



SecretTechnologies

Защищенный корпоративный
файловый сервис

Secret Cloud Enterprise



Содержание

● <u>О компании Secret Technologies</u>	<u>3</u>
● <u>Защищенный корпоративный файловый сервис Secret Cloud Enterprise</u>	<u>7</u>
● <u>Возможности Secret Cloud Enterprise</u>	<u>15</u>
● <u>Secret Cloud Enterprise в ИТ-инфраструктуре</u>	<u>26</u>
● <u>Secret Cloud Enterprise для защиты КИИ</u>	<u>29</u>
● <u>Дополнительные функции Secret Cloud Enterprise</u>	<u>33</u>
● <u>Совместимость с другими программными решениями и минимальные технические требования</u>	<u>37</u>
● <u>СМИ о нас</u>	<u>41</u>



семейство продуктов*

Secret Cloud

безопасный файловый обмен
с сотрудниками и партнерами.
SCE сертифицирован ФСТЭК РФ
по 4 уровню доверия



DataMask

обезличивание чувствительных
данных

с 2016 года

на рынке ИБ



Trace Doc

создание уникальных копий
документов



VideoAnalyzer

система автоматизированного
анализа видео- и аудиоархивов

> 100 тысяч

пользователей продуктов



Screen Guard

защита экрана монитора от
фотографирования



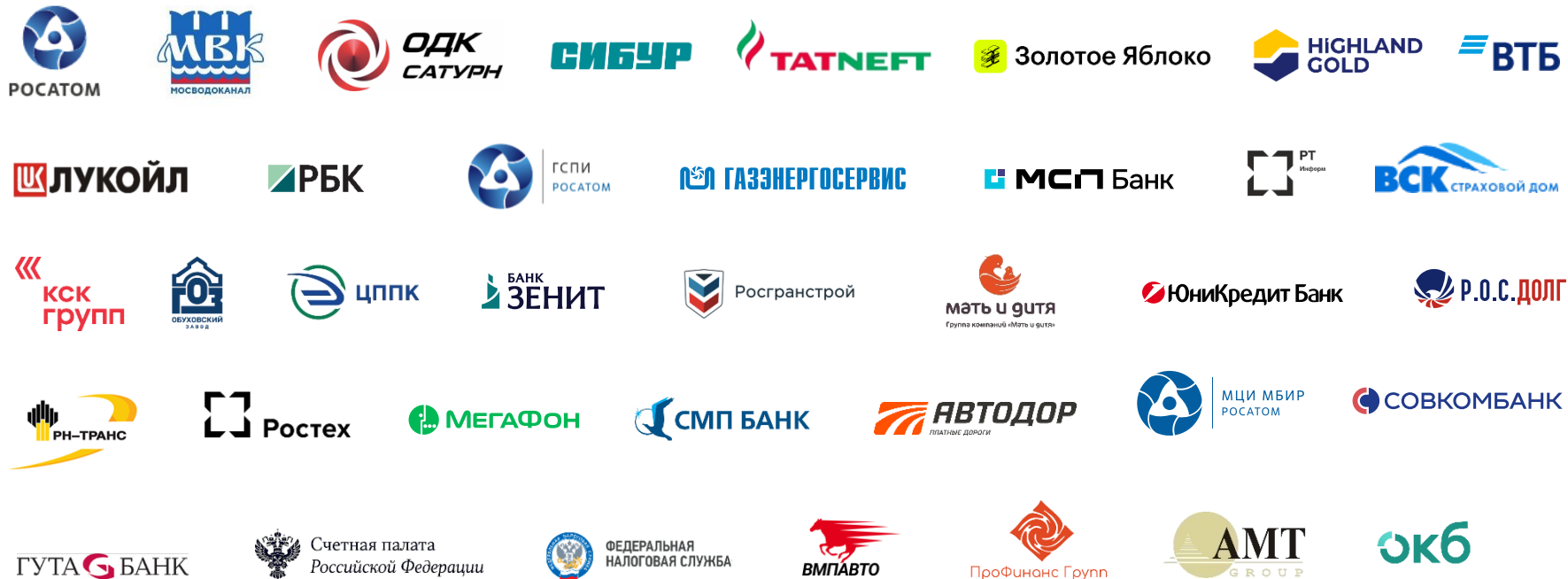
Printer Guard

контроль и экономия печати

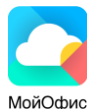
8 продуктов

в собственном портфеле решений

Наши клиенты



Наши партнеры



Цифры и факты



около **75%**

офисных сотрудников используют небезопасные способы обмена файлами

до **20%**

рабочего времени сотрудники могут тратить на поиск нужной документации, если у них нет доступа к эффективным системам.



Передача больших файлов через эл. почту замедляет работу почтового сервиса и перегружает почтовые ящики.

≈ **5,5** млн руб.

крупный бизнес и государственный сегмент теряют от одной утечки данных.

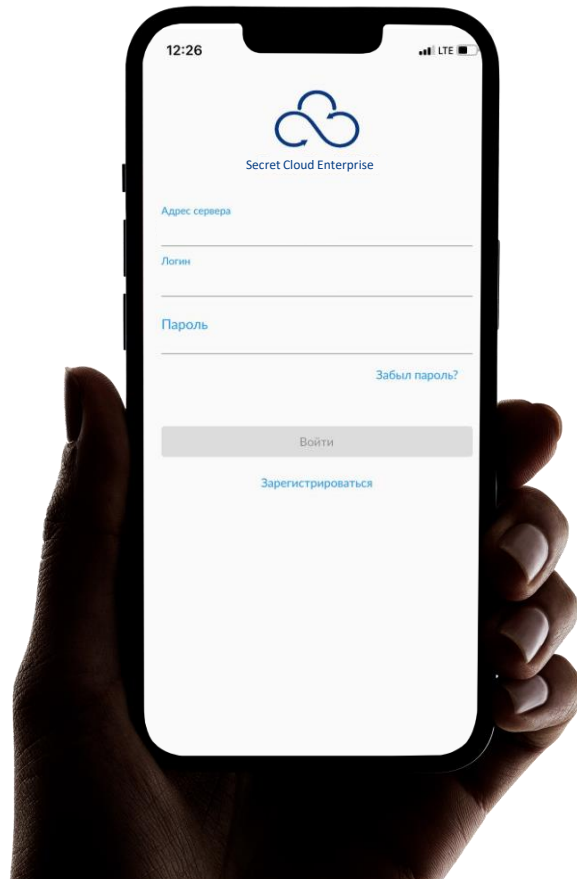


Штрафы за несоблюдение защиты персональных данных, игнорирование инцидентов и нанесенный ущерб пользователям.

