Рекомендации по обеспечению информационной безопасности при работе с системой DIRECTUM

В документе описаны механизмы защиты информации, используемые в системе DIRECTUM, а также даны рекомендации к ИТ-инфраструктуре организации. Выполнение этих рекомендаций позволит защитить автоматизированную систему (АС), частью которой является DIRECTUM, до класса защищенности 1Г включительно.

Обеспечение информационной безопасности автоматизированной системы требует комплексного подхода и защиты информации на законодательном, административном, процедурном и программно-техническом уровне. Законодательный уровень защиты информации регламентируется государственными органами.

Чтобы обеспечить защиту информации **на административном и процедурном уровне**, разработайте комплект организационно-распорядительной документации. Он должен регламентировать права, обязанности и полномочия администратора безопасности, регламент антивирусного контроля, регламент установки в систему нового программного обеспечения, в том числе порядок действий при изменении версии системы, регламент тестирования работоспособности системы защиты информации. Кроме того, он должен определять ответственных за обеспечение информационной безопасности и регламентировать физическую защиту устройств и носителей информации, чтобы не допустить несанкционированного проникновения.

Чтобы обеспечить защиту информации **на программно-техническом уровне**:

- применяйте сертифицированные средства защиты информации для АС класса защищенности 1Г включительно. Они должны обеспечивать контроль целостности программных средств системы DIRECTUM и обрабатываемой информации, а также неизменность программной среды;
- используйте сертифицированные средства антивирусной защиты и средства обнаружения вторжений нужного типа и класса защиты;
- используйте сертифицированные межсетевые экраны требуемого класса защищенности при подключении АС к информационно-телекоммуникационным сетям международного информационного обмена.

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

- управление доступом: идентификация пользователей в системе и контроль прав доступа;
- регистрация и учет данных: логирование и ведение истории работы с объектами;
- криптография: шифрование текстов и подписание ЭП;
- обеспечение целостности и доступности информации: резервное копирование базы данных и использование кластеров.

Обеспечение безопасной работы отдельных компонент системы DIRECTUM имеет свои особенности. Подробнее см. в разделах:

- «Сервер СУБД и сервисные службы системы DIRECTUM»
- «Файловые хранилища»
- «Механизмы межсистемного взаимодействия (DCI)»
- «Службы взаимодействия систем (DICS)»
- «Веб-доступ»
- «Федеративный поиск»
- «Мобильные приложения»

Содержание

Сертификация системы DIRECTUM

Система DIRECTUM сертифицирована Федеральной службой по техническому и экспортному контролю (ФСТЭК).

Сертификат удостоверяет, что система электронного документооборота DIRECTUM 5, разработанная и производимая в соответствии с техническими условиями RU.14739140.50618-02 98 01, является программным средством защиты от несанкционированного доступа к информации, не содержащей сведений, составляющих государственную тайну, реализующим функции идентификации и аутентификации, управления доступом и регистрации событий безопасности, соответствует требованиям руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) – по 4 уровню контроля и технических условий. Система DIRECTUM может использоваться для защиты информации в информационных системах персональных данных до 1 уровня защищенности включительно, а также автоматизированных системах обработки конфиденциальной информации до класса защищенности 1Г включительно.

Сертифицированы все компоненты системы DIRECTUM, кроме сервера NOMAD и клиентских приложений DIRECTUM Jazz и DIRECTUM Solo для Android.

Общие механизмы защиты информации в DIRECTUM

Управление доступом

Аутентификация

Для входа в систему DIRECTUM необходима аутентификация пользователей. Способ аутентификации для пользователя задается администратором системы в компоненте **Пользователи** в поле ***Аутентификация**. В соответствии с указанными настройками пользователи заполняют параметры аутентификации при первом входе в систему.

Тип аутентификации, указанный в компоненте, действует как на десктоп-клиент, так и на веб-клиент и мобильные приложения. Однако в веб-клиенте и мобильных приложениях можно настроить дополнительные параметры аутентификации. Например, при условии выполнения дополнительных настроек пользователь с Windows-аутентификацией сможет аутентифицироваться в веб-клиенте с помощью сквозной Windows-аутентификации.

Десктоп-клиент

В десктоп-клиенте предусмотрены следующие способы аутентификации:

- Windows-аутентификация – рекомендуется для пользователей при наличии домена в локальной сети предприятия. Пользователи входят в систему под именами соответствующих пользователей операционной системы, без повторного ввода имени и пароля, и получают доступ к данным БД через роль приложения «IS-Builder Application Role2». Активация роли происходит при загрузке проводника системы;
- аутентификация по перекодированному паролю – рекомендуется для пользователей при отсутствии домена в локальной сети предприятия. При входе в систему запрашиваются регистрационное имя и пароль. Пользователи не имеют доступа к данным из других приложений. Их пароль на SQL-сервере отличается от пароля в системе DIRECTUM;

- Novell-аутентификация – рекомендуется для пользователей при наличии Novell eDirectory в локальной сети предприятия. Пользователи входят в систему под именами соответствующих пользователей Novell eDirectory, без повторного ввода имени и пароля;
- аутентификация по паролю – рекомендуется для администраторов в случае невозможности использования Windows-аутентификации. При входе в систему запрашиваются регистрационное имя и пароль. Пользователи могут работать с базой данных системы, минуя компоненты IS-Builder, например, через утилиту Microsoft SQL Server Management Studio. Их пароль входа на SQL-сервер совпадает с паролем входа в систему.

Наиболее безопасным способом аутентификации является Windows-аутентификация.

Для пользователей с аутентификацией по паролю и перекодированному паролю доступно включение политик паролей Windows: политики сложности и истечения срока действия пароля. Настроенная политика паролей обеспечивает дополнительную защиту учетных записей пользователей от несанкционированного доступа.

Политики паролей также включаются в компоненте **Пользователи** при установке флажка **Применять политику паролей**. Если флажок установлен, пароль пользователя проверяется на соответствие политикам паролей Windows компьютера, на котором установлен SQL-сервер системы.

Веб-доступ

В веб-клиенте предусмотрены следующие способы аутентификации:

- аутентификация путем ввода реквизитов и их последующей передачи по каналам связи (Windows-аутентификация, аутентификация по паролю). Для использования этих типов аутентификации рекомендуется обеспечить безопасность каналов связи;
- сквозная Windows-аутентификация. Для работы сквозной Windows-аутентификации необходимо настроить доверие делегирования служб Kerberos. Используйте данный тип аутентификации, если это не противоречит политикам безопасности организации;
- аутентификация с помощью сторонних провайдеров. Например, Active Directory Federation Services (AD FS), PingFederate, провайдер собственной реализации.

  Такой способ аутентификации реализует принцип единого входа (Single-Sign-On). Когда пользователь проходит аутентификацию на одном сервисе, он автоматически получает доступ ко всем остальным зарегистрированным веб-ресурсам организации.

  Для работы с внешними провайдерами аутентификации веб-доступ использует службу C2WTS, для которой необходимо настроить ограниченное делегирование. Подробнее см. в руководстве администратора веб-доступа, раздел «Настройка внешних провайдеров аутентификации»;
- аутентификация с помощью клиентского сертификата. Можно использовать только для входа пользователей, которые авторизуются в системе DIRECTUM с помощью Windows-аутентификации. Безопасность данного типа аутентификации обеспечивается тем, что:
  - реквизиты пользователя не передаются по сети;
  - для работы требуется настройка HTTPS-соединения.

Наиболее безопасным способом аутентификации в веб-клиенте является сквозная Windows-аутентификация.

Мобильные приложения

В мобильных решениях DIRECTUM Jazz и DIRECTUM Solo предусмотрено два способа аутентификации:

- аутентификация путем ввода реквизитов и их последующей передачи по каналам связи (Windows-аутентификация, аутентификация по паролю). Для использования этих типов аутентификации рекомендуется обеспечить безопасность каналов связи и устройства пользователя;
- аутентификация с помощью клиентского сертификата – можно использовать только для входа пользователей, которые авторизуются в системе DIRECTUM с помощью Windows-аутентификации. Данный тип аутентификации является наиболее безопасным, поскольку:
    - реквизиты пользователя не хранятся на устройстве и не передаются по сети;
    - для его работы требуется настройка HTTPS-соединения и блокировка устройства с помощью пароля или PIN-кода.

> Примечание
> Аутентификация с помощью сертификата поддерживается только в мобильных приложениях на базе Android.

Права доступа

Доступ к системе DIRECTUM имеют только зарегистрированные пользователи в пределах назначенных им прав.

Создавать и удалять, включать и отключать пользователей может только администратор системы DIRECTUM, обладающий необходимыми правами для установки и настройки системы.

> Примечание
> Чтобы генерировать пользователей на SQL-сервере, нужно входить в предопределенную роль SQL-сервера **securityadmin**.

Администратор также может настраивать права доступа к объектам, например задать начальные права на этапе настройки системы. В дальнейшем права к объектам системы могут настраивать пользователи.

В некоторых организациях разделяются роли администратора автоматизированной системы и администратора безопасности информации. В этом случае администратор автоматизированной системы несет ответственность за функционирование автоматизированной системы в установленном штатном режиме работы, может заниматься настройкой модулей системы, поддержкой функциональности, обновлением системы. Администратор безопасности информации несет ответственность за защиту автоматизированной системы от несанкционированного доступа, может управлять учетными записями, следить за соблюдением внутренних регламентов и политик конфиденциальности. Если описанные функции разделяются между двумя сотрудниками, права и привилегии администратора системы DIRECTUM могут делиться между ними.

Пользователям доступны только те объекты, к которым у них есть права доступа.

В процессе работы в системе пользователям могут быть настроены разные виды прав. Подробнее см. раздел «Виды прав доступа пользователей».

Для разных объектов системы выделяют различные уровни прав доступа. Подробнее об объектах и возможных к ним прав доступа см. в разделе «Уровни прав доступа к объектам системы».

