Содержание

Руководство по информационной безопасности

Обеспечение безопасности данных

Хранение информации и доступ к ней

Вся информация, кроме документов, хранится в одной базе данных. Документы хранятся в специальной папке на сервере приложения (C:\SL_Files\Doc_Files). Для обеспечения безопасного доступа рекомендуется создать пользователя в Active Directory, от имени которого будет запускаться пул IIS, и который будет иметь доступ к папке с документами.

Сервер приложения обращается к серверу базы данных, используя специально выделенную администратором учетную запись на SQL сервере.

Сервер приложения осуществляет проверку прав доступа согласно заданным установкам, прежде чем вернуть данные в ответ на запрос пользователя.

Учетные записи пользователей

Для входа в систему пользователь должен указать логин и пароль, который был указан в процессе регистрации в системе. Логин и пароль для пользователей не должны назначаться сторонними лицами.

Пароль, выбранный пользователем при регистрации, в Системе нигде не хранится (ни в базе данных, ни в файловой системе), а хранится только образ пароля, который используется для аутентификации пользователей.

Алгоритм, создающий образ пароля, не является реверсивным, таким образом, никто не может получить и использовать данные чужой учетной записи.

Администратор может задать срок действия учетных записей пользователей. Это имеет смысл делать для сотрудников, доступ к системе которым выдается временно на определенный период. Например, только на срок выполнения проекта.

Для пользователей можно настроить срок действия пароля. По истечении этого срока пользователи получат сообщение о необходимости сменить пароль.

Также настраивается число попыток ввода пароля, при превышении которого пользователь будет заблокирован. Список заблокированных пользователей находится в разделе Администрирование → Управление безопасностью → Безопасность.

Учетная запись Администратора

Рекомендуется формировать в Системе две учетные записи для Администратора:

1. С лицензией Администратор.
   Она привязана на общую почту администраторов (к примеру, support@mail.company). При увольнении Администратора Системы очень просто сменить (восстановить) пароль через почту другому администратору и продолжать пользоваться этой учетной записью для необходимых настроек.
2. С обычной лицензией (исполнитель\руководитель), если таковая необходима.
   При увольнении Администратора эта учетная запись может быть закрыта в обычном порядке. Таким образом, полномочия Администратора могут быть переданы другому пользователю при необходимости.

Для управления доступом пользователям в Системе рекомендуется выделить отдельную пользовательскую учетную запись, которая не будет иметь все права администратора (доступно с версии Системы 3.24 и позднее). Как правило, то важно для крупных компаний, так как часто задачи управления доступом пользователей выполняет сотрудник, который не должен иметь полных прав ко всем данным системы и к изменениям настроек.

Передача данных по сети

Для предотвращения перехвата информации при ее передаче по сетям общего пользования (например, Интернет) необходимо использовать протокол HTTPS с длиной ключа не менее 128 бит.

В целях безопасности все остальные порты можно блокировать.

Доставка уведомлений по электронной почте

Система ADVANTA рассылает уведомления по электронной почте тем пользователям, тем пользователям, у которых стоит флаг о разрешении отправки уведомлений. Для предотвращения перехвата информации, содержащейся в уведомлениях, рекомендуется использовать email через SSL и предпринимать меры по защите информации локально на компьютерах пользователей.

Работа в VPN

Сервер системы ADVANTA может быть установлен внутри сети компании (например, в локальной сети офиса). При этом пользователи удаленных сетей (локальные сети в офисах других городов) могут совершенно прозрачно обращаться к серверу через VPN (Virtual Private Network) по адресу (IP или имени), указанному администратором.

Мониторинг пользователей

Список событий в Системе

Все существующие типы событий по действиям пользователей в конкретном экземпляре

системы расположены на странице `https://адрес_приложения/api/businessevents`.

Список событий может быть выгружен в json-файл.

Системный протокол

Системный протокол — важная часть безопасности системы.