О решении

Secret Cloud Enterprise (SCE) - это комплексное решение для эффективной совместной работы и управления файлами, которое сочетает в себе простоту использования, быстрое внедрение и высокий уровень безопасности.

SCE позволяет компаниям оптимизировать рабочие процессы, повысить продуктивность команды и обеспечить надежную защиту данных, предоставляя все необходимые инструменты в одном удобном интерфейсе.



Защищенный корпоративный файловый сервис SCE

Решение, обеспечивающее максимальное удобство совместной работы:

Понятный интерфейс и расширенные возможности для совместного редактирования документов в реальном времени.

Универсальная замена популярных файлообменников, FTP-серверов и облачных хранилищ, предоставляющая единую платформу для всех потребностей в управлении документами и совместной работы.

Удобный доступ к файлам с любого устройства, обеспечивающий гибкость и мобильность в работе. Минимальное время обучения для начала работы.



Защищенный корпоративный файловый сервис SCE

Надежная защита данных и соответствие требованиям



Сертификация ФСТЭК 4 уровня доверия.



Соответствие требованиям законодательства в области защиты критической информационной инфраструктуры (КИИ).



Мандатная модель разграничения доступа и двухконтурная система обмена файлами минимизируют риски утечек данных.



Защищенный корпоративный файловый сервис SCE

**Быстрое внедрение и эффективное
импортозамещение**



Легкая интеграция в существующую ИТ-инфраструктуру.



Поддержка распространенных редакторов файлов, российских СУБД и ОС.



Полностью отечественная разработка, в том числе соответствующая регуляторным требованиям защиты КИИ.



Возможности SCE

Обмен и хранение файлов



Создание удобной структуры хранения папок и файлов.



Обмен файлами с внешними контрагентами.



Мониторинг всех операций с файлами (изменение, скачивание, просмотр)



Загрузка файлов любого размера (с учетом особенностей инфраструктуры компании).



Доступ с мобильных устройств с помощью приложений на базе Android и IOS.



Работа с системой через десктопное приложение или веб-браузер



Подключение личного раздела "Мои файлы" как отдельного сетевого диска через протокол WebDav.



Доступ к файлам и папкам с возможностью ограничения количества скачиваний и срока действия ссылки.

Возможности SCE



Совместная работа с документами



Совместное онлайн-редактирование документов.



Отображение изменений для всех участников редактирования в реальном времени.



Максимальная совместимость с docx, xlsx, pptx и поддержка других популярных форматов



Сохранение версионности файлов с возможностью восстановить или скачать предыдущие версии.



Предпросмотр содержимого файлов различных форматов (электронные таблицы, текстовые документы, презентации, изображения, аудио и видео).



Возможность автоматической замены крупных вложений на защищенные ссылки при отправке файлов через электронную почту и корпоративные мессенджеры.

Возможности SCE

Защита данных



Мандатный доступ, реализованный с помощью назначения меток безопасности файлам, пользователям и группам пользователей.



Возможность организации двухконтурной системы обмена файлами.



Блокирование передачи файлов с вредоносным кодом.



Интеграция с различными СЗИ: антивирусы, SIEM, DLP, DAG/DCAP, Sandbox, PAM, WAF и т.д.



Возможность интеграции с решениями, уже развёрнутыми в инфраструктуре организации.



Сквозная аутентификация пользователей (SSO) через Keycloak.



Настройка автоматической блокировки пользователей после заданного периода неактивности.



Разные права доступа в зависимости от точки подключения.

Возможности SCE

Защита данных



Настройка водяных знаков для режима предпросмотра документа.



Установка ограничения доступа к системе SCE и запретов на действия для администраторов, пользователей и контрагентов, а также для третьих лиц, получающих доступ к системе посредством публичной ссылки.



Просмотр и изменение параметров хранилища файлов (резерв хранилища, добавление администраторов).



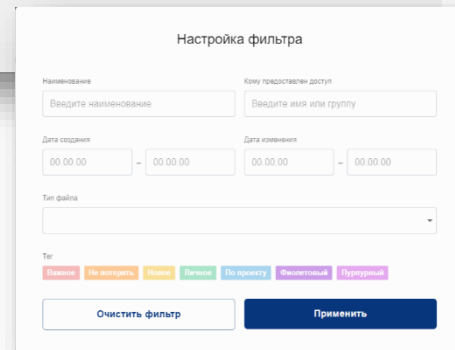
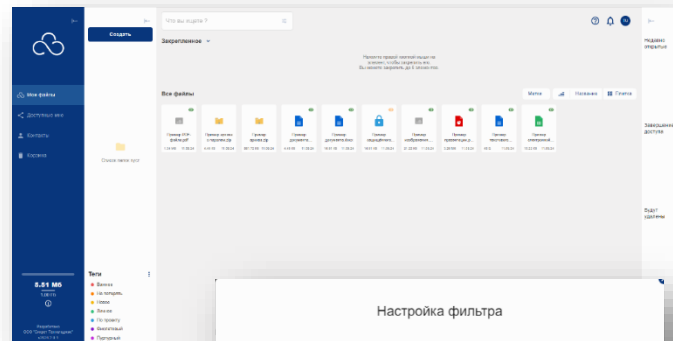
Возможность разделения пользователей и администраторов по отдельным предприятиям в рамках одной инсталляции позволяет эффективно разграничивать данные и настройки для каждого из них.