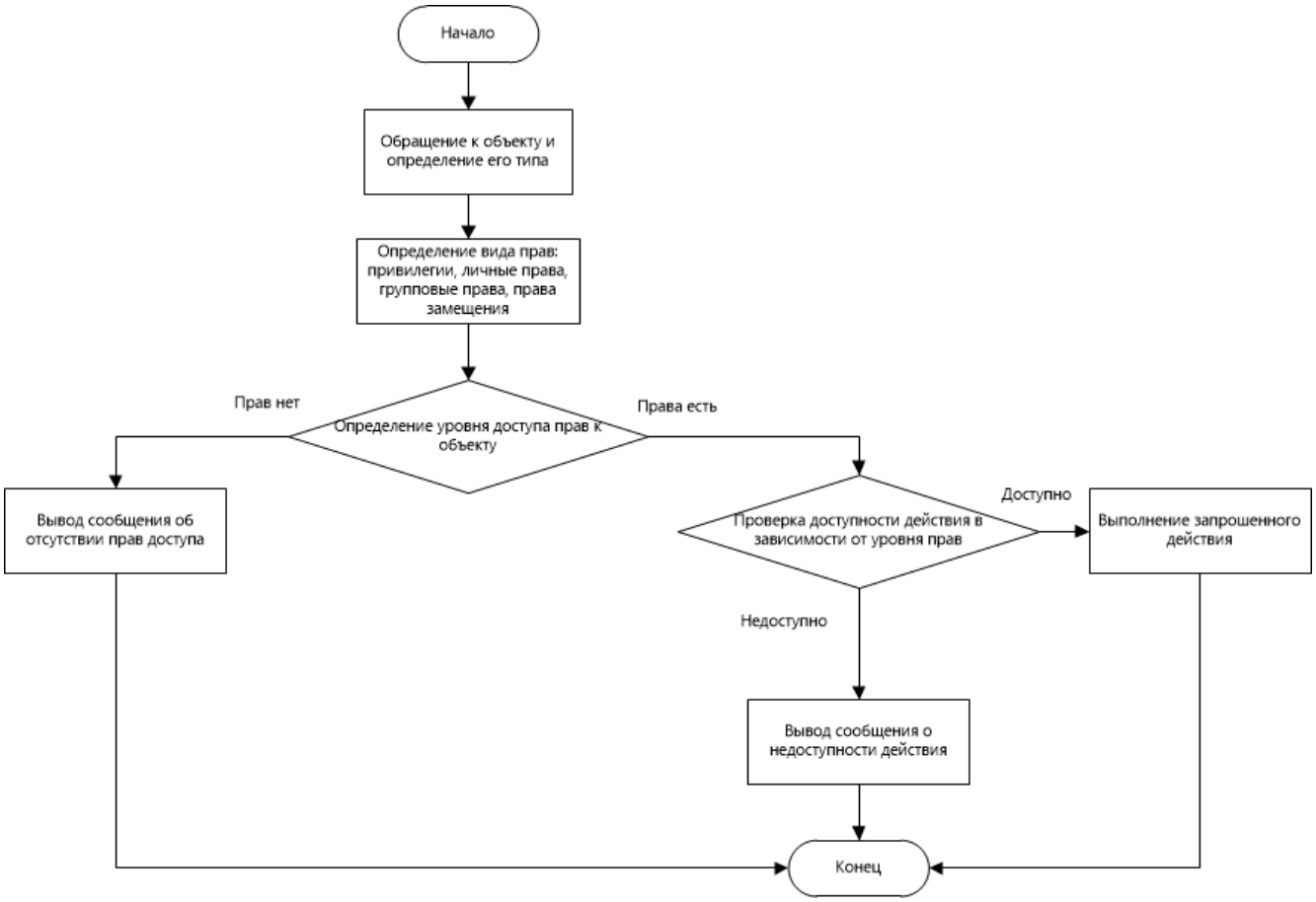
В системе DIRECTUM существует возможность ограничить права на записи компонент типа «Отчеты» или «Справочники». Например, когда пользователям системы должны быть доступны не все записи данных компонент. Это реализовывается с помощью механизма фильтраторов.

Также в системе можно скрывать отображение оргструктуры предприятия в некоторых окнах, например в окне настройки прав доступа на объекты. В этом случае в дереве «Пользователи» в окне настройки прав доступа будут скрыты пользователи и группы пользователей.

Подробнее об этих механизмах см. в документации DIRECTUM, в руководстве администратора, разделы «Ограничение прав по записям на компоненты типа «Отчеты», «Ограничение прав по записям на компоненты типа «Справочник» и «Скрытие оргструктуры предприятия».

Схема работы механизма прав доступа

Общая схема механизма прав доступа в системе DIRECTUM имеет вид:



Виды прав доступа пользователей

Права пользователей системы DIRECTUM складываются из:

- привилегий – права пользователей или групп пользователей на выполнение действий и работу с объектами системы. Например, привилегии «Полный доступ к объектам», «Управление репликацией» и т.д. Привилегии назначаются в компонентах системы **Пользователи**, **Группы пользователей** и **Привилегии**;
- прав пользователя – права, назначенные лично пользователю. Права доступа пользователя к документам, папкам и задачам, заданиям, уведомлениям назначаются в карточках объектов. Права доступа к компонентам системы DIRECTUM назначаются в компонентах системы **Пользователи** или **Компоненты**;

- прав групп пользователей – права, назначенные группам пользователей, в которые входит пользователь. Группы задаются в компоненте **Пользователи** или **Группы пользователей**. Права групп к документам, папкам и задачам, заданиям, уведомлениям назначаются в карточках объектов. Права групп к компонентам системы DIRECTUM назначаются в компоненте **Группы пользователей** или **Компоненты**;
- прав замещения – права, которые получает пользователь в результате замещения какого-либо пользователя системы. Замещение настраивается в справочнике **Замещение пользователей**. Права замещения распространяются только на папки, документы и задачи, задания, уведомления. На компоненты системы DIRECTUM права замещения не распространяются.

  Замещающим пользователям не передаются привилегии замещаемых.

Пользователь и группа, в которую он входит, могут иметь разные права на один и тот же объект системы и/или обладать разными привилегиями. Также пользователь может получить права по замещению. В результате пользователь получает максимальные из назначенных прав и привилегий, с учетом замещения, вне зависимости от того, какие права назначены лично пользователю, а какие группе.

Уровни прав доступа к объектам системы

Для разных объектов системы DIRECTUM выделяются различные уровни прав доступа, и отличается порядок назначения прав к ним:

Тип объекта	Уровень прав доступа	Пример доступных действий	Способ назначения прав
Документы	Просмотр	Просмотр документа	Назначаются пользователями в карточках документов или определяются привилегией «Просмотр объектов»
		Передача прав с уровнем «Просмотр» на документ	Устанавливается флажок **Разрешить передавать права** в окне «Настройка прав доступа к электронному документу» пользователем, обладающим полным типом прав на данный документ
	Изменение	Просмотр и изменение документа	Назначаются пользователями в карточках документов или определяются привилегией «Полный доступ к объектам»
		Передача прав с уровнем «Просмотр» или «Изменение» на документ	Устанавливается флажок **Разрешить передавать права** в окне «Настройка прав доступа к электронному документу» пользователем, обладающим полным типом прав на данный документ
	Полный	Просмотр, изменение, удаление и управление доступом к документу	Назначаются пользователями в карточках документов или определяются привилегией «Полный доступ к объектам»
Папки	Просмотр	Просмотр папки	Назначаются пользователями в карточках папок или определяются привилегией «Просмотр объектов»

Тип объекта	Уровень прав доступа	Пример доступных действий	Способ назначения прав
	Изменение	Просмотр и изменение папки	Назначаются пользователями в карточках документов и папок или определяются привилегией «Полный доступ к объектам»
	Полный	Просмотр, изменение, удаление и управление доступом к папке	
Задачи, задания, уведомления	Просмотр	Просмотр задач и заданий семейства	Назначаются пользователями в карточке главной задачи семейства или определяются привилегией «Просмотр объектов»
	Доступ инициатора задачи	Просмотр задач и заданий семейства, изменение задачи и соответствующих ей заданий (отключаемо с помощью флажка **Запретить инициаторам выполнять задания** в настройках системы). Для главных задач дополнительно управление доступом к семейству задач	Определяются автоматически по тому, кем является пользователь по отношению к задаче, или по наличию привилегии «Полный доступ к объектам»
	Доступ исполнителя задания	Просмотр задач и заданий семейства, изменение задания	
Компоненты	Без ограничений	Все действия в компоненте	Назначаются администратором в компонентах **Пользователи**, **Группы пользователей**, **Компоненты** или определяются по наличию привилегии «Полный доступ к компонентам»
	Просмотр	Просмотр записей компоненты	Назначаются администратором в компонентах **Пользователи**, **Группы пользователей**, **Компоненты**
	Выполнение	Выполнение отчета	
	Добавление	Добавление новой записи	
	Изменение	Изменение существующей записи	
	Утверждение	Утверждение существующей записи	
	Удаление	Удаление записи компоненты	

При изменении прав доступа к папкам, документам, задачам, заданиям, новые права вступают в силу при обращении к объекту, выполнении поиска или обновлении содержимого папки в проводнике системы.

При изменении прав доступа к компоненте, новые права вступают в силу при следующем обращении к ней, например при запуске.

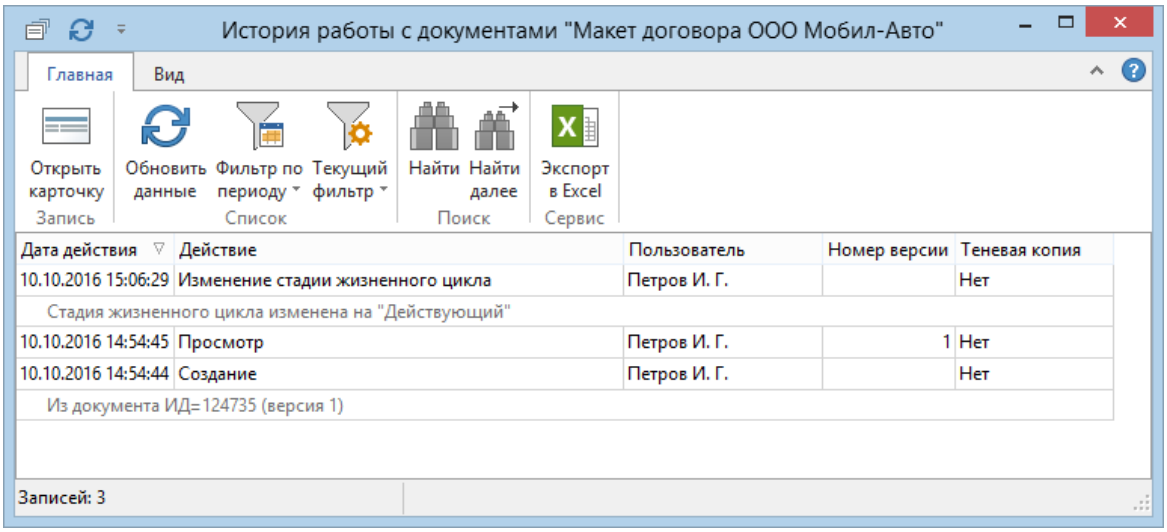
Регистрация и учет данных

История работы с объектами

Запись истории работы с объектами – один из важных аспектов безопасности системы. Например, если пользователь неправильно выдал права на документ, то возникает потребность понять, кто и когда выполнил это действие.

В системе DIRECTUM для всех объектов ведется история работы, в которой фиксируются основные действия с объектом.

