

ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ»

СИСТЕМА РЕДАКТИРОВАНИЯ И СОВМЕСТНОЙ РАБОТЫ (СО)

СИСТЕМА ХРАНЕНИЯ ДАННЫХ (PGS)

3.3

РУКОВОДСТВО ПО НАСТРОЙКЕ

ИНТЕГРАЦИИ С DLP

Версия 1

На 13 листах

Дата публикации: 18.03.2025

**Москва
2025**

Все упомянутые в этом документе названия продуктов, логотипы, торговые марки и товарные знаки принадлежат их владельцам.

Товарные знаки «МойОфис», «MyOffice» и «Squadus» принадлежат ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ».

Ни при каких обстоятельствах нельзя истолковывать любое содержимое настоящего документа как прямое или косвенное предоставление лицензии или права на использование товарных знаков, логотипов или знаков обслуживания, приведенных в нем. Любое несанкционированное использование этих товарных знаков, логотипов или знаков обслуживания без письменного разрешения их правообладателя строго запрещено.

СОДЕРЖАНИЕ

1 Общие сведения	5
1.1 Назначение	5
1.2 О компонентах продукта	5
2 Особенности интеграции	6
2.1 Архитектурная схема	6
2.2 Совместимые DLP-системы	7
3 Порядок сбора и передачи данных	8
4 Установка и настройка DPS-сервиса	10
4.1 Установка сервиса DPS	10
4.2 Настройки сервиса DPS в ETCD	10
5 Установка и настройка Searchinform	13

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ, ТЕРМИНОВ И ОПРЕДЕЛЕНИЙ

В настоящем документе применяют следующие сокращения с соответствующими расшифровками (табл. 1).

Таблица 1— Сокращения и обозначения

Сокращение, термин	Расшифровка и определение
API	Application Programming Interface, интерфейс программирования приложений
CA	Certificate Authority, удостоверяющий центр для подтверждения подлинности ключей шифрования
CO	Система редактирования и совместной работы
DNS	Domain Name System, система доменных имен
ETCD	Распределенная система хранения конфигурации
FQDN	Fully Qualified Domain Name, полностью определенное имя домена
Inventory	Файл для настройки Ansible с перечислением ролей и их IP-адресов
PGS	Система хранения данных
URL	Uniform Resource Locator, единый указатель ресурса
ОС	Операционная система
ПК	Персональный компьютер
ПО	Программное обеспечение
Маппинг	Определение соответствия между различными моделями данных

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Назначение

Настоящая инструкция описывает интеграцию Системы редактирования и совместной работы и Системы хранения данных с внешней DLP-системой.

Интеграция с DLP-системой позволяет сформировать список клиентских действий и провести их анализ. Список клиентских действий, на основе которых формируется сообщение:

- Скачивание файла/экспорт;
- Отправка файла по почте (размер файла ограничен 50мб);
- Изменение прав доступа к файлу (при удалении доступа к файлу события не передаются);
- Создание публичной ссылки для файла;
- Перемещение файла.

Формирование списка предназначено только для файлов офисных форматов: *.docx, *.xlsx, *.pptx, *.odt, *.ods, *.odp, *.xodt, *.xott, *.xods, *.xots, *.xodp, *.xotp.

1.2 О компонентах продукта

Система хранения данных — компонент, предназначенный для безопасного хранения корпоративных файлов и обеспечения возможностей авторизации, аутентификации и разграничения прав доступа пользователей.

Система редактирования и совместной работы — компонент, предназначенный для индивидуального и совместного редактирования текстовых и табличных документов, а также просмотра и демонстрации презентаций.

Представленные компоненты входят в состав следующих продуктов:

- «МойОфис Документы Онлайн»;
- «МойОфис Профессиональный 2»;
- «МойОфис Профессиональный 3»;
- «МойОфис Схема»;
- Squadus PRO.

Подробное описание возможностей продукта приведено в документе «Функциональные возможности».

2 ОСОБЕННОСТИ ИНТЕГРАЦИИ

2.1 Архитектурная схема

Архитектурная схема взаимосвязи Системы хранения данных, Системы редактирования и совместной работы и DLP-системы показана на рисунке 1.