Возможности Secret Cloud Enterprise

Структура хранения файлов и папок

Secret Cloud Enterprise предоставляет пользователям возможность создавать собственную структуру файлов и папок, обеспечивая удобное и интуитивно понятное управление данными.



Пользователи могут создавать новые папки и загружать файлы с ПК через функцию перетаскивания (drag-and-drop), просто перемещая элементы в окно программы.

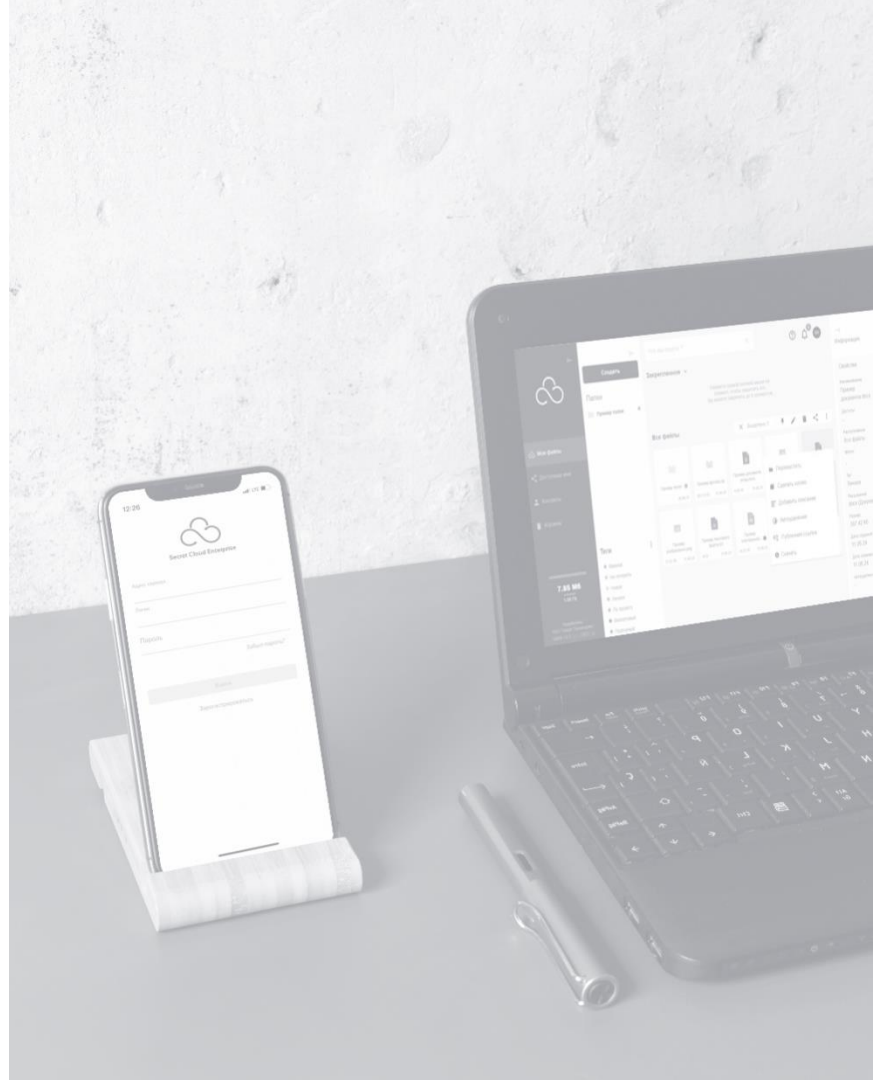
Файлам и папкам можно присваивать теги для удобной категоризации. Часто используемые файлы и папки можно закреплять на панели быстрого доступа для мгновенного доступа.



Пользователи могут создавать новые папки. Доступны различные способы сортировки файлов: по типу, дате создания, названию, размеру. Также предусмотрена фильтрация по различным параметрам: по степени конфиденциальности документа, тегам, названию, типу файла, что позволяет быстро находить нужные файлы.

Мультиплатформенный доступ

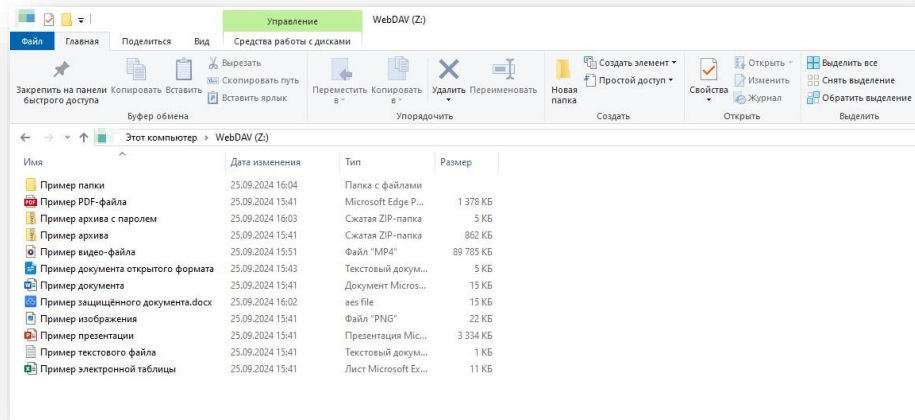
Доступ в Secret Cloud Enterprise возможен через десктопное приложение или веб-браузер, и также с мобильных устройств с помощью приложений на базе Android и IOS.



Подключение через WebDav

С помощью протокола WebDav можно подключить раздел «Мои файлы» пользователя как отдельный сетевой диск.

Это позволяет работать с файлами в интерфейсе проводника, при этом файлы синхронизируются в Secret Cloud Enterprise.



