnetfra mework	4.5.4
System.ValueTuple	Предоставляет структуры System.ValueTuple, которые реализуют базовые типы для кортежей в C# и Visual Basic. Добавляет поддержку кортежей значений, поскольку они включены только в более поздние версии .NET Framework.	25rogramma,dotnetfra mework	4.5.0
Thrift	Используется для определения протокола удаленной связи	Apache	0.13.0.0

НАИМЕНОВАНИЕ SOUP	ОПИСАНИЕ ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ	ИЗГОТОВИТЕЛЬ	ВЕРСИЯ
Unity	Unity Container (Unity) — это полнофункциональный, расширяемый контейнер внедрения зависимостей.	Unity Container Project	5.8.13
WebSync	Используется для интеграции канала данных настройки	FM (Frozen Mountain)	4.9.32.0
Библиотеки времени выполнения MS-VisualC++ 7.1	Библиотеки времени выполнения Microsoft Visual C++	Microsoft	7.10.6030.0
Драйвер электронного защитного ключа WAP BT	Драйвер электронного защитного ключа WAP BT (электронный защитный ключ настройки)	iAnywhere Solutions	3.0.0.6095
Распространяемый компонент PC VC++ 2008	Распространяемый компонент Microsoft Visual C++ 2008	Microsoft	9.0.30729.6161
Распространяемый компонент Microsoft Visual C++ 2010 x86	Распространяемый компонент Microsoft Visual C++ 2010	Microsoft	10.0.40219.325
Распространяемый компонент Microsoft Visual C++ 2012	Распространяемый компонент Microsoft Visual C++ 2012	Microsoft	11.0.61030.0
Распространяемый компонент Microsoft Visual C++ 2017 (x86)	Распространяемый компонент Microsoft Visual C++ 2017	Microsoft	14.16.27024.1
Рендеринг Xps в PDF (NiXPS)	Конвертирует файлы 25rogrammatically xps в pdf; используется в отчетах приложений настройки.	NiXPS	2.6.7.0

14. ЛИТЕРАТУРА

Заголовок	Веб-сайт
Инструкция по применению (электронная)	https://ifu.advancedbionics.com/
Глобальная политика конфиденциальности Advanced Bionics	https://advancedbionics.com/privacy
HIMSA	https://www.himsa.com/
Noah System 4	https://www.himsa.com/products/all-about-noah-system-4/
Резервное копирование и восстановление данных в базе данных Noah	https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/backing-up-and-restoring-the-data-in-your-noah-database/
Достигнута максимальная емкость базы данных системы Noah.	https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/noah-system-database-capacity-has-been-reached/
TeamViewer — список используемых портов	https://community.teamviewer.com/English/kb/articles/4139-ports-used-by-teamviewer
BCP 195	https://www.rfc-editor.org/info/bcp195
Документация по безопасности сервера LiveSwitch	https://developer.liveswitch.io/liveswitch-server/server/security.html
Белая книга EHIMA «Рекомендации по безопасной настройке слуховых устройств»	https://www.ehima.com/wp-content/uploads/2021/09/EHIMA Cybersecurity-FSW-Security-Whitepaper v1-Sep2021 .pdf

CE 0123

Advanced Bionics LLC
28515 Westinghouse Place
Valencia, CA 91355, United States
T: +1.661.362.1400

info.us@advancedbionics.com

EU REP Advanced Bionics GmbH
Feodor-Lynen-Strasse 35
D-30625 Hannover

info.switzerland@advancedbionics.com

Для получения информации о других представительствах компании AB посетите веб-сайт *advancedbionics.com/contact*

AB – A Sonova brand

Для получения разрешения контролирующего органа и информации о доступности в вашем регионе свяжитесь с местным представителем компании AB.

ADVANCED BIONICS
POWERFUL CONNECTIONS

029-S396-26 Rev A 2025-09-15