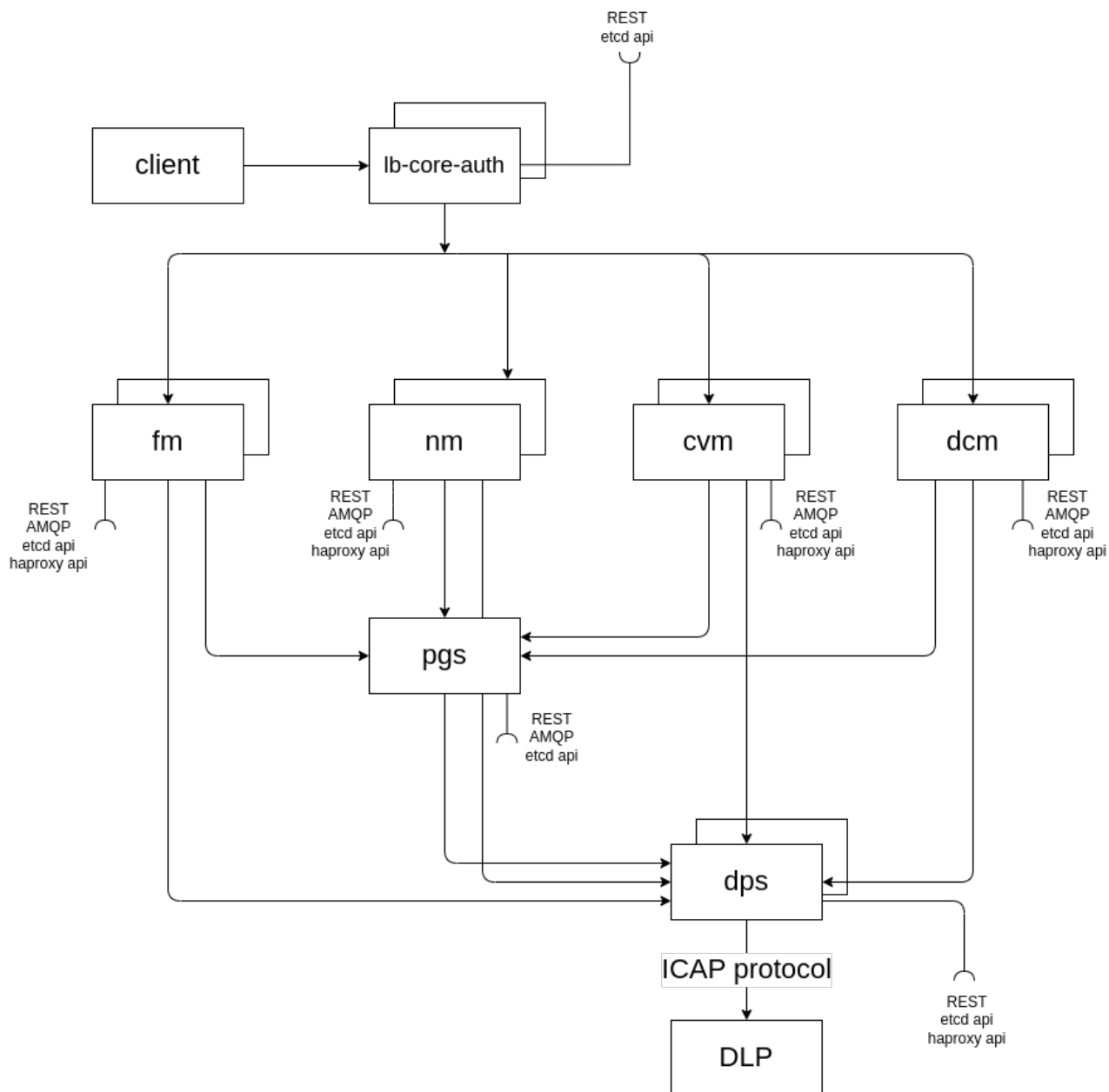


Рисунок 1 — Архитектурная схема интеграции с DLP

Таблица 2 — Описание подсистем и сервисов

Наименование компонента	Наименование сервиса	Описание
Система редактирования и совместной работы	Lb-core-auth (nginx-wfe)	Расширенный веб-сервер NGINX с поддержкой Lua. Отвечает за авторизацию, доступность API, балансировку
	CVM	Conversion Manager, сервис управления конвертированием файлов. При конвертации документов использует пул CU юнитов или Jod
	FM	File Manager, сервис файлового менеджера. Отвечает за создание, удаление, добавление файлов, предоставление доступа другим пользователям
	NM	Notification Manager, сервис управления уведомлениями
	DCM	Document Collaboration Manager, сервис управления редактированием документов. При редактировании документов использует пул DU юнитов
	DPS	Data Protection Service, сервис сбора и передачи событий в DLP-систему
	DLP	Data Loss Prevention, внешняя система защиты от потери данных
Система хранения данных	PGS	Включает в себя различные сервисы для хранения данных

2.2 Совместимые DLP-системы

Для отправки сообщений в DLP систему интеграционный сервис DPS использует протокол ICAP и поддерживает два режима работы (REQMOD и RESPMOD).

Поддержана совместимость со следующими DLP-системами:

- Searchinform. Подробное описание системы представлено на сайте <https://searchinform.ru/>

3 ПОРЯДОК СБОРА И ПЕРЕДАЧИ ДАННЫХ

Клиентские запросы инициализируют отправку сообщений в DLP-систему. Сообщения формируются в сервисах FM, NM, CVM, DCM, PGS и по REST протоколу передаются асинхронно в сервис DPS (data protection service). Все сервисы имеют единую точку обработки и отправки сообщений - исходя из данных клиентского запроса, заполняется содержимое.

Описание основных полей представлено в таблицах 3 и 4.

Таблица 3 — Обязательные запросы

Имя поля	Пример заполнения	Описание поля
X-Co-File-Name	res.xlsm	Имя и формат файла
X-Co-File-Type	application/vnd.ms-excel.sheet.macroenabled.12	Медиатип файла