Предпросмотр документов

Администраторы могут разрешать или запрещать предпросмотр различных типов файлов (Word, Excel, PDF, изображения и другие), обеспечивая гибкость в управлении доступом к документам.

Настройка водяных знаков также осуществляется через интерфейс системы. Можно изменять текст, цвет, размер шрифта, положение и прозрачность водяных знаков. Водяные знаки могут применяться ко всем файлам или только к файлам с определенными метками. Дополнительно можно включить отображение даты, имени пользователя, IP-адреса и ссылки на систему SCE в текст водяного знака.



Secret Technologies
we keep your secrets safe

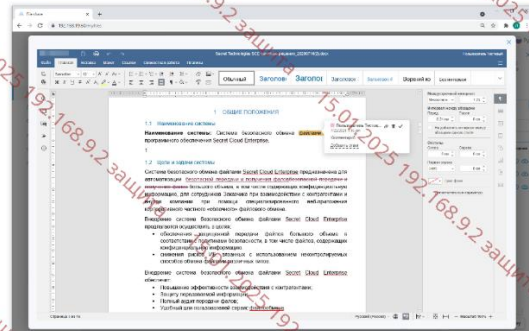
Совместная работа с документами в Secret Cloud Enterprise через веб-браузер

Secret Cloud Enterprise – корпоративное решение для обеспечения безопасного файлового обмена и совместной работы.

В веб-интерфейсе Secret Cloud Enterprise реализована интеграция редактора, который позволяет обеспечивать работу с документом.

Редактирование производится аналогично сервису Google Документы.

Редактирование текстового документа:



Пользователи могут одновременно бесконфликтно редактировать документы прямо через веб-интерфейс.

Все изменения отображаются в реальном времени и видны всем участникам редактирования.

Поддерживается максимальная совместимость с docx, xlsx, pptx + поддержка других популярных форматов.

При изменении и сохранении документа сохраняется ее новая версия. Пользователь может восстановить или скачать предыдущие версии.

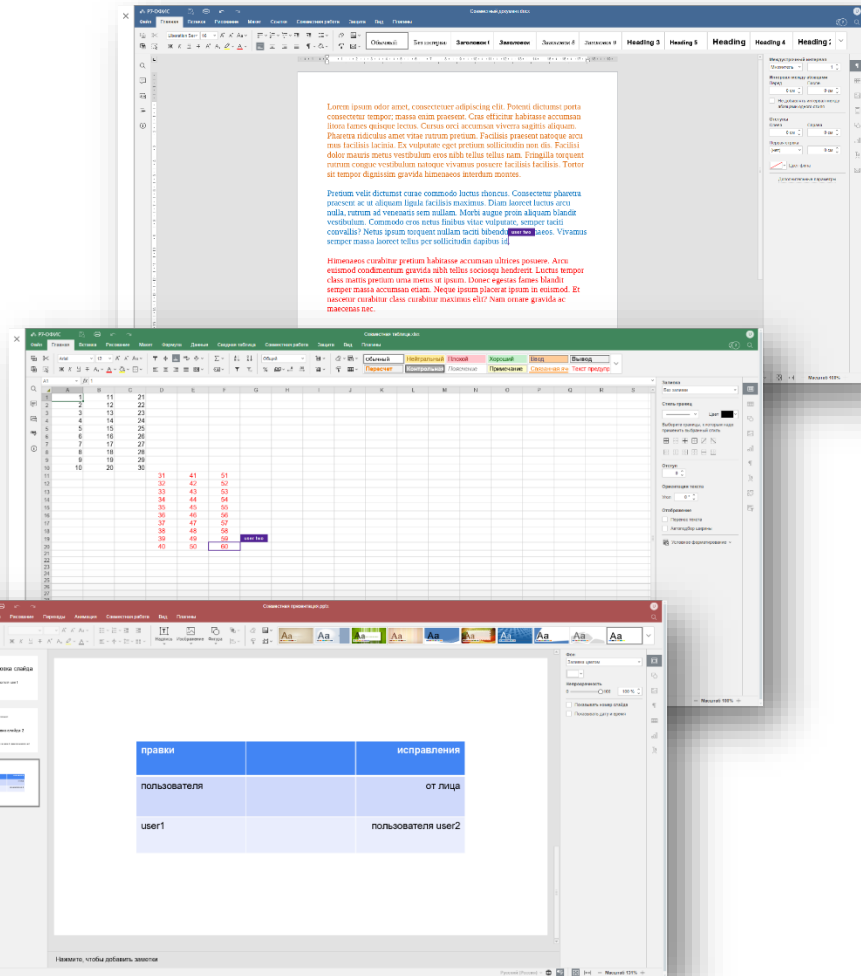
Совместное редактирование файлов

Пользователи могут одновременно бесконфликтно редактировать документы прямо через веб-интерфейс.

Все изменения отображаются в реальном времени и видны всем участникам редактирования.

Максимальная совместимость с docx, xlsx, pptx и поддержка других популярных форматов.

При изменении и сохранении документа сохраняется ее новая версия. Пользователь может восстановить или скачать предыдущие версии.



Обмен с контрагентами

В Secret Cloud Enterprise возможно настроить взаимодействие с контрагентами: ограничение количества скачиваний по ссылке, установка длительности доступа к файлу и выбор способа авторизации для получения и передачи документов.

Дополнительная лицензия для контрагентов, необходимая для работы в системе, не требуется.