Список действий и данных о них отображаются в окне истории. Например, для документов окно имеет вид:



В окне истории работы для каждого действия могут указываться, например, дата и время действия, тип действия, сетевое имя пользователя, код рабочей станции, имя приложения, сервер и т.д.

Основные действия фиксируются в истории объектов по умолчанию.

Документы

Действие	Детальное описание
Создание документа	Имя документа-источника, если документ создан копированием
Изменение прав доступа	
Просмотр текста документа	
Изменение текста документа	
Изменение карточки	
Изменение типа карточки	
Подписание документа	
Изменение жизненного цикла документа	Новый жизненный цикл документа
Изменение вида документа	
Копирование документа	

Действие	Детальное описание
Удаление документа	
Создание версии документа	
Изменение состояния версии	Новое состояние версии
Изменение видимости версии	
Удаление версии документа	
Просмотр теневой копии	
Изменение хранилища документа	
Шифрование документа сертификатом	
Шифрование паролем и сертификатом	
Шифрование документа паролем	
Перешифрование документа	
Отключение шифрования	
Изменения пароля шифрования	
Экспорт документа с блокировкой	Имя файла, в который экспортируется документ
Экспорт документа без блокировки	Имя файла, в который экспортируется документ
Блокировка документа	
Разблокировка документа	
Импорт документа с разблокировкой	Имя файла, из которого импортируется документ
Импорт документа без разблокировки	Имя файла, из которого импортируется документ
Восстановление документа из локальной копии	
Отправка документа по почте	
Закрепление документа для сервера	
Снятие закрепления документа для сервера	
Перемещение в архив системы	
Извлечение из архива системы	

Задачи и задания

Задачи	Задания по задаче	Задания
Создание	Создание	Создание
Старт	Прекращение	Прекращение
Рестарт	Возобновление	Возобновление
Подписание	Пометка как прочитанного	Пометка как прочитанного
Изменение карточки задачи	Пометка как непрочитанного	Пометка как непрочитанного
На доработку	Изменение карточки задачи	Изменение карточки задания

Задачи	Задания по задаче	Задания
Прекращение	Выполнение	Выполнение
Возобновление	Подписание	Подписание
Изменение схемы маршрута	Принятие задания-контроль	–
Перешифрование	–	–
Перемещение в архив системы	Перемещение в архив системы	Перемещение в архив системы
Извлечение из архива системы	Извлечение из архива системы	Извлечение из архива системы
Добавление вложения	Добавление вложения	Добавление вложения
Удаление вложения	Удаление вложения	Удаление вложения

Папки

В истории работы с папками фиксируются следующие действия:

- создание папки;
- изменение карточки папки.

Записи справочника

В истории работы с записями справочника фиксируются следующие действия:

- создание;
- изменение;
- перемещение в архив системы;
- извлечение из архива системы.

Администратор может дополнить список фиксируемых действий и добавить к ним детальную информацию. Настроить можно следующие действия:

Справочники	Документы	Папки	Задачи и задания
Создание записи справочника		Создание папки	Создание задачи или задания
Просмотр карточки	Просмотр карточки		
	Изменение карточки	Изменение карточки	Изменение задачи или задания
Изменение записи справочника			
	Изменение прав доступа	Изменение прав доступа	
Удаление записи справочника	Удаление документа	Удаление папки	Удаление задачи или задания

Примечание
Просмотр карточки фиксируется только при работе пользователя в десктоп-клиенте.

Например, благодаря настройке истории администратор может определить, кто выдал права на документ пользователю.

Действия фиксируются в базе данных. Информацию об удаленных объектах можно получить с помощью SQL-запроса.

> Примечание
> В истории объектов не отражается факт просмотра или изменения документа с помощью мобильного приложения. Вместо этого в истории фиксируется действие «Экспорт без блокировки».

Логирование

В системе DIRECTUM ведется логирование различных событий – исключений и другой служебной информации, в том числе событий безопасности.

Клиентская часть системы DIRECTUM

В случае возникновения ошибок в ходе работы клиентской части DIRECTUM информация записывается в следующие лог-файлы:

- <имя компьютера>.is-builder.sbrte.log – документы, задачи, задания, уведомления
- <имя компьютера>.is-builder.sbdte.log – утилиты экспорта и импорта разработки
- <имя компьютера>.is-builder.sblogon.log – служба паролей
- <имя компьютера>.is-builder.sbsce.log – сценарии, запускаемые SAJobRunner
- <имя компьютера>.is-builder.sblauncher.log – загрузка пользовательских компонент
- <имя компьютера>.is-builder.isbexec.log – обработчик ISB-файлов
- <имя компьютера>.is-builder.sajobrunner.log – утилита запуска агентов (SAJobRunner)
- <имя компьютера>.is-builder.sblanguagesetup.log – утилита установки текущего языка системы
- <имя компьютера>.is-builder.sasystemactivator.log – утилита SASystemActivator
- <имя компьютера>.is-builder.sakeyregistration.log – Утилита SAKeyRegistration

Клиентская часть системы DIRECTUM также ведет лог-файл профайлинга.

В лог-файлах фиксируется следующая информация: дата и время ошибки, ИД процесса, сервер и имя базы данных, логин пользователя, тип исключения, текст сообщения об ошибке, стек вызова метода, который повлек ошибку, процесс или приложение, которое вызвало ошибку, версия системы, в которой вызвана ошибка, тип компоненты, при работе с которой вызвана ошибка.

С точки зрения безопасности в лог-файлах клиентской части фиксируются ошибки о неправильном имени или пароле при входе пользователя в систему, ошибки о недостоверности подписи, ошибки об отсутствии прав доступа к объектам.

В лог-файле профайлинга фиксируется информация об открытии проводника, выполнении поисков, запуске сценариев и отчетов, работе со справочниками, документами, папками, задачами, заданиями и уведомлениями.

Лог-файлы могут храниться централизованно для всех пользователей на одном компьютере, в одной папке и в своем каталоге для каждого пользователя. Для удобства доступа к лог-файлам рекомендуется хранить их централизованно.

Для записи информации в лог-файл пользователям необходимы минимальные права доступа на папку с лог-файлами клиентской части: «Список содержимого папки», «Чтение» и «Запись».

Путь до хранения лог-файлов указывается в файле LogSettings.xml. Если для пользователя в файле LogSettings.xml не указана папка для ведения логов или не удается записать лог-файл в заданную папку, то лог-файл записывается в папку профиля пользователя %APPDATA%\NPO Computer\IS-Builder. Если папка профиля пользователя недоступна или не существует, то лог-файл записывается в папку %SYSTEMDRIVE%\Users\Default\AppData\Roaming\NPO Computer\IS-Builder учетной записи по умолчанию.

Служба Workflow

Информация о работе службы Workflow записывается в лог-файлы:

- <имя компьютера>.is-builder.sbworkflowproc.log – ошибки в ходе обработки задач
- <имя компьютера>.is-builder.sbworkflowsrv.log – ошибки в работе службы WorkFlow

Путь до хранения лог-файлов указывается в файле LogSettings.xml.

В лог-файлы фиксируется информация, аналогичная той, что фиксируется в лог-файлы клиентской части системы.

> Примечание
> Исключения и события службы Workflow также регистрируются в журнале событий Windows (источник – SBWorkflowProcessingServer).

Сервер сеансов

Информация о работе сервера сеансов записывается в лог-файлы:

- <имя компьютера>.is-builder.sbsessionsrv.log – ошибки в работе сервера сеансов
- Протокол обращений к серверу сеансов – количество обращений к серверу сеансов по протоколу TCP/IP
- Протокол подключения пользователей – когда и какие пользователи входили в систему, и когда выходили из нее, а также указывается количество свободных лицензий в каждый момент времени

Путь до хранения лог-файла указывается в файле LogSettings.xml.

В лог-файл фиксируется информация, аналогичная той, что фиксируется в лог-файлы клиентской части системы.

С точки зрения безопасности в лог-файлы и протоколы сервера сеансов фиксируется информация о сессиях пользователей, отключении клиентов при долгом отсутствии ответа, например, из-за проблем с сетью, сообщения о неверном ключе системы и завершении срока действия ключа.

Путь и имена файлов протоколов задаются в параметрах файла SBSessionSrvSettings.xml, который находится на компьютере, на котором установлен сервер сеансов, в папке, указанной при установке. Если в файле не указан путь до файлов протоколов, протоколы вестись не будут. При этом в лог-файле сервера сеансов появится соответствующее предупреждение.

> Примечание
> Исключения и события сервера сеансов также регистрируются в журнале событий Windows (источник – SBSessionServer).

Служба обработки событий

Информация о работе службы обработки событий записывается в лог-файлы:

- <имя компьютера>.sbeventprocessingproc.log – ошибки в ходе обработки серверных событий;
- <имя компьютера>.sbeventprocessingsrv.log – ошибки в работе службы.

Путь до хранения лог-файлов указывается в файле LogSettings.xml.

В лог-файлы фиксируется информация, аналогичная той, что фиксируется в лог-файлы клиентской части системы.

> Примечание
> Исключения и события службы обработки событий также регистрируются в журнале событий Windows (источник – SBEventProcessingServer).

Служба файловых хранилищ

Информация о работе службы файловых хранилищ записывается в лог-файл <имя компьютера>.is-builder.sbfilestorageserver.log.

Путь до хранения лог-файла указывается в файле LogSettings.xml.

В лог-файл фиксируется информация, аналогичная той, что фиксируется в лог-файлы клиентской части системы.

С точки зрения безопасности в лог-файл службы файловых хранилищ фиксируется информация о неверном коде авторизации, а также ошибки выдачи прав на папку с версией документа.

> Примечание
> Исключения и события службы файловых хранилищ также регистрируются в журнале событий Windows (источник – SBFileStorageService).

Служба поиска

Служба поиска выполняет полнотекстовые поисковые запросы. Механизм основан на поисковой системе Elasticsearch

Информация о работе службы поиска записывается в лог-файл <имя компьютера со службой>.is-builder.sbsearchservice.log. Путь до хранения лог-файла указывается в файле LogSettings.xml.

Информация о работе Elasticsearch записывается в лог-файл <имя компьютера со службой>.is-builder.sbelasticsearchservice. Путь к папке с лог-файлами задается во время установки компонентов Elasticsearch, по умолчанию %PROGRAMFILES(x86)%\DIRECTUM Company\Elasticsearch\logs.

В лог-файлы фиксируется информация, аналогичная той, что фиксируется в лог-файлы клиентской части системы.

Служба проверки подписей

Информация о работе службы проверки подписей фиксируются в лог-файле <имя компьютера>.is-builder.w3wp_cms_encryption.log. Путь до хранения лог-файла указывается в файле LogSettings.xml.

В лог-файле фиксируется информация, аналогичная той, что фиксируется в лог-файлы клиентской части системы.