X-Co-User-Name	admin@<domain_name>	Имя пользователя, выполняющего операцию
X-Co-Request-Id	41f3af16f0594854a8a854b39f4c102e	ID операции

Таблица 4 — Необязательные запросы

Имя поля	Описание поля
X-Co-Client-Host-Name	Имя хоста пользователя
X-Co-Client-Ip	IP адрес хоста пользователя
X-Co-Request-Method	HTTP метод в запросе от пользователя (для внутреннего использования)
X-Co-Request-Uri-Host	Uri-Host запрашиваемый пользователем (для внутреннего использования)
X-Co-Request-Uri-Path	Uri-Path запрашиваемый пользователем (для внутреннего использования)

Пример запроса:

```
RESPMOD icap://172.17.0.1:1344/echo ICAP/1.0
Allow: 204 # режим нотификации при обработке
запроса
Host: 29c14c5a57a3 # адрес клиентского узла (обязательный
параметр)
X-Co-File-Name: res.xlsm
X-Co-File-Type: application/vnd.ms-excel.sheet.macroenabled.12
X-Co-User-Name: comar@srv.tacos.devoffice.ru
X-Co-Request-Id: 41f3af16f0594854a8a854b39f4c102e
Encapsulated: res-hdr=0, res-body=96 # список смещений в байтах
(обязательный параметр)

HTTP/1.1 200 OK

Content-Length: 12893

Content-Disposition: attachment; filename="res.xlsm"

PK.....!k..^[Content_Types].xml ...(T.N.O..#....(v...j...#
.....c[^S...g..
P....'.wfv.q.8o\1.D6.J...(..`..T.....e...\X.....NO./
..Tp..J.9.k.H.....8..2.....0Au..]*|F...b.A.....rq7..K%#.Eq.\.RU
.btVCf.j..l.....(g#xJ.
u.j#XBG{.~J.Wr%Wv.T.Hg....vf..U.#.....
R~...Rs.>B..B... ..q..I...l@.p.a.....`.*Iu...
(.....J. .t`.m'..... ..y...f.!...C:r.K.}.5$4.9q.....;....]..H....w.
+.mu...S.....f...l;...A..
.O.E..w....E$I..'....v..fR3S....q....?|.>....9$...jPH]..]-.O.....Z.
\.fQeKla...Zs7`\.. $......y..{..
%.zS...>....$.P3.....o.....c6Z..o.....PK.....!u>.i.....x
l/theme/themel.xml.Y[.F.~/?.?..;..I....l.N..&!...q1....4F3.. ..<..PHK_

ICAP/1.0 204 No modifications needed
Date: Tue, 21 Jan 2025 15:13:35 GMT
Encapsulated: null-body=0
ISTag: epoch-1737472415
Service: echo service
X-ICAP-Metadata: lp4buhitjwdf43hojlhr
X-ICAPeg-Shadow-Service: false
```