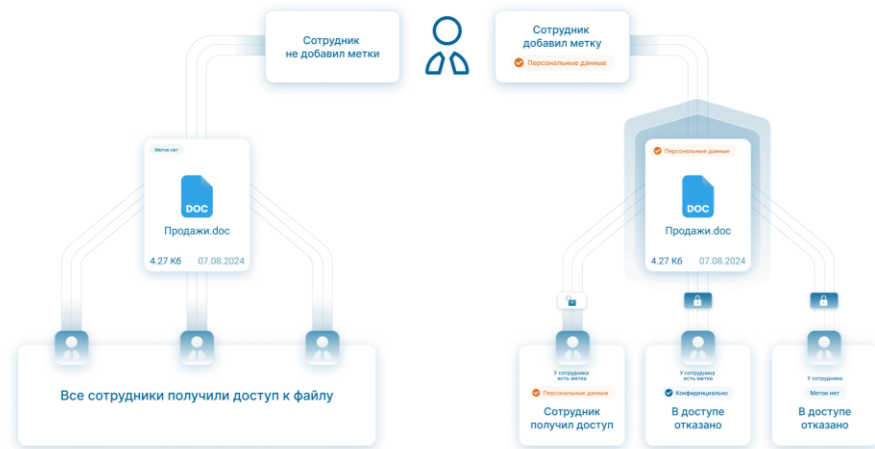
The image shows a composite of three screenshots from the Secret Cloud Enterprise web interface. The top screenshot displays the 'Контрагенты' (Counterparties) management page, featuring a search bar, a 'Добавить' (Add) button, and a table of existing counterparties. The middle screenshot shows the 'Добавление контрагента' (Add counterparty) form, which includes fields for email, name, surname, organization, position, and phone number. The bottom screenshot shows the 'Создать запрос' (Create request) dialog, which prompts for the counterparty's email, a comment, the number of file downloads, and the authentication method (selected as 'Через интерфейс с аутентификацией').

Мандатное управление доступом

Мандатное управление доступом позволяет разграничивать права доступа к документам, пользователям и группам пользователей с помощью меток безопасности.

Метки безопасности - это система организации файлов по категориям в зависимости от их важности и секретности.

Пользователь может работать с документом только при совпадении меток безопасности его учетной записи и документа.



Мандатное управление доступом

По умолчанию доступны метки безопасности для документов:

- Общего назначения – для всех пользователей.
- Конфиденциально – для ограниченной группы пользователей.
- Строго конфиденциально – только для определенных пользователей по разрешению.

При необходимости изменения метки безопасности пользователь может обратиться к администратору.



Управление метками

Логин: [] Логи запросов Предзаданные метки

Новая метка

Название метки*

Описание метки

Обособленное отображение ☐

Режим простановки метки* Автоматическое назначение по установленным правилам

Режим работы метки* Принудительная установка метки файлу

Значение веса для автоматической классификации*

Регулярные выражения для классификации метки* +

Регулярное выражение	Вес выражения	
<code>{.*}(K k)ommerchesk[a-я]+ тайн[a-я]+{.*}</code>	100	

Отмена Сохранить

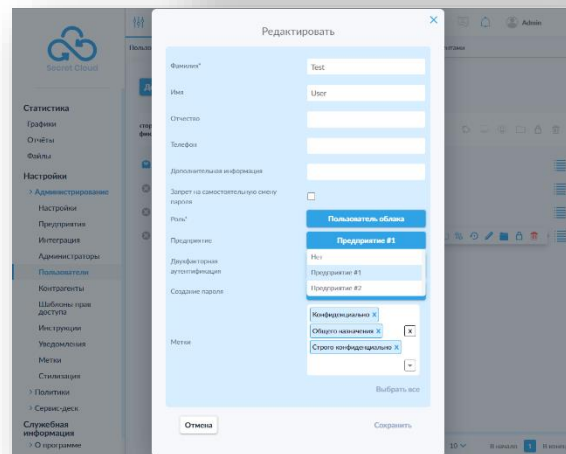
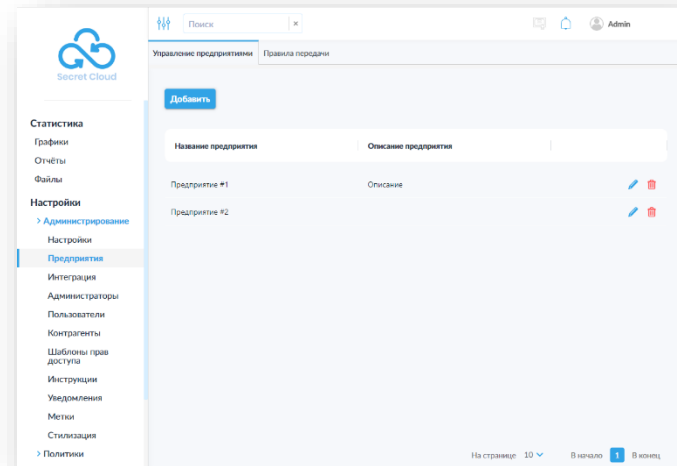
Управление предприятиями

Функция обеспечивает мультитенантность, позволяя эффективно обслуживать множество клиентов в рамках одной инсталляции. Подходит для холдингов, организаций с несколькими филиалами и сервис-провайдеров.

Система сегментирует пользователей и администраторов по предприятиям, регулируя доступ к информации и её обмен между ними.

Администраторы предприятий управляют запросами своих сотрудников, сохраняя автономность, и устанавливают правила обмена данными с учетом конфиденциальности.