Службы ввода и преобразования

Лог файл служб ввода и преобразования ведется в журнале событий Windows, имя журнала – DCTS EventLog.

В зависимости от настроек, указанных в файле LogSettings.config, который находится в папке со службами, можно фиксировать информацию разного типа. Например, включать и выключать запись ошибок, предупреждений и информационных сообщений.

Журнал событий фиксирует полный стек для ошибок, в остальных случаях – только сообщение.

Службы взаимодействия систем

Лог-файл служб взаимодействия систем ведется в журнале событий Windows, имя журнала – DICS EventLog.

Журнал событий создается с помощью утилиты DicsPreInstaller.exe. Утилита получает на вход один параметр – имя конфигурационного файла.

Создание журнала выполняется от лица учетной записи, от которой работает утилита DicsPreInstaller.exe. Для корректного создания у учетной записи должны быть права на выполнение операции создания журнала.

Журнал событий настраивается с помощью утилиты DicsPreInstaller.exe или в конфигурационном файле LogSettings.config.

Серверная часть веб-доступа

- <Имя сервера>WebAccess.log – ошибки и предупреждения, возникающие в ходе работы серверной части веб-доступа
- Клиентская статистика – информация о взаимодействии пользователя со страницей
- Счетчики – диагностическая информация, например, количество пользователей, счетчики эффективности
- Профайлинг операций – время выполнения операций, например, открытие карточек, выполнение заданий

Путь до хранения лог-файла указывается в параметре **LogFileName** файла Web.config. Как правило, лог-файл располагается в папке C:\Inetpub\wwwroot\Directum\directumWebAccess\logs. Каждый день создается новый файл, а файл за предыдущий день переименовывается по формату <имя сервера>.WebAccess.<дата>.log.

Фиксируется следующая информация: дата и время, источник, тип ошибки, текст ошибки, стек вызова, имя и версия сборки, [адрес страницы, тип браузера, IP].

С точки зрения безопасности в лог-файлы серверной части веб-доступа фиксируются события о запуске и завершении процессов SBRte и SBLogon, проверке лицензий на модуль, ошибки о неверном логине и пароле при входе пользователя, ошибки об отсутствии прав доступа на объекты, ошибки о недостоверности подписи.

Клиентская статистика, счетчики и профайлинг операций ведутся, если в файле Web.config для каждого из этих параметров указано значение **enabled="true"**.

> Примечание
> На клиентском компьютере также ведутся лог-файлы, например лог-файл агента веб-доступа.

Сервер NOMAD

<имя сервера>.DirectumWebService.<дата ротации лога>.log – ошибки и предупреждения, возникающие в ходе работы сервера NOMAD.

С точки зрения безопасности в лог-файле сервера NOMAD фиксируются ошибки о неверном логине и пароле при входе пользователя, ошибки о недостоверности подписи, экспорт и импорт документов, выполнение различных операций.

Путь до хранения лог-файла указывается в параметре **LogsDirectory** файла Web.config. Если папка не существует или не указана, лог-файлы помещаются в папку веб-сервиса в App_Data\Logs.

Уровень детальности лог-файла настраивается в параметре **LogLevel** файла Web.config. Возможные уровни:

- **0** – исключения и сообщения об ошибках;
- **1** – исключения, сообщения об ошибках и предупреждения;
- **2** – исключения, сообщения об ошибках, предупреждения и информационные сообщения;
- **3** – все сообщения.

> Примечание
> Лог-файлы также ведутся на устройствах, на которых установлены клиентские приложения NOMAD.

Механизмы межсистемного взаимодействия (DCI)

Информация о работе механизмов межсистемного взаимодействия записывается в лог-файл <Имя компьютера>.<Сервис DCI>.log. Папка для хранения лог-файлов задается при установке сервисов DCI.

В лог-файлы записываются ошибки, предупреждения и другая информация о работе сервисов. Уровень протоколирования определяет, какая информация записывается.

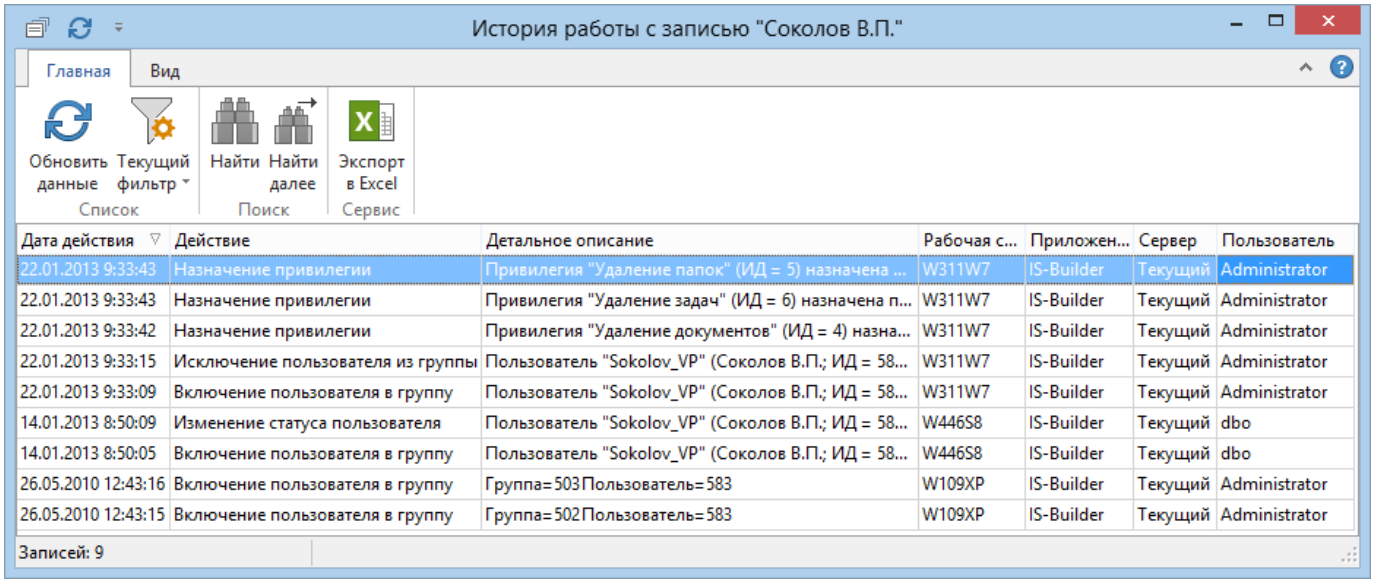
По умолчанию сервисы DCI ведут логирование в файлы. Администратор может настроить логирование в базу данных Microsoft SQL Server.

Подробнее см. документ «DIRECTUM 5.6. Механизмы межсистемного взаимодействия 1.1. Описание технического решения», раздел «Лог-файлы сервисов DCI».

История изменений прав доступа

Для контроля назначения прав доступа на компоненты и объекты системы существует возможность просматривать историю изменений записей компонент **Пользователи**, **Группы пользователей**, **Компоненты** и **Привилегии**.

Информация об изменении прав доступа к записи компоненты доступна в окне истории работы с записью в колонке «Действие», например:



Дата действия	Действие	Детальное описание	Рабочая с...	Приложен...	Сервер	Пользователь
22.01.2013 9:33:43	Назначение привилегии	Привилегия "Удаление папок" (ИД = 5) назначена ...	W311W7	IS-Builder	Текущий	Administrator
22.01.2013 9:33:43	Назначение привилегии	Привилегия "Удаление задач" (ИД = 6) назначена п...	W311W7	IS-Builder	Текущий	Administrator
22.01.2013 9:33:42	Назначение привилегии	Привилегия "Удаление документов" (ИД = 4) назна...	W311W7	IS-Builder	Текущий	Administrator
22.01.2013 9:33:15	Исключение пользователя из группы	Пользователь "Sokolov_VP" (Соколов В.П.; ИД = 58...	W311W7	IS-Builder	Текущий	Administrator
22.01.2013 9:33:09	Включение пользователя в группу	Пользователь "Sokolov_VP" (Соколов В.П.; ИД = 58...	W311W7	IS-Builder	Текущий	Administrator
14.01.2013 8:50:09	Изменение статуса пользователя	Пользователь "Sokolov_VP" (Соколов В.П.; ИД = 58...	W446S8	IS-Builder	Текущий	dbo
14.01.2013 8:50:05	Включение пользователя в группу	Пользователь "Sokolov_VP" (Соколов В.П.; ИД = 58...	W446S8	IS-Builder	Текущий	dbo
26.05.2010 12:43:16	Включение пользователя в группу	Группа=503Пользователь=583	W109XP	IS-Builder	Текущий	Administrator
26.05.2010 12:43:15	Включение пользователя в группу	Группа=502Пользователь=583	W109XP	IS-Builder	Текущий	Administrator

Записей: 9

В историю записываются совершенные действия, например, изменение прав доступа, включение и выключение шифрования для документа, назначение привилегии, изменение пароля пользователя.

Инциденты безопасности записываются не в историю работы с записью, а в лог-файлы.

Криптография

В системе DIRECTUM есть возможность подписывать электронной подписью и шифровать тексты документов и задач.

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

Шифрование предназначено для дополнительной защиты документов и задач и позволяет скрыть их от администраторов системы и замещающих.

Способы подписания и шифрования текстов:

- подписание на основе сертификата;
- шифрование на основании сертификата;
- шифрование с паролем.

Чтобы пользователи могли подписывать и шифровать тексты на основе сертификата, администратор выдает и регистрирует сертификаты, а также настраивает на рабочих местах модули шифрования и подписания.

> Примечания
> 1. Для подписания и шифрования текстов в веб-доступе на компьютере пользователя должен быть установлен Агент веб-доступа.
> 2. В мобильных приложениях DIRECTUM не поддерживается работа с шифрованными документами, задачами и заданиями. Если документ зашифрован с помощью сертификата, в NOMAD-приложение передается только ссылка на документ.

В стандартную поставку системы DIRECTUM входят три модуля, которые используют разные криптографические средства.

Модули устанавливаются автоматически при установке клиентской части системы DIRECTUM. Возможность использования зависит от установленного программного обеспечения.

Модуль	Действие	Требуемое ПО
Standard Encryption	Шифрование Подписание	Microsoft .NET Framework 3.5 SP1 и выше
GOST Encryption	Шифрование Подписание	Криптопровайдер КриптоПро или ViPNet, Microsoft .NET Framework 3.5 SP1 и выше
Bicrypt Signing	Подписание	Криптопровайдер Бикрипт

Standard Encryption

Модуль расширения Standard Encryption используется для шифрования и подписания по алгоритмам 3DES, RSA и DSA и ECDSA.

Поддерживаются сертификаты, выданные программно через CryptoAPI или Cryptography API: Next Generation (CNG).

