ООО «ВЭБ КОНТРОЛ ДК»

Автоматизированная система контроля и управления привилегированным доступом «sPACE»

ОПИСАНИЕ ФУНКЦИОНАЛЬНЫХ ХАРАКТЕРИСТИК

Москва, 2021

СОДЕРЖАНИЕ

1 Общие сведения

Этот документ представляет собой описание функциональных характеристик программного продукта «sPACE» (далее Система, «программа», «программный продукт»).

Документ включает в себя главы с общим описанием программы и пояснениями по основному ее функционалу. Документ предназначен для специалистов, которые желают ознакомиться с возможностями Системы.

2 ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ, ИСПОЛЬЗУЕМЫЕ СОКРАЩЕНИЯ

Термин/сокращение	Определение
Привилегированный доступ (ПД)	Неограниченный доступ для просмотра и изменения данных, изменения параметров конфигурации, запуска программ и т.д.
Сеанс привилегированного доступа	Интерактивный обмен данными, имеющий ограниченный временной интервал, в ходе которого владельцу учетной записи предоставляется привилегированный доступ. Сеанс считается запущенным с момента отображения на экране пользователя окна инструмента администрирования и законченным в момент выхода из инструмента администрирования.
Наряд-допуск (НД)	Разрешение на выполнение определенной задачи с использованием sPACE, в котором содержится название задачи, срок действия наряда-допуска, инициирующее и согласующее лицо, обоснование и объекты администрирования.
ОА	Объект администрирования. Целевая система, действия с которой производятся с использованием привилегированного доступа
ИА	Инструмент Администрирования. Приложение, запускаемое на сервере ЗСА, с помощью которого осуществляются привилегированный доступ к ОА.
ЗСА	Защищенная Среда Администрирования. Выделенный сервер, на котором выполняется сеанс привилегированного доступа.
FQDN	Fully Qualified Domain Name, имя домена, не имеющее неоднозначностей в определении. Включает в себя имена всех родительских доменов иерархии DNS
СОС	Служба Обмена Сообщениями. Служба, обеспечивающая коммуникацию между компонентами sPACE.
ВСАС	Внутренняя система видеоаудита, осуществляющая запись скриншотов действий пользователей.

3 Общие сведения о системе sPACE

3.1 Назначение программы

«sPACE» — это автоматизированная система организации и управления рабочим процессом привилегированных пользователей с интегрированной защищенной средой реализации полномочий и подсистемой управления жизненным циклом паролей и ключей доступа.

Система «sPACE» предназначена для автоматизации работы привилегированных пользователей, повышения уровня безопасности учетных данных, адресного предоставления привилегированным пользователям минимально необходимых привилегий на ограниченное время, повышения скорости предоставления привилегированным пользователям необходимых для работы привилегий, децентрализации процесса предоставления привилегированного доступа и организации объективного контроля сеансов привилегированного доступа на крупных предприятиях и в компаниях среднего и малого бизнеса.

СУПД «sPACE» не обеспечивает безопасность сама по себе. Это инструмент для организации привилегированного доступа, который работает в защищённой среде и позволяет пользователям подключаться к ней. При этом нельзя забывать о других средствах информационной и компьютерной безопасности, которые должны быть правильно настроены и исправно работать.

3.2 Краткое описание функционала программы

В программе реализован следующий функционал:

- предоставление защищенной среды администрирования (ЗСА), изолированной от потенциально вредоносной среды рабочей станции, с которой осуществляется привилегированный доступ;
- автоматизация процесса согласования привилегированного доступа;
- хранение паролей без раскрытия пользователю в защищенном хранилище, их ротация;
- контроль доступа к совместным учетным данным;
- контроль команд и действий, выполняемых специалистами;
- мониторинг и запись сеансов привилегированного доступа;
- поддержка протоколов удаленного администрирования;

- предоставление аналитических данных о действиях привилегированных пользователей с помощью консоли, отчетов и аналитики;
- двухфакторная аутентификация с использованием технологии RuToken, TOTP;
- разграничение доступа к управлению программой;
- управление работой программы;
- добавление новых объектов и инструментов привилегированного доступа;
- аварийный режим
- возможность интеграции с существующими системами информационной безопасности посредством API.

3.3 Права доступа к функционалу sPACE

3.3.1 Роли пользователей в Системе sPACE

Персоналу, работающему с Системой, могут быть назначены следующие роли:

- пользователь с ограниченными правами (базовый);
- стандартный пользователь;
- ответственный пользователь;
- администратор;
- аудитор;
- продвинутый аудитор;
- привилегированный администратор.

Сотрудникам, работающим с Системой, может быть назначено несколько ролей.

3.3.1.1 Пользователь с ограниченными правами (базовый)

Базовый пользователь имеет следующие права:

- запуск сеансов привилегированного доступа в защищенной среде.

Под сеансом привилегированного доступа понимается интерактивный обмен данными, имеющий ограниченный временной интервал, в ходе которого владельцу учетной записи предоставляется неограниченный доступ для просмотра и изменения данных, изменения параметров конфигурации, запуска программ и т. д. Сеанс считается запущенным с момента отображения на экране пользователя окна инструмента администрирования и законченным в момент выхода из инструмента администрирования.

Для запуска сеанса привилегированного доступа базовому пользователю необходимо иметь согласованный наряд-допуск к конкретному информационному ресурсу. Наряд-допуск согласуется сотрудником, отвечающим за предоставление привилегированного доступа к данному объекту администрирования.

Под нарядом-допуском в данном документе понимается разрешение на выполнение определенной задачи с использованием sPACE, в котором содержится следующая информация:

- название задачи,
- информационный ресурс (объект), к которому запрашивается доступ,
- инструмент взаимодействия (оснастки, инструменты администрирования, программы, интерфейс) с информационным ресурсом, к которому запрашивается доступ,
- срок действия разрешения,
- учетное имя, используемое для доступа к ресурсу,
- лицо, согласующее доступ к данному информационному ресурсу,
- обоснование запроса на получение привилегированного доступа к данному информационному ресурсу (номер заявки из ITSM системы, например, текстовое описание ситуации, которая привела к необходимости получить привилегированный доступ к данному информационному ресурсу (объекту).

3.3.1.2 Стандартный пользователь

Стандартный пользователь системы имеет следующие права:

- запуск сеансов привилегированного доступа в защищенной среде,
- запрос наряда-допуска для себя,
- просмотр записей собственных сеансов, если для них есть соответствующие данные BCAC.

Сотрудник с ролью «Пользователь» имеет право согласовывать наряд-допуск, если его учетное имя добавлено в список лиц, согласующих наряд-допуск к данному информационному ресурсу (объекту администрирования). Он также имеет возможность просматривать записи собственных сеансов.

3.3.1.3 Ответственный пользователь

Ответственный пользователь имеет следующие права:

- запуск сеансов привилегированного доступа,
- запрос наряда-допуска для себя,
- запрос наряда-допуска для других пользователей.
- просмотр записей собственных сеансов, если для них есть соответствующие данные BCAC.

Сотрудник с ролью «Ответственный пользователь» имеет право согласовывать наряд-допуск, если его учетное имя добавлено в список лиц, согласующих наряд-допуск к данному информационному ресурсу (объекту администрирования).

3.3.1.4 Администратор

Администратор sPACE осуществляет управление задачами на работу с информационными ресурсами, объектами ИТ инфраструктуры компании, инструментами администрирования и учетными записями.

3.3.1.5 Аудитор

Аудитор имеет право просматривать сеансы привилегированного доступа в реальном времени и в архиве.

3.3.1.6 Продвинутый аудитор

Помимо стандартных возможностей аудитора, данный тип пользователей имеет право на просмотр данных из key-log и clipboard для сеансов привилегированного доступа.

3.3.1.7 Привилегированный администратор

Привилегированный администратор – это сотрудник, который в дополнение к правам администратора имеет право перевода Системы в аварийный режим.

Аварийный режим – это режим Системы, при котором базовые, стандартные и ответственные пользователи имеют возможность узнать учетные данные объектов администрирования, доступ к которым для них согласован.

3.3.2 Перечень функционала, доступного для каждой роли

Таблица Функционал, доступный каждой роли

Наименование	Права
Пользователь с ограниченными правами	**Доступен раздел "Сеансы"** ● Запуск сеансов администрирования на основе согласованных "Нарядов-допусков".
Стандартный пользователь	**Доступен раздел "Сеансы"**

	● Просмотр объектов администрирования, сгруппированных в виде задач. ● Запрос наряда-допуска на объекты администрирования для своей учетной записи. ● Запуск сеансов администрирования на основе согласованных нарядов-допусков. ● Согласование нарядов-допусков, если пользователь входит в группу согласующих для соответствующей задачи администрирования. ● Просмотр записей собственных сеансов, если для них есть соответствующие данные ВСАС.
Ответственный пользователь	**Доступен раздел "Сеансы"** ● Просмотр объектов администрирования, сгруппированных в виде задач. ● Возможность запросить "Наряд-допуск" на объекты администрирования для своей учетной записи и для чужих учетных записей. ● Запуск сеансов администрирования на основе согласованных "Нарядов-допусков". ● Согласование "Нарядов-допусков" если пользователь входит в группу согласующих для соответствующей задачи администрирования. ● Просмотр записей собственных сеансов, если для них есть соответствующие данные ВСАС.
Администратор	**Доступен раздел "Управление системой"** ● Управление пользователями. ● Управление группами согласования. ● Добавление задач. ● Добавление и настройка объектов и инструментов администрирования. ● Настройка сценариев запуска и приложений. ● Просмотр и управление нарядами-допусками. ● Просмотр и управление сеансами привилегированного доступа. ● Просмотр системных настроек и статуса компонентов системы. ● Просмотр статистики. ● Настройка серверов защищенной среды (ЗС). ● Просмотр и управление системами видеоаудита, в том числе внутренней системой видеоаудита (ВСАС) и хранилищами для нее. ● Просмотр лицензии. ● Просмотр и управление агентами паролей.
Аудитор	**Доступен раздел "Аудит"** ● Просмотр журнала доступа пользователя ● Просмотр сеансов администрирования в реальном времени. ● Просмотр видеозаписей данных сеансов ● Просмотр списка сеансов.
Продвинутый аудитор	**Доступен раздел "Аудит"** ● Просмотр журнала доступа пользователя

	● Просмотр сеансов администрирования в реальном времени. ● Просмотр видеозаписей данных сеансов ● Просмотр списка сеансов. ● Просмотр данных key-log и clipboard для сеансов.
Привилегированный администратор	**Доступен раздел "Управление системой"** ● Управление пользователями. ● Управление группами согласования. ● Добавление задач. ● Добавление и настройка объектов и инструментов администрирования. ● Настройка сценариев запуска и приложений. ● Просмотр и управление нарядами-допусками. ● Просмотр и управление сеансами привилегированного доступа. ● Просмотр системных настроек и статуса компонентов системы. ● Просмотр статистики. ● Настройка серверов защищенной среды (ЗС). ● Просмотр и управление системами видеоаудита, в том числе внутренней системой видеоаудита (ВСАС) и хранилищами для нее. ● Просмотр лицензии. ● Просмотр и управление агентами паролей. ● Перевод Системы в аварийный режим.

3.3.3 Настройка прав доступа для каждой роли

При работе Система автоматически добавляет в Систему пользователей из соответствующих групп службы каталогов Windows. Для этого необходимо наличие пользователей в Active Directory Users and Computers.

Назначение или изменение роли учетной записи происходит путем добавления пользователя в соответствующую группу Active Directory. Рекомендуемое соответствие ролей в Системе группам Active Directory приводится в Инструкции по развертыванию.

4 Подробное описание возможностей sPACE

Для функционирования «sPACE» на аппаратное обеспечение должно быть установлено программное обеспечение. Установка и настройка программного обеспечения, необходимого для работы «sPACE», описана в Инструкции по развертыванию.

Вся работа в Системе осуществляется посредством работы на портале. На нём присутствует три глобальных раздела: «Сеансы», «Управление системой», «Аудит». Доступность этих разделов зависит от роли пользователя в Системе.

Раздел «**Сеансы**» позволяет пользователю выполнять следующие действия:

- Просмотр своих сеансов привилегированного доступа.
- Просмотр записей ВСАС своих сеансов привилегированного доступа.
- Фильтрация своих сеансов привилегированного доступа.
- Запуск нового сеанса привилегированного доступа.
- Просмотр задач на управление объектами администрирования, сгруппированные по объектам администрирования.
- Просмотр своих нарядов-допусков.
- Запрос нового наряда-допуска для себя.

Раздел «**Управление системой**» используется для настройки Системы в условиях конкретной ИТ-инфраструктуры компании и предполагает выполнение следующих действий:

- Управление пользователями.
- Управление группами согласования.
- Управление учётными записями.
- Управление объектами администрирования.
- Управление приложениями и сценариями запуска.
- Управление задачами администрирования.
- Настройка и управление нарядами-допусками.
- Настройка и управление сеансами привилегированного доступа.
- Настройка и управление серверами защищенной среды (ЗС).
- Просмотр системных настроек.
- Просмотр информации о статусе компонентов Системы.
- Просмотр информации о лицензии Системы.

- Управление агентами паролей.
- Управление встроенной системой внутреннего видеоаудита
- Управление хранилищами ВСАС.
- Управление сторонними системами видеоаудита.
- Просмотр статистики и формирование отчётности по использованию Системы.

Раздел «**Аудит**» позволяет осуществлять аудит Системы, а именно:

- Осуществление аудита сеансов пользователей.
- Осуществление аудита доступа пользователей к порталу.
- Осуществление аудита операций рандомизации.

Ниже будут подробнее рассмотрен функционал, доступный для каждого из разделов «Управление системой» и «Аудит».

4.1 Управление пользователями

Для управления пользователями администратор может выполнить следующие действия:

- Просмотреть список всех пользователей Системы,
- Добавить новых пользователей,
- Редактировать данные существующих пользователей,
- Удалить существующих пользователей,
- Ограничивать существующих пользователей,
- Подключить или отключить поддержку двухфакторной аутентификации.

4.2 Управление группами согласования

Группа согласования — это определенная группа пользователей, которые имеют право согласовать (одобрять) наряды-допуски на управление объектами администрирования в рамках выполнения задачи. При создании задачи обязательно должна указываться та группа пользователей, которая будет ее согласовывать.

В рамках управления группами администратор может выполнять следующие действия:

- Просматривать все группы согласования.
- Добавлять группы согласования,
- Редактировать группы согласования

- Добавлять пользователей в группу согласования,
- Удалять пользователей из группы согласования,
- Удалять группу согласования.

4.3 Управление учетными записями

Администраторы могут выполнять следующие действия с учетными записями:

- Просматривать все учетные записи,
- Добавлять учетную запись,
- Редактировать учетную запись,
- Удалять учётные записи.

4.4 Управление объектами администрирования

Объект администрирования — это объект защищенной среды, на который пользователь не может попасть напрямую, а только через сервер ЗСА.

Для управления объектами администрирования администратору доступен следующий функционал:

- Просматривать все объекты администрирования/типы объектов администрирования,
- Добавлять объект администрирования/тип объекта администрирования,
- Редактировать объект администрирования/тип объекта администрирования,
- Удалять объекты администрирования/типы объектов администрирования,
- Задавать внешний ID для объекта администрирования,
- Добавлять один или несколько объектов администрирования к определённому серверу защищённой среды.

4.5 Управление приложениями и сценариями запуска

Пользователи управляют объектами администрирования при помощи инструментов администрирования (приложений), которые предварительно настраивает администратор.

В рамках настройки и управления приложениями и сценариями запуска