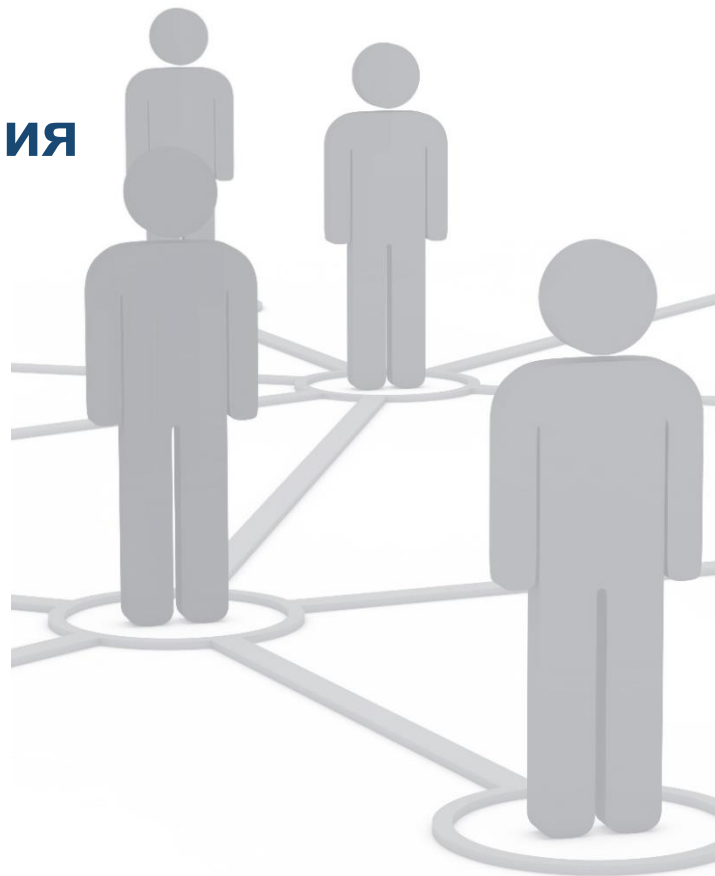
Это обеспечивает безопасное взаимодействие и точный контроль доступа, поддерживая баланс между централизованным управлением и автономностью отдельных предприятий.



Разграничение прав доступа в зависимости от точки подключения

В системе возможно установить ограничение подключения по подсети или IP-адресу для снижения риска компрометации данных компании в случае предоставления доступа из недоверенных сетей.

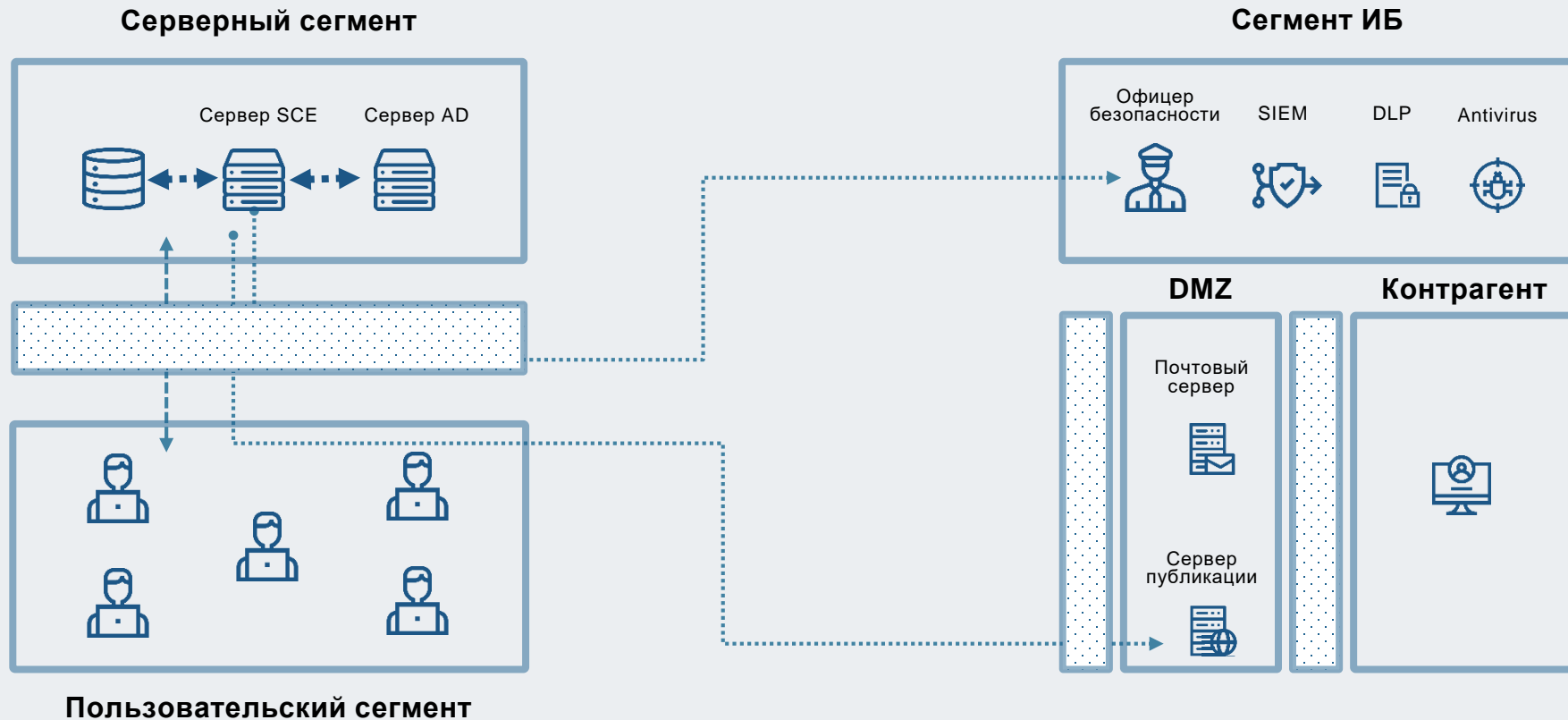
Создание «белых» и «черных» списков подмену позволяет работать с доверенными (разрешенными) контрагентами и установить запрет доступа подключения доменов с высоким потенциалом взлома из-за своей доступности в систему.





Secret Cloud Enterprise в ИТ-инфраструктуре

Как работает SCE



Интеграция SCE в инфраструктуру организации





Secret Cloud Enterprise для защиты КИИ

Secret Cloud Enterprise для КИИ

SCE помогает соблюдать требования Федерального закона №187 «О безопасности критической информационной инфраструктуры Российской Федерации», обеспечивая защищённый обмен данными с разработчиками программных средств компонентов КИИ благодаря своим функциональным возможностям.