4 УСТАНОВКА И НАСТРОЙКА DPS-СЕРВИСА

4.1 Установка сервиса DPS

DPS сервис устанавливается в составе компонента Система редактирования и совместной работы и служит для формирования списка клиентских запросов и отправки в DLP-систему.

Для установки сервиса необходимо открыть с помощью текстового редактора файл `extra_vars.yml` и добавить переменные, представленные в таблице 5.

Таблица 5— Переменные сервиса DPS

Наименование переменной	Тип переменной	Описание переменной
<code>common_dps_enabled</code>	boolean	Установка сервиса DPS при запуске или обновлении продукта
<code>dps_icap_server_address</code>	string	IP-адрес или DNS-имя внешнего сервера

Переменную возможно задать при запуске установки продукта, без использования файла `extra_vars`. Пример команды настройки функции:

```
ansible-playbook playbooks/main.yml \
-e common_dps_enabled = true -e dps_icap_server_address = 11.111.111.111
```

При установке сервиса после развертывания продукта необходимо запустить установку для тегов `co_common`, `dps`, `confd`, `haproxy`

4.2 Настройки сервиса DPS в ETCD

Для настройки DPS-сервиса с помощью ETCD необходимо открыть ветку `nct/co/config/dps`

Основные переменные для настройки DPS-сервиса представлены в таблице 6.

Таблица 6 — Основные переменные для настройки DPS-сервиса

Наименование переменной	Тип переменной	Значение по умолчанию	Описание переменной
<code>Icap.Mode</code>	string	REQMOD	Режим работы отправки сообщений в DLP систему по протоколу ICAP (принимает значения REQMOD и RESPMOD)

Наименование переменной	Тип переменной	Значение по умолчанию	Описание переменной
Icap.Client.Timeout	integer	50s	Таймаут в секундах, который будет использоваться по умолчанию, если различные серверные таймауты (см. ниже) не выставлены
Icap.Server.Address	string	"{{ docker_bridge_ip default('172.17.0.1') }}"	IP адрес/FQDN сервера ICAP
Icap.Server.Port	integer	1344	Порт ICAP сервера
Icap.Server.ReadTimeout	string	50s	Таймаут в секундах на чтение данных, принимаемых от сервера ICAP
Icap.Server.Scheme	string	"icap"	Схема протокола ICAP Принимает значения icap или icaps
Icap.Server.Service	string	"icap"	Сервис ICAP (зависит от DLP системы), используется по аналогии с Uri Path
Icap.Server.WriteTimeout	string	50s	Таймаут в секундах на запись данных, отправляемых серверу ICAP
Icap.Vendor.Name	string	searchinform	Наименование поставщика DLP системы.

Переменные возможно задать перед установкой сервиса DPS. Для этого необходимо открыть с помощью текстового редактора файл `extra_vars.yaml` и добавить переменные из таблицы. Следует обратить внимание, что переменные при использовании с `ansible` незначительно отличаются по формату имени. Пример:

```
dps_icap_client_timeout: "50s"
dps_icap_mode: "REQMOD"
dps_icap_server_address: "{{ docker_bridge_ip | default('172.17.0.1') }}"
dps_icap_server_port: 1344
dps_icap_server_read_timeout: "50s"
dps_icap_server_scheme: "icap"
dps_icap_server_service: "icap"
dps_icap_server_write_timeout: "50s"
dps_icap.vendor.name: "searchinform"
```

5 УСТАНОВКА И НАСТРОЙКА SEARCHINFORM

Установка выполняется в соответствии с документацией Searchinform, представленной на сайте <https://docs.searchinform.ru/>

Перед началом работы с DLP-системой следует обратиться к вендору для создания правил политики безопасности, исходя из информации, передаваемой в событиях.