GOST Encryption

Модуль расширения GOST Encryption используется для шифрования и подписания по алгоритмам ГОСТ. Для использования модуля расширения необходим криптопровайдер КриптоПро или ViPNet.

Bicrypt Signing

Модуль расширения Bicrypt Signing используется для подписания электронной подписью. Для использования модуля расширения необходим криптопровайдер Бикрипт-КБС-С.

При выборе СКЗИ (средства криптографической защиты информации) следует обращать внимание на наличие и срок действия сертификации СКЗИ в государственных органах, а также на класс защищенности. Так, например, криптопровайдер Бикрипт имеет сертификат соответствия ФСБ: его можно использовать для обеспечения целостности и подлинности информации, не содержащей государственную тайну.

Для использования любого модуля расширения администратор задает настройки модуля в окне параметров системы DIRECTUM на закладке «Модули расширения». Подробнее см. в руководстве администратора, раздел «Модули подписания и шифрования».

В организации можно установить собственный центр сертификации – службу сертификации Active Directory. Службы сертификатов Active Directory можно использовать для создания одного или нескольких центров сертификации, которые будут получать запросы на сертификаты, проверять данные запросов, идентифицировать запрашивающую сторону, выдавать и отзывать сертификаты,

публиковать данные об отзывах сертификатов. Следует учитывать, что сертификаты, выдаваемые собственным центром сертификации, не будут считаться квалифицированными.

Подробнее порядок установки и настройки службы сертификации Active Directory и ее компонентов см. в руководстве администратора, в разделе «Центр сертификации».

> Примечание
> В разделе описан пример настройки службы сертификации. Настраивайте службу сертификации Active Directory и ее компоненты с учетом политики безопасности предприятия.

В целях повышения безопасности данных закрытые ключи, используемые для шифрования и подписания документов DIRECTUM, рекомендуется хранить на съемных носителях. Например, в качестве такого носителя может выступать электронный идентификатор Рутокен. Безопасность обеспечивается тем, что подписание производится непосредственно на токене, закрытый ключ при этом недоступен вне токена. Токен сертифицирован ФСБ и ФСТЭК, поэтому, ЭП, установленная на документ с их помощью считается квалифицированной. Один токен можно использовать для подписания документов в десктоп-клиенте, веб-клиенте и мобильном приложении DIRECTUM Solo для Android.

> Примечание
> В мобильных приложениях DIRECTUM, за исключением DIRECTUM Solo и DIRECTUM Jazz для Android, поддерживается работа только с криптопровайдером КриптоПро. В приложениях DIRECTUM Solo и DIRECTUM Jazz, помимо КриптоПро, поддерживается подписание с помощью сертификатов, выданных УЦ Microsoft.

Объектная модель IS-Builder позволяет программно устанавливать ЭП в расширенных форматах CAdES-XL и CAdES-A. CAdES-XL обеспечивает защиту от подмены сертификата и возможность офлайн-проверки подписи. CAdES-A, дополнительно к CAdES-XL, обеспечивает юридическую значимость документов при их длительном хранении за счет использования архивных штампов времени. Подробнее см. в руководстве по объектной модели IS-Builder, в разделе «Криптография и ЭП».

Обеспечение целостности и доступности информации

Для обеспечения целостности и доступности информации, которая хранится в системе DIRECTUM, необходимо осуществлять:

- резервное копирование и восстановление БД
- кластеризацию

Резервное копирование и восстановление БД

Одним из способов обеспечения сохранности и безопасности данных является создание резервных копий базы данных. Копии должны храниться на носителе, физически расположенном в месте, отличном от места хранения базы данных (на случай пожаров, потопов, терактов, стихийных бедствий и других чрезвычайных происшествий).

Выделяют полное резервное копирование БД, разностное резервное копирование БД и резервное копирование журнала транзакций. Резервное копирование осуществляется по расписанию с использованием заданий SQL-сервера.

В SQL Server для БД существует три модели восстановления:

- **Full model** – позволяет восстановить БД до состояния, в котором она была на момент сбоя или на любой указанный момент времени. Этот режим обеспечивает максимальные возможности восстановления;
- **Bulk-Logged model** – позволяет восстановить БД до состояния, в котором она была на момент сбоя или на любой указанный момент времени, если после последнего полного резервного копирования в базе данных не выполнялись команды:
    - массовая вставка, например, при репликации;
    - вставка/изменение больших двоичных данных, например, при изменении данных в текстовых реквизитах, изменении версий документов;
    - операции по созданию, перестроению и удалению индексов, например, при генерации серверной части при конвертации системы;
- **Simple model** – позволяет восстановить БД только до момента, на который была сделана последняя полная или разностная резервная копия. Подразумевает более простое восстановление базы в случае сбоя – восстанавливается последняя полная копия базы данных и последняя разностная резервная копия.

  Этот режим устанавливается по умолчанию у базы данных при установке DIRECTUM.

В стандартной версии DIRECTUM настраивается полное резервное копирование один раз в день и разностное резервное копирование каждый час. В случае перевода базы данных в режим восстановления **Full** или **Bulk-logged** рекомендуется создавать раз в день полную копию БД, разностные резервные копии каждые 1-2 часа, резервные копии журнала транзакций каждые 15-30 минут. Это позволит минимизировать потери и действия по восстановлению базы в случае сбоя.

Подробнее см. в руководстве администратора, в главе «Обслуживание БД», раздел «Резервное копирование БД».

Подробнее порядок создания резервных копий и восстановления БД см. в руководстве администратора, в разделе «Резервное копирование БД», входит в комплект документации.

Кластеры

Для обеспечения отказоустойчивости системы DIRECTUM рекомендуется использовать кластер – совместная работа группы независимых серверов позволит повысить доступность приложений и служб. Подробнее см. документ «DIRECTUM. Инструкция по установке», входит в комплект документации.

Для обеспечения бесперебойной работы веб-доступа также можно использовать кластер. Для распределения клиентских запросов между узлами кластера используется служба Network Load Balancing (NLB). Служба объединяет в кластер несколько одновременно работающих серверов и тем самым обеспечивает высокую доступность и масштабируемость веб-доступа.

Доступность обеспечивается за счет перенаправления клиентских запросов на работающие узлы кластера в случае сбоя или отключения одного из узлов. Масштабируемость и повышение управляемости достигается за счет того, что запросы пользователей равномерно перераспределяются по узлам кластера.

Подробнее о настройке кластера см. в документе «DIRECTUM. Инструкция по установке», входит в комплект документации.

Сервер СУБД и сервисные службы системы DIRECTUM

В состав системы DIRECTUM входят сервисные службы:

- сервер сеансов – служба «IS-Builder Session Server». Осуществляет мониторинг подключений к системе и управление блокировками объектов;
- служба Workflow – служба «IS-Builder Workflow Processing». Обеспечивает обработку маршрутов задач;
- служба обработки событий – служба «IS-Builder Event Processing». Обрабатывает серверные события.

  Сервер сеансов, служба Workflow и служба обработки событий взаимодействуют с базой данных системы DIRECTUM от имени предопределенного пользователя системы ISBuilderSystem;
- служба поиска – служба «IS-Builder Search Service». Выполняет полнотекстовые поисковые запросы. Индексирование данных выполняется с помощью набора серверных событий. Механизм полнотекстового поиска основан на поисковой системе Elasticsearch;
- служба проверки подписей – служба «DIRECTUM Signature Verifier Service». Проверяет отдельные элементы электронных подписей – штампы времени и OCSP-ответы. Служба обеспечивает взаимодействие плагинов шифрования с приложениями КриптоПро TSP Client и КриптоПро OCSP Client.

  OCSP-ответ (Online Certificate Status Protocol) – ответ, полученный от OCSP-сервера удостоверяющего центра о статусе сертификата и подписанный сертификатом OCSP-сервера;
- служба преобразования документов – предназначена для преобразования документов из различных форматов в форматы PDF и HTML, например, при экспорте или импорте документа, создании версии документа.

Информацию о взаимодействии компонентов системы см. в руководстве администратора, в разделе «Архитектура системы DIRECTUM».

В зависимости от нагрузки сервисные службы можно установить на один компьютер с серверной частью (сервер СУБД) или на разные компьютеры. Например, при большом потоке задач рекомендуется установить несколько служб Workflow на разных серверах. Подробнее см. в документе «Типовые требования к аппаратному и программному обеспечению», входит в комплект документации.

Службу поиска и компоненты Elasticsearch рекомендуется устанавливать на отдельный компьютер. В этом случае требуется настройка безопасного доступа к Elasticsearch. Подробнее см. в руководстве администратора, раздел «Настройка безопасного доступа к Elasticsearch».

Сервисные службы в процессе работы используют один порт TCP/IP, а клиентские процессы – несколько портов в определенном диапазоне. Номера портов задаются при установке системы и отражаются в установках системы:

- **SessionServerPort** – порт сервера сеансов. Значение по умолчанию **32300**;
- **WorkflowServicePort** – порт службы Workflow. Значение по умолчанию **32310**;
- **ClientMinimalPort** – минимальный номер порта клиента. Значение по умолчанию **32330**;
- **ClientMaximalPort** – максимальный номер порта клиента. Значение по умолчанию **32714**.

Для корректной работы **служб преобразования документов в PDF и HTML** необходимо указать номер TCP-порта с учетом нагрузки на службу преобразования. Допустимы значения от **1025** до **65535** включительно. По умолчанию указаны значения **40108**, **40109** и **40110** для PDF и **40111** для HTML. Для каждой службы номера портов должны отличаться.

> Примечание
> Если при установке служб преобразования документов выбран вариант использования одной службы преобразования документов в PDF, необходимо указать только один порт.

Для корректной работы сервисных служб на компьютерах с установленными сервисными службами и на клиентских рабочих станциях должны быть открыты следующие порты:

- на компьютере с установленным сервером сеансов– порт из установки **SessionServerPort**;
- на компьютере с установленной службой Workflow – порт из установки **WorkflowServicePort** и порты из диапазона [**ClientMinimalPort**, **ClientMaximalPort**];
- на компьютере с установленной службой обработки событий и на клиентских рабочих станциях – порты из диапазона [**ClientMinimalPort**, **ClientMaximalPort**].

Для работы SQL-сервера на компьютере с установленной серверной частью системы DIRECTUM должны быть открыты порты: TCP-порт **1433** и UDP-порт **1434**.

Для корректной работы системы порты не должны использоваться другими приложениями и должны быть открыты в брандмауэре. Порты сервисных служб не должны попадать в диапазон портов клиентской части.

При установке и активации системы DIRECTUM создаются предопределенные пользователи и предопределенные роли SQL-сервера для использования во внутренних механизмах IS-Builder и начальной настройки системы. Подробнее см. разделы «Предопределенные пользователи системы DIRECTUM» и «Предопределенные роли SQL-сервера».

Сервисные учетные записи

Для работы системы DIRECTUM необходимы следующие сервисные учетные записи:

- для установки системы – учетная запись пользователя, обладающая правами локального администратора Windows, например Администратор;
- для работы с SQL-сервером – учетная запись, обладающая правами администратора SQL-сервера, как правило, это пользователь sa, либо пользователь Windows, обладающий полными правами на базу данных DIRECTUM.

  Если пользователь, от имени которого идет обращение к SQL-серверу не sa, то для него необходимо указать серверные роли **sysadmin** или **securityadmin**, чтобы иметь полный функционал управления учетными записями пользователей DIRECTUM.

  Под полными правами над базу данных DIRECTUM понимается вхождение в роль **db_owner** БД системы DIRECTUM.

Предопределенные пользователи системы DIRECTUM

При установке и активации системы создаются следующие пользователи:

- **Conductor** – служебный пользователь, обладающий минимальными привилегиями. Используется при запуске SBLogon.exe для получения данных, необходимых для аутентификации пользователей;
- **ISBuilderSystem** – предопределенный служебный администратор. Используется сервером сеансов и службой Workflow. Имеет набор привилегий, соответствующий набору привилегий группы «Администраторы». Для пользователя генерируется пароль высокой сложности, уникальный в рамках сервера;
- **Administrator** – предопределенный администратор системы. Имеет набор привилегий, соответствующий набору привилегий группы «Администраторы». Используется для начальной настройки системы. После первоначальной настройки можно изменить пароль и тип аутентификации в соответствии с политиками безопасности организации, или вовсе отключить этого пользователя.

Предопределенные роли SQL-сервера

При установке и активации системы создаются следующие предопределенные роли SQL-сервера:

- **IS-Builder Application Role2** – роль приложения, активируется при работе пользователей с Windows-аутентификацией. Создается при генерации серверной части, при активации системы генерируется пароль высокой сложности.

  В системе DIRECTUM оставлена роль приложения «IS-Builder Application Role» для совместимости с ее ранними версиями;
- **IS-Builder Users** – роль базы данных, в которую входят пользователи системы с аутентификацией, отличной от Windows-аутентификации. У роли нет прав на таблицы базы данных, изменение которых запрещено из соображений безопасности.

Прозрачное шифрование данных (TDE)

В случае несанкционированного доступа к информационному ресурсу злоумышленник получает прямой доступ к данным. Например, при хищении физического носителя с базой данных или ее резервной копией. Одним из решений является шифрование данных.

В Microsoft SQL Server 2012 и выше есть функция прозрачного шифрования данных (Transparent Data Encryption, TDE). TDE в реальном времени шифрует данные, журналы и резервные копии БД.

Администратор SQL-сервера имеет доступ к зашифрованным данным. Подробнее см. в документации Microsoft, статью «Прозрачное шифрование данных (TDE)».

> Примечание
> Прозрачное шифрование может увеличивать загрузку процессора сервера СУБД в 2-3 раза.

Клиентская часть

Для обеспечения безопасности на рабочие места всех пользователей, кроме администраторов и разработчиков, рекомендуется устанавливать Lite-версию клиентской части. По сравнению с полной версией клиентской части, Lite-версия не содержит утилиты, предоставляющие доступ к управлению разработкой и администрированием системы. Отсутствие таких файлов ограничивает доступ пользователей к работе с данными, что дает дополнительную защиту системы от некорректных действий в БД.

Файловые хранилища

Файловые хранилища предназначены для размещения текстов документов в файловых системах одного или нескольких компьютеров. Это позволяет уменьшить объем БД SQL-сервера и предоставляет широкие возможности в организации работы с документами. Например, в файловых хранилищах можно размещать документы большого объема.

На каждом компьютере, на котором размещается файловое хранилище, устанавливается служба файловых хранилищ «IS-Builder File Storage Service». Служба управляет доступом к файлам хранилищ текстов документов. Если документы должны учитываться при полнотекстовом поиске, служба файловых хранилищ должна работать от имени доменной учетной записи.

Все экземпляры службы файловых хранилищ должны быть настроены на работу через один и тот же порт. Для корректной работы системы порт должен:

- быть открыт в брандмауэре;
- не использоваться другими приложениями;
- не попадать в диапазон портов клиентской части.

По умолчанию для службы файловых хранилищ используется порт **32320**.

Для ограничения доступа пользователей к файлам хранилища рекомендуется использовать контроль прав доступа. Права доступа к файлам назначаются автоматически службой файловых хранилищ при выполнении условий:

- в справочнике **Хранилища текстов документов** в поле ***Контроль прав доступа** указано значение **Да**;
- в сети используется домен или рабочая группа Windows;
- если используется рабочая группа, то на компьютере с файлами хранилища зарегистрированы все пользователи этой группы.

В результате при обращении пользователя к документу, текст которого размещен в файловом хранилище, пользователь получит права доступа, соответствующие правам доступа на документ в системе DIRECTUM.

Чтобы избежать потери текстов документов, размещаемых в файловых хранилищах, следует настраивать их резервное копирование. Подробнее см. в руководстве администратора, в разделе «Резервное копирование файлов хранилища».

Серверные события

Серверные события предназначены для выполнения ISBL-вычислений на отдельном сервере. В карточке серверного события указываются сценарии, которые реализуют логику события. Серверные события запускаются из ISBL-вычислений и обрабатываются службой обработки событий, которая выполняет сценарии этого события.

Некоторые вычисления рекомендуется выполнять на отдельном сервере с точки зрения информационной безопасности. А именно:

- вычисления, которые либо небезопасно выполнять на клиентском компьютере, либо невозможно из-за требования повышенных привилегий. Вычисления выполняются на сервере от имени предопределенного пользователя системы ISBuilderSystem. При этом обычные пользователи не смогут посмотреть ISBL-код или повлиять на его работу;
- вычисления, использующие конфиденциальную информацию, которая не должна обрабатываться на компьютерах пользователей;
- вычисления, требующие специального ПО, которое нецелесообразно использовать на клиентских компьютерах по соображениям безопасности.

Механизмы межсистемного взаимодействия (DCI)

Механизмы межсистемного взаимодействия DIRECTUM (DIRECTUM Cross-system Interaction Toolset, DCI) предназначены для организации сквозных бизнес-процессов и синхронизации данных между несколькими разнородными бизнес-приложениями.

Механизмы DCI включают:

- **Компоненты DCI в бизнес-приложении**, необходимые для реализации межсистемного взаимодействия. В стандартную поставку DCI входит набор компонент системы DIRECTUM, включающий в себя ISBL-функции, серверные события и справочники;
- **Адаптер к бизнес-приложению** – веб-приложение на IIS, которое получает данные от системы, участвующей во взаимодействии. В стандартную поставку DCI входит адаптер к DIRECTUM.

  Сообщение межсистемных процессов – единица информации, которой обмениваются системы друг с другом в рамках межсистемного процесса;
- **Сервис маршрутизации DCI** – веб-приложение на IIS, которое распределяет сообщения межсистемных процессов по получателям;
- **Адаптер к транспорту DCI** – веб-приложение на IIS, которое преобразует сообщения межсистемных процессов в транспортные пакеты и передает их транспорту.

  Транспортный пакет – единица информации, которая передается через транспорт. Одно сообщение для передачи в другую систему может быть преобразовано в один или более транспортных пакетов;
- **Транспорт DCI** – веб-приложение на IIS, которое осуществляет прием и передачу пакетов между адаптерами к транспорту систем-участниц межсистемного процесса.

В межсистемном взаимодействии участвуют только синхронизируемые системы. При этом системы слабо зависят друг от друга, так как передается только необходимая информация.

Есть два основных варианта связи систем:

- системы находятся внутри одной локальной сети. Рекомендуется их связывать без использования транспортов DCI;
- системы находятся в разных локальных сетях. Рекомендуется их связывать через полный набор сервисов DCI.

Также возможен комбинированный вариант, при котором две системы находятся в одной локальной сети, а третья – в другой.

Доступ к папкам для хранения передаваемых пакетов, лог-файлов ограничивается правами пользователей Windows, от имени которых работают пулы приложений.

Администратор настраивает список разрешенных сертификатов для подключения к сервису маршрутизации, адаптеру к DIRECTUM, транспорту DCI и адаптеру к транспорту DCI.

Чтобы обеспечить дополнительную безопасность, рекомендуется:

- для работы всех веб-приложений использовать защищенный протокол HTTPS;
- в IIS с помощью настройки IP Address Restrictions разрешить доступ к веб-приложениям только с указанных IP-адресов;
- транспорт DCI устанавливать в демилитаризованных зонах (ДМЗ);
- сервисы рабочей и тестовой систем устанавливать на разных серверах.

Подробнее см. документ «DIRECTUM 5.6. Механизмы межсистемного взаимодействия 1.1. Описание технического решения», раздел «Настройка безопасного обмена».

Службы взаимодействия систем (DICS)

Службы взаимодействия систем предназначены для обмена объектами с другими системами DIRECTUM.

Для обмена данными с другими системами в локальной сети устанавливаются и настраиваются один или несколько агентов – отдельный для каждого объединения DICS. Обмен данными между агентами системы осуществляется посредством контроллеров. В объединении может быть один или несколько контроллеров, в зависимости от политики администрирования, принятой в данном объединении.

Службу агента DICS и службу контроллера рекомендуется запускать от учетной записи, обладающей правами администратора Windows, но при необходимости можно настроить запуск служб от учетных записей, не обладающих правами администратора. Подробнее см. в книге «Службы взаимодействия систем», в главе «Управление агентами и контроллерами».

По умолчанию для серверной и клиентской части агента DICS, а также контроллера DICS используется порт **80**.

Безопасность обмена данными обеспечивается тем, что DICS может использоваться только с организациями, которые входят в объединение DICS. При этом системы слабо зависят друг от друга – передается только необходимая информация.

Передавать и принимать объекты из других систем могут только пользователи, в карточке которых установлен флажок **Публичный пользователь**. Включение пользователя в публичную группу или роль не делает его публичным.

Верно обрабатываются ситуации, когда в удаленную систему отправляется задача от непубличного пользователя (например при программном создании задачи). В этом случае инициатор заменяется служебным пользователем LocalSystem, чтобы информация о локальном пользователе не распространилась в удаленную систему.

Чтобы повысить уровень безопасности передачи данных между системами, рекомендуется:

- устанавливать контроллер DICS на отдельный сервер, расположенный вне локальной сети предприятия, так как контроллер DICS выводится во внешнюю сеть;
- использовать сертификаты шифрования для безопасного обмена данными между контроллером и агентом.

Веб-доступ

Веб-доступ предназначен для работы с системой DIRECTUM через браузеры компьютеров и планшетов. Пользователи заходят на сайт веб-доступа и выполняют действия с объектами системы DIRECTUM. Доступ к сайту может осуществляться через локальную сеть организации или через глобальную сеть Интернет. Действия пользователей обрабатываются серверной частью веб-доступа, которая должна находиться в локальной сети организации.

Для работы серверной части веб-доступа требуется создать учетные записи:

- пользователь Windows, от имени которого будет запускаться пул приложений DIRECTUMWebAccess. Создается в операционной системе на веб-сервере. Не рекомендуется использовать учетные записи по умолчанию. Пользователя необходимо включить в локальную группу «IIS_IUSRS»;
- регистрационная запись на SQL-сервере (login) для внутренней связи серверной части веб-доступа с БД системы DIRECTUM. Создается в БД Microsoft SQL Server. Пользователь должен входить в роли «Public» на SQL-сервере и «db_owner» в БД системы DIRECTUM;
- пользователь для запуска процессов DIRECTUM. Создается в операционной системе на веб-сервере. Пользователь должен входить в группу Windows «Пользователи DCOM» и иметь права на локальный вход в систему.

Подробнее об учетных записях и правах доступа, необходимых для работы, см. в документе «Инструкция по установке», входит в комплект документации.

После установки сервера веб-доступа разрешите соединение по портам:

- протокол TCP/IP:
    - для связи с SQL сервером – по умолчанию порт 1433;
    - для связи с сервером с установленной службой сеансов – по умолчанию порт 32300;
    - для работы сервера веб-доступа по протоколу HTTPS – порт 443;
    - для работы сервера веб-доступа по протоколу HTTP – порт 80;
- протокол UDP/IP: для разрешения имен NetBIOS – по умолчанию порты 137-139.

> Примечание
> Указан минимальный набор портов и протоколов связи. При использовании в продуктивной среде возможно расширение разрешающих правил. К примеру, для работы служб файловых хранилищ понадобится дополнительно открыть порты 445 и 32320 по протоколу TCP.

Безопасная и бесперебойная работа веб-доступа обеспечивается:

- шифрованием информации, передаваемой по каналам связи, на основе протокола HTTPS – это позволяет защитить соединение серверной части веб-доступа с системой DIRECTUM;
- настройкой демилитаризованной зоны для дополнительной защиты веб-сервера в организации;
- настройкой VPN для подключения к сети организации;
- настройкой параметров безопасности для приложений Microsoft Office, открываемых в предпросмотре. Подробнее см. в руководстве администратора веб-доступа, раздел «Настройка приложений Microsoft Office»;
- шифрованием параметров подключения к базе данных в конфигурационном файле веб-доступа.

Взаимодействие с компонентами системы

Веб-доступ обращается к данным системы DIRECTUM через .NET-сборку SBRSE.

SBRSE взаимодействует с другими компонентами системы:

- создает сессию пользователя на сервере сеансов;
- использует SBLogon.exe для аутентификации пользователей с перекодированным паролем;
- запрашивает объекты системы в базе данных;
- обращается к серверу сеансов для проверки лицензий и установки блокировок на объекты системы.

Все запросы к базе данных SBRSE выполняет под одной учетной записью – системным пользователем SBRSE. Это позволяет максимально эффективно использовать пул соединений с базой данных.

При каждом запросе данных происходит проверка прав пользователя. Это обеспечивает контроль доступа к объектам системы.

Ограничения в API веб-доступа исключают прямой доступ к базе данных. Это защищает ее от выполнения запросов без авторизации действий, а также запросов в обход бизнес-логики продукта.

Аутентификация запросов Агента веб-доступа

Агент веб-доступа – это приложение, которое позволяет редактировать документы, подписывать и шифровать документы, задачи и задания.

Для аутентификации и авторизации запросов Агента к серверу веб-доступа используются токены операций. Сервер веб-доступа сравнивает адрес входящего запроса и адрес, привязанный к токену.

Если пользователю нужно выполнить действие с помощью Агента, то клиентский код, выполняемый в браузере, запрашивает у сервера веб-доступа токен операции. После этого:

1. Сервер веб-доступа генерирует токен.
2. Сервер веб-доступа привязывает токен к определенному пользователю по IP-адресу клиента, а также к операции, которую пользователь собирается выполнить.
3. Агент получает токен вместе с запросом, который он должен выполнить.
4. Агент прикрепляет полученный токен к запросу на сервер веб-доступа вместе с другими параметрами.
5. Сервер веб-доступа определяет, есть ли в запросе токен операции. Если в запросе есть токен и он корректен, то авторизация запроса проходит успешно и действие пользователя выполняется.

Токен имеет срок жизни. Когда срок истекает, токен не используется.

Чтобы исключить перехват токена, взаимодействие между браузером и Агентом веб-доступа происходит по протоколу HTTPS.

Настройка защищенного соединения

Для обеспечения безопасной передачи информации по каналам связи, рекомендуется настроить защищенное соединение по протоколу HTTPS. В результате информация, передаваемая по каналам связи, будет шифроваться. Подробнее о настройке защищенного соединения см. в документе «Инструкция по установке», входит в комплект документации.

При входе на сайт веб-доступа пользователь переходит по ссылке **Установить сертификат удостоверяющего центра** и устанавливает скачанный сертификат. При попытке подключения по HTTPS с использованием невалидного сертификата пользователь уведомляется о возможных угрозах безопасности, при этом дальнейшая работа с веб-доступом невозможна.

Рекомендуется, чтобы сертификат удостоверяющего центра отвечал следующим требованиям:

- длина закрытого ключа – 2048 бит;
- алгоритм хеширования – SHA256;
- криптографический протокол – TLS 1.1 или TLS 1.2.

> Примечание
> Некоторые устаревшие версии браузеров могут не поддерживать протоколы TLS 1.1 и TLS 1.2.

VPN для подключения к сети организации

В некоторых случаях публикация отдельных веб-приложений для организации не является возможной, например в связи с необходимостью получения индивидуального доменного имени для сервиса или с требованиями службы безопасности предприятия.

В такой ситуации для использования веб-доступа можно обеспечить подключение к внутренней сети организации с помощью технологии VPN. Для этого настройте и включите VPN перед подключением к сайту веб-доступа.

Рекомендуется использовать только защищённые VPN, такие как IPSec, OpenVPN, PPTP.

Организовать подключение к VPN можно как нативными средствами ОС, так и с использованием сторонних решений.

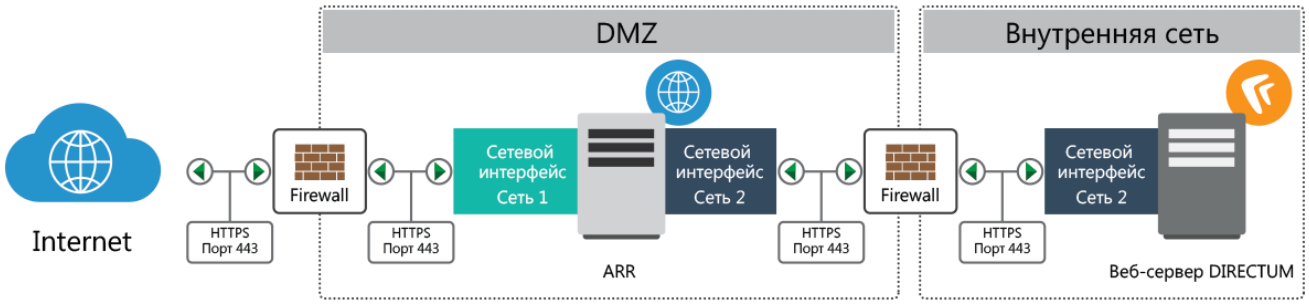
Использование DMZ и брандмауэров для защиты веб-сервера

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

> Примечание
> Данные рекомендации также можно использовать для обеспечения безопасности сервера NOMAD и серверов с другими веб-приложениями.

Для этого понадобится настроить сервера:

- сервер ARR – физический или виртуальный сервер, предназначенный для балансировки нагрузки веб-фермы IIS и реализованный с помощью продукта Microsoft Application Request Routing (ARR);
- сервер веб-доступа – физический или виртуальный сервер, на котором развернут сервер веб-доступа к системе DIRECTUM.



Сервер ARR использует два сетевых интерфейса. Пример настройки сетевых интерфейсов серверов ARR и WebAccess:

- 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 Web Access сети 2 – 192.168.1.2/255.255.255.0.

Настройка сервера ARR

На сервере ARR развернута веб-ферма, в которую добавлен сервер WebAccess. Благодаря веб-ферме сервер ARR используется как прокси для веб-запросов из Интернета, адресованных серверу веб-доступа к системе DIRECTUM.

> Примечание
> Подробнее о создании и настройке веб-фермы IIS с помощью Application Request Routing см. в документе «DIRECTUM. Инструкция по установке», входит в комплект документации.

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 веб-доступа

Для дополнительной безопасности рекомендуется ограничить количество потенциальных точек доступа к серверу WebAccess из внутренней сети и разрешить сетевые соединения сервера веб-доступа только с сервером балансировки нагрузки веб-фермы, СУБД и серверами приложений. Для этого настройте правила брандмауэра WebAccess для входящих и исходящих соединений и разрешите соединения по необходимым портам. Список портов см. в разделе «Веб-доступ».

Федеративный поиск

Федеративный поиск предназначен для поиска документов и задач по заданным критериям одновременно в нескольких системах DIRECTUM, в том числе территориально распределенных. Поддерживается поиск в системах DIRECTUM текущей версии и в системах версии 5.0 и выше.

Федеративный поиск состоит из трех компонент:

- сайт федеративного поиска – сайт для поиска документов и задач по нескольким экземплярам системы DIRECTUM. Используется для выбора систем для поиска, задания критериев и отображения результатов;
- сервис федеративного поиска – сервис, являющийся частью сайта федеративного поиска. Отправляет поисковые запросы пользователя сервисам поиска и собирает результаты поиска в единый список;
- сервис поиска данных – сервис, являющийся частью веб-доступа. Выполняет поиск объектов в конкретной системе DIRECTUM по запросу сервиса федеративного поиска.

Чтобы работать с сайтом федеративного поиска, нужно на компьютере пользователя в браузере разрешить выполнение активных сценариев.

Чтобы обеспечивать безопасность федеративного поиска, необходимо защитить два канала связи:

- от пользователя до сайта федеративного поиска. Канал защищается настройкой соединения по протоколу HTTPS;
- от сайта федеративного поиска и сервиса федеративного поиска до сервиса поиска данных. Канал защищается настройками безопасности сервисов поиска. Подробнее см. в книге «Федеративный поиск», раздел «Настройка доступа к сайту и сервисам поиска».