Сертифицированные ФСТЭК России механизмы безопасности при передаче данных объекта КИИ и между сетевыми контурами.

Верификация со стороны администратора при передаче файлов и предоставления доступа к ним, а также добавление внешних пользователей или контрагентов.

Настройка списка разрешённых / запрещённых доменов.

Запрет на инициативную связь с сервером закрытого контура.

Соответствие мерам безопасности, обозначенным в приказе ФСТЭК России № 239.

Обмен между контурами безопасности

Внешний «открытый» контур безопасности

Передача данных из внешнего контура во внутренний



Автоматическая проверка на допустимость передачи определенных политиками безопасности типов файлов



Антивирусная проверка для входящих файлов (в том числе и путем использования технологии sandbox)

Внешний «открытый» контур безопасности

Передача данных из внутреннего контура во внешний

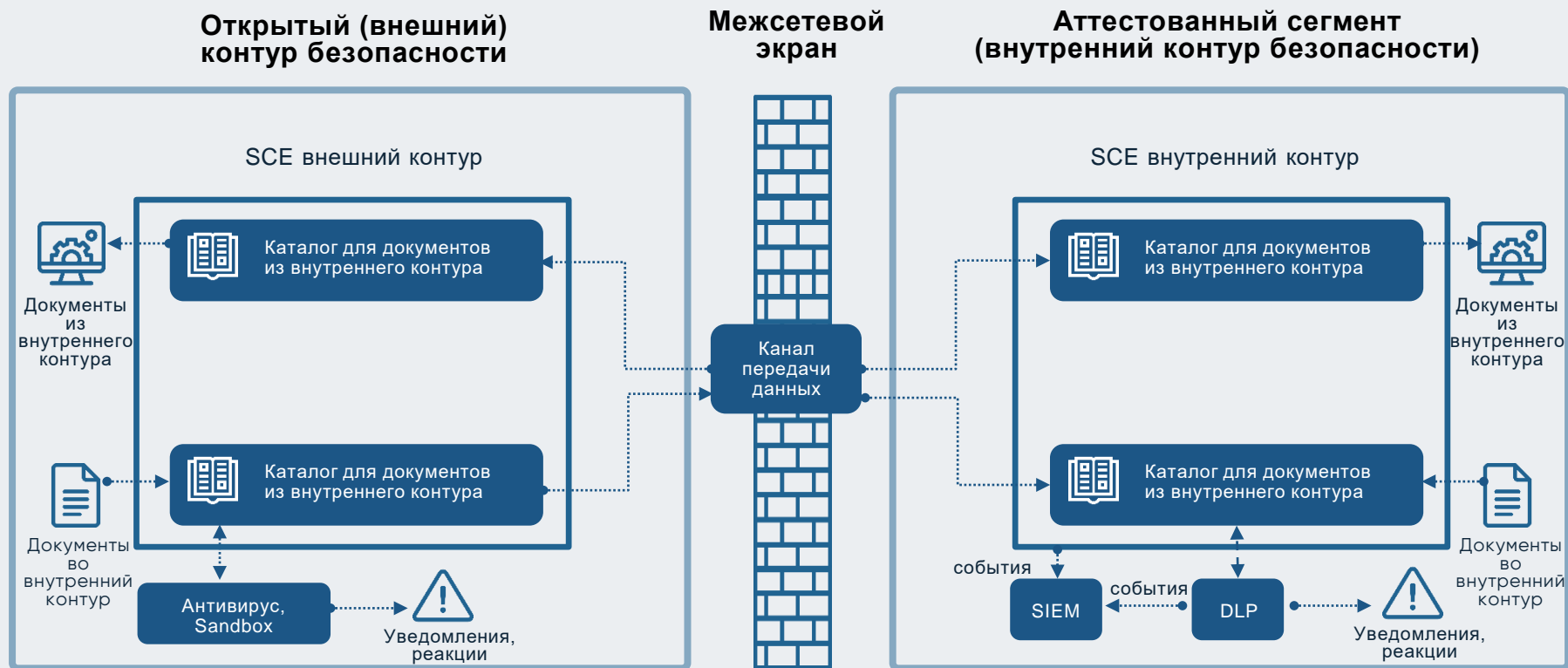


Верификация Отдела ИБ (осуществляемой как вручную, так и с использованием системы контроля за утечками информации (DLP-системы))



Запись в журнал событий всех действий и событий, связанных с процессом обмена файлами (с последующей передачей в SIEM-систему)

Обмен между контурами безопасности





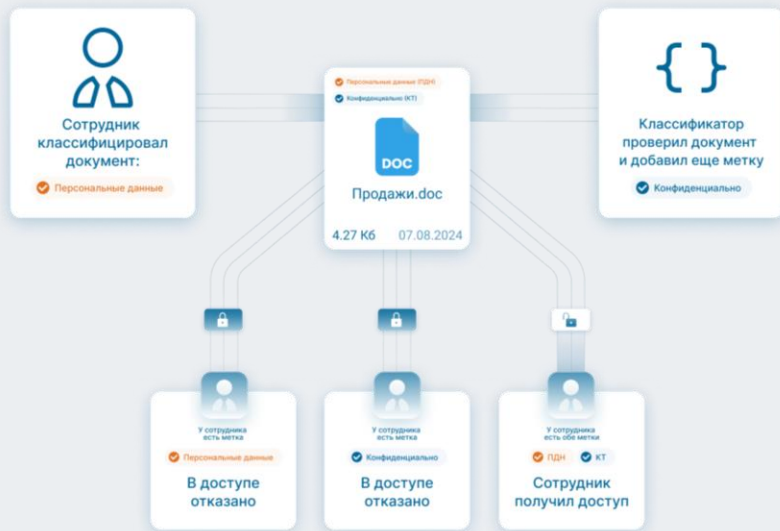
Дополнительные функции безопасности Secret Cloud Enterprise для гарантированной защиты файлов

Дополнительные функции безопасности

Автоназначение меток безопасности

С помощью анализа текста в файле, на основе заданных правил, система автоматически назначает метки безопасности. Это позволяет минимизировать ошибки ручной классификации конфиденциальной информации и экономить время сотрудников.