В системном протоколе отражаются события, которые:

- возникают в результате действий администратора, в том числе изменения прав доступа;
- возникают в результате действий пользователей в процессе работы;
- выполняются в системе автоматически.

Список отображаемых действий пользователей:

- скачивание, добавление, обновление и удаление документов (в том числе скачивание выгруженных в виде файлов отчетов);
- создание, удаление директорий;
- действие с проектами: создание, удаление, выполнение, просроченные проекты и т.п.;
- действия с дискуссиями;
- действия с записями справочников.

Список можно отфильтровать:

- по типу события,
- по временному интервалу,
- по пользователю, который инициировал событие.

Как найти: Администрирование → Управление безопасностью → Системный протокол.

События системного протокола можно выгрузить в *.xls.

Подробнее - по ссылке.

Лог авторизаций

Лог авторизаций в системе доступен по следующему пути: Администрирование → Управление безопасностью → Безопасность, портлет «Лог авторизаций».

В этот лог записываются следующие данные: время авторизации в формате ДД.ММ.ГГГГ ЧЧ:ММ:СС; имя пользователя в Системе; IP адрес.

Также в системе записываются неудачные попытки авторизации.

Отчёт по правам пользователей

Вы можете посмотреть, к каким объектам системы у конкретного пользователя есть доступ. Отчет доступен только администратору.

Отчет можно выгрузить в MS Excel.
Как найти: зайдите на карточку пользователя → меню три точки → «Права пользователя».

Подробнее - по ссылке.

Отчет по правам пользователей на уровне объектов

Вы можете увидеть, у каких пользователей какие права есть по конкретным объектам системы, воспользуйтесь отчетом по правам объекта.
Отчет возможно просмотреть в разрезе операций прав доступа для проектных и системных ролей и отдельно в разрезе каждой роли получить список пользователей в привязке к иерархической структуре проекта.
Как найти: зайдите в объект, доступ к которому вы хотите проверить → меню “три точки” → «Права доступа» → в портлете «Роли безопасности проекта» → «отчёт по правам».

Подробнее - по ссылке.

События электронной почты

В системе можно просматривать события электронной почты в разделе Администрирование → Управление безопасностью → Электронная почта.
В этом разделе возможно посмотреть системные сообщения электронной почты. Доступно следующее отображение сообщений: отправленные, неотправленные, полученные.

Также доступная фильтрация сообщений по количеству отображаемых сообщений и выбор временного периода и количества для отображения сообщений на странице.

В портлете «Ошибки при отправке сообщений» также доступна фильтрация по временному периоду и пользователям. Фильтрация становится доступна при появлении соответствующих событий.

Обслуживание системы

Создание резервной копии данных системы

В части управления бэкапами рекомендуем обязательно настроить регулярные автоматические бэкапы системы. Кроме того, рекомендуем с определенной частотой дублировать бэкапы на другом физическом носителе (сервере).

Для того чтобы сделать резервную копию системы на определенный момент времени, нужно создать резервные копии:

1. Базы данных streamline (подробнее см. справка Microsoft, подраздел «Как создать резервную копию базы данных (среда SQL Server Management Studio)», ссылка на статью).
2. Документов системы (путём копирования папки с документами системы, например, на внешний носитель и или сетевой каталог для хранения резервных копий.

Путь до папки указывается в разделе <constructor>, имя параметра documentsFolder, в файле client.config, расположенном в папке веб-контента системы).

3. Веб-контента системы (путём копирования папки C:\Inetpub\wwwroot\streamline, например, на внешний носитель и или сетевой каталог для хранения резервных копий).

Тестовая среда

В части управления обновлениями и настройками рекомендуем иметь на предприятии тестовый контур, на котором производить проверку предполагаемых изменений настроек, а также делать внутреннее тестирование получаемых обновлений.
Данная практика рекомендуется нами для систем с большим числом пользователей, сложными настройками, а также там, где остановка системы даже на короткий период имеет критическое значение.