Далее рассмотрим аспекты безопасности при использовании разных типов аутентификации:

- сквозная Windows-аутентификация
- аутентификация через форму
- федеративная аутентификация

Сквозная Windows-аутентификация

Сквозная Windows-аутентификация позволяет пользователю не вводить свои учетные данные при входе на сайт федеративного поиска. Вход на сайт происходит автоматически под учетной записью текущего пользователя Windows.

Особенности:

- реквизиты для подключения не передаются по сети;
- сайты федеративного поиска и веб-доступа должны работать в одном домене либо в доменах с настроенным доверием.

Аутентификация через форму

К аутентификации через форму относят Windows-аутентификацию и аутентификацию по паролю.

Особенности:

- реквизиты для подключения передаются с формы браузера на сайт федеративного поиска в открытом виде. Необходима защита соединения от рабочего места пользователя до сайта федеративного поиска;
- сайты федеративного поиска и веб-доступа могут находиться в разных доменах без настроенного доверия.

Федеративная аутентификация

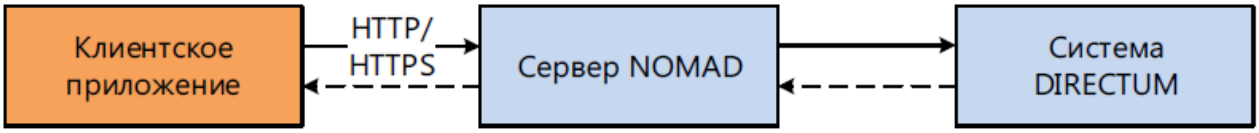
Если используется аутентификация с помощью внешнего провайдера Active Directory Federation Services (AD FS), то при переходе на сайт федеративного поиска открывается сайт провайдера. Пользователь заполняет форму на сайте аутентификации и получает доступ к сайту федеративного поиска.

Администратор настраивает тип аутентификации на сайте AD FS: Windows-аутентификация, аутентификация по паролю.

Все сайты веб-доступа, которые подключены к федеративному поиску с использованием федеративной аутентификации, должны работать по протоколу HTTPS.

Мобильные приложения

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



Для работы с сервером NOMAD требуется создать учетные записи:

- пользователь Windows, от имени которого будет запускаться пул приложений веб-сервиса NOMAD. Создается в операционной системе на веб-сервере. Права пользователя настраиваются автоматически при установке сервера, при необходимости настройте их вручную. Пользователя необходимо включить в группу «IIS_IUSRS»;
- регистрационная запись на SQL-сервере (Login) для внутренней связи сервера NOMAD с базой данных системы DIRECTUM. Создается в базе данных Microsoft SQL Server;
- пользователь для запуска процессов DIRECTUM. Создается в операционной системе на сервере.

Подробнее об учетных записях и правах доступа, необходимых для работы, см. в документе «Инструкция по установке», входит в комплект документации.

Взаимодействие сервера NOMAD с мобильными устройствами 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:

- сервера-посредника между внутренней сетью предприятия и сетью Интернет;
- канала связи;
- устройства пользователя;
- электронной подписи;
- данных приложения.

О политике конфиденциальности читайте на сайте DIRECTUM.

Безопасность сети предприятия

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

Безопасность передачи данных

Можно выделить следующие виды передаваемых данных:

- аутентификация:
    - логин и пароль при аутентификации по паролю (SOAP);
    - SSL Client Certificate authentication при аутентификации по сертификатам;

- бинарные данные:
    - тела документов;
    - фотографии сотрудников;
- метаинформация (SOAP). Например, карточки документов, справочников, заданий, переписка по заданиям.

Приложения могут взаимодействовать с сервисом по протоколу HTTP – открытому небезопасному каналу связи. Использовать его рекомендуется только в условиях работы с тестовой средой или демостендом.

При попытке подключения по открытым каналам приложения DIRECTUM Jazz и DIRECTUM Solo для Android сообщат о возможной угрозе безопасности.

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

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

Мобильные приложения DIRECTUM используют протоколы TLS 1.1 и TLS 1.2. Протокол и версия, с которой клиент будет взаимодействовать с сервером, зависит от настроек IIS на сервере.

При попытке подключения по HTTPS с использованием невалидного сертификата мобильное приложение сообщает пользователю о возможной угрозе безопасности. Дальнейшая работа с сервисом невозможна.

Если сертификат выдан внешним доверенным центром сертификации (ЦС), то дополнительная настройка не требуется.

Если сертификат выдан внутренним ЦС, то необходимо настроить доверие к ЦС. Для этого установите сертификат удостоверяющего центра в соответствующее хранилище устройства.

> Примечание
> Сертификат SHA-1 считается небезопасным. С версии iOS 10.3 для работы с ним требуется дополнительная настройка.

Рекомендации к сертификату см. в разделе «Настройка защищенного соединения».

Безопасность устройства

Безопасность устройства с установленным мобильным приложением обеспечивается:

- 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 один час с момента последней активности пользователя. Продолжительность жизни сессии настраивается администратором;
- централизованным управлением мобильными устройствами с помощью MDM-решений. Например, с помощью решения SafePhone администратор может удаленно установить доверенное приложение или запретить его использование;
- подтверждением подключения мобильного устройства пользователя к серверу 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 сервера NOMAD на устройство;
- удалением данных приложений Jazz и Solo с мобильного устройства пользователем. Например, в случае утери устройства.

  Для приложений Jazz с версии 1.7.1 и Solo с версии 2.1 доступно дистанционное удаление данных с мобильного устройства администратором. Также администратор может запретить работу устройствам, на которых установлены более ранние версии приложений.

Далее в разделе приведены рекомендации по обеспечению безопасности устройств на базе iOS и Android.

Устройства на Android

При авторизации приложение передает реквизиты для подключения пользователя в открытом виде. Для безопасной передачи данных рекомендуется использовать HTTPS-соединение. При этом необходимо использовать сертификат, выданный доверенным центром сертификации.

Особенности хранения данных приложения:

- логин и пароль пользователя хранятся в системных аккаунтах устройства, пароль хранится в зашифрованном виде;
- при аутентификации по сертификату логин и пароль не используются и не хранятся на устройстве;
- загруженные документы хранятся в системной папке приложения в незашифрованном виде. Рекомендуется ограничивать доступ к устройству;
- данные пользователя хранятся в системной базе данных SQLite без шифрования;
- закрытый ключ для подписания документов хранится в KeyChain – системном хранилище учетных данных;
- поддерживается работа с шифрованной файловой системой Full Disk Encryption.

> Примечание
> Не рекомендуется использовать устройства с root-доступом, так как это снижает безопасность использования приложения.

Устройства на iOS

Приложение работает в изолированной области памяти устройства. Другие приложения не имеют к ней доступ. Безопасность данных пользователя обеспечивается средствами операционной системы.

Логин и пароль для подключения хранятся на устройстве с использованием сервисов Keychain и передаются в SOAP-пакете по HTTP-каналу. При аутентификации по сертификату логин и пароль не используются и не хранятся на устройстве.

Документы пользователя загружаются в контейнер приложения, доступ к которому из других приложений или с компьютера невозможен. Сторонние приложения могут получить доступ к документам, только если экспортировать их из DIRECTUM Solo.

Документы шифруются AES-алгоритмом. Для сохранности данных необходимо использовать блокировку устройства. Рекомендуется использовать PIN-код. Графический ключ или отпечаток пальца не являются достаточными мерами защиты.

> Примечание
> Не рекомендуется использовать устройства с jailbreak, так как это снижает безопасность использования приложения.

В DIRECTUM Solo для iOS дополнительно можно настроить шифрование документов средствами КриптоПРО. Если шифрование настроено, веб-сервис на время сеанса работы пользователя генерирует временный ключ, асимметрично шифруемый сертификатом пользователя, и шифрует все передаваемые документы ГОСТ-алгоритмами. В приложении документы также сохраняются в зашифрованном виде. Для просмотра или редактирования документа сессионный ключ расшифровывается закрытым ключом пользователя, и создается расшифрованная копия документа, которая удаляется по окончании сеанса работы в приложении.

Электронная подпись

Мобильное приложение DIRECTUM Solo использует для подписания механизмы:

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

КриптоПро CSP

Подписание с использованием КриптоПро CSP поддерживается во всех мобильных приложениях DIRECTUM. 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 из папки на устройстве и с компьютера пользователя.

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:
   - в ОС Android – средствами ОС с использованием КриптоПро CSP;
   - в ОС iOS – средствами встроенного модуля КриптоПро CSP.
3. Полученный хеш вместе атрибутами, необходимыми для формирования подписи, подписывается в зависимости от ОС аналогично п.2.

Аппаратный ключ (токен)

Мобильные приложения поддерживают токены:

- Solo для iOS – RutokenBT;
- Solo для Android – RutokenBT и JaCarta microUSB.

С токенов можно использовать сертификаты с поддержкой алгоритмов ГОСТ и RSA. Для взаимодействия с токенами используется интерфейс стандарта PKCS#11.

Перед использованием токен 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 пользовательских сертификатов сертификатам, найденным на токене, и определение используемого сертификата.
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.

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.

Устройства на Android

Для подписания используются базовые средства ОС Android. Поддерживаются только RSA-сертификаты.

> Примечание
> В ОС Android для работы с криптографией используется набор библиотек Spongy Caste из стандартной поставки ОС.

На компьютере пользователя создается контейнер с закрытым ключом с расширением .pfx или .p12. После этого контейнер копируется на мобильное устройство. На устройстве сертификат с закрытым ключом устанавливается в системное хранилище KeyChain. В дальнейшем контейнер рекомендуется удалить из папки на устройстве и с компьютера пользователя.

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

Устройства на iOS

Подписание реализовано средствами платформы .NET – обертки Microsoft RSACryptoServiceProvider. Поддерживаются только RSA-сертификаты.

> 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 через iTunes 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 КрипроПро 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 пин-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 DIRECTUM Solo 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 пин-кодом или TouchID.

Безопасность данных

Защита конфиденциальной информации

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 клиентских приложений. Можно запретить или разрешить выгрузку данных на устройство.

Настройки задаются администратором в файле IsBuilderAdapter.config.

Ограничение доступа по логину или группе пользователей

Администратор может настроить доступ к приложениям NOMAD по механизмам белого и черного списков. В настройках плагина UserGroupsValidationPlugin, входящем в состав сервера NOMAD, указываются логины и группы пользователей, для которых доступ к приложениям разрешен или запрещен.

Блокировка приложения по истечении определенного времени бездействия пользователя

В DIRECTUM Solo можно настроить блокировку приложения, которая будет срабатывать по истечении 15 минут неактивности пользователя. Снять блокировку можно по пин-коду или отпечатку пальца. После 5 неудачных попыток входа ввод пин-кода или отпечатка пальца блокируется на некоторое время.