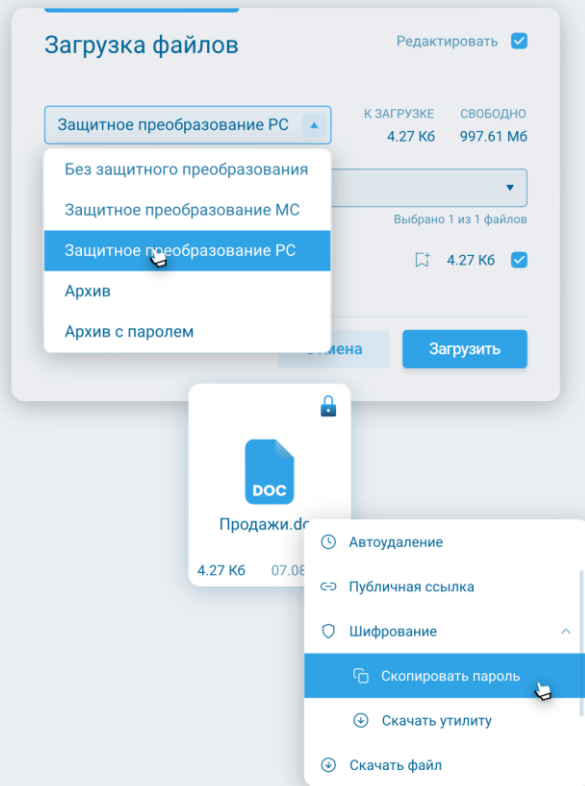
Назначение меток безопасности возможно в принудительном и рекомендательном режиме, а изменение их производится через запрос администратору.



Дополнительные функции безопасности

Контейнеры DRM

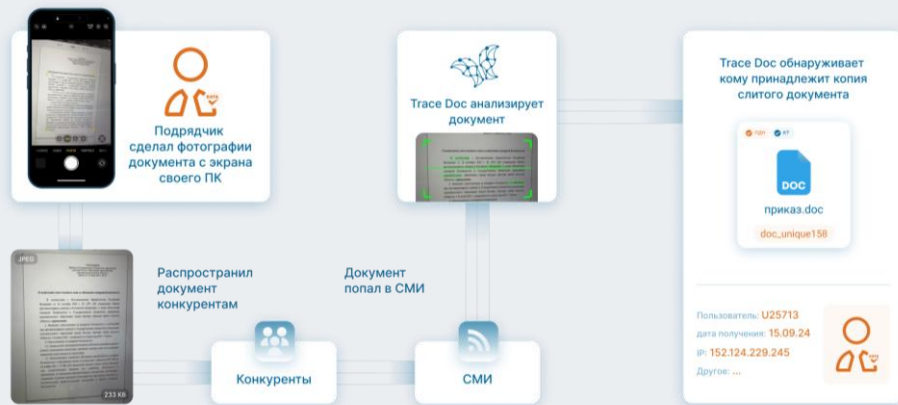
- Для защиты от несанкционированного доступа файлы помещаются в специализированные контейнеры, которые обеспечивают дополнительную безопасность.
- Виртуальный диск создается под каждого адресата с ограниченным сроком действия. Скачанный файл-контейнер можно открыть только на ПК первого доступа, предотвращая распространение. Работа с файлом ведется исключительно в контейнере, без возможности извлечения.
- Система поддерживает различные типы шифрования (ГОСТ, AES) для сотрудников и контрагентов, обеспечивая гибкость и соответствие требованиям безопасности при различных сценариях использования.



Дополнительные функции безопасности

Скрытое маркирование

- Идентификация злоумышленника, разгласившего конфиденциальной информации.
- С помощью продукта для создания уникальных копий документов Trace Doc в любые документы с текстовым содержанием добавляются скрытые метки в виде пиксельных сдвигов. Таким образом для каждого пользователя появляется уникализированная копия документа.
- Расследование инцидентов происходит утечки данных по фотографии, скриншоту или распечатанной копии документа за счёт считывания скрытых меток.



Совместимость программных решений и минимальные технические требования

Совместимость

Операционные системы и офисные редакторы



СУБД



СЗИ



Интеграции и совместимости

Совместимые антивирусы по протоколу ICAP



Kaspersky®
Web Traffic Security

Совместимые DLP по протоколу ICAP



SEARCHINFORM
INFORMATION SECURITY



Совместимые песочницы по протоколу ICAP



Kaspersky
Anti Targeted
Attack



Совместимые SIEM по протоколу SYSLOG



Минимальные технические требования

Количество пользователей	Хранилище для 1 пользователя, Гб	Исполнение	Количество VM	vCPU всего, шт.	ОЗУ всего, Гб	Хранилище и файлы всего, Гб***
100	10	Отказоустойчивое	15	92	100	11 430
100	10	Неотказоустойчивое	1	8	12	3 530
1000	10	Отказоустойчивое	15	152	152	103 500
1000	10	Неотказоустойчивое	1	24	48	34 220
5000	10	Отказоустойчивое	17	504	504	512 960

**vCPU должен быть на уровне 2,5 ГГц. Если мощнее, то количество процессоров может быть пропорционально уменьшено.

***для работы SCE нужны SSD. При использовании HDD требования к системе могут быть изменены.

СМИ о нас



Организация эффективной
и безопасной работы
внешних сотрудников
с данными компании
(видео)



РБК Компании

Как сделать коммуникацию
максимально безопасной



Онлайн-офис с защитой:
почему стоит перейти
на VDR-решения



Организация защищённого
файлообмена в КИИ на базе
Secret Cloud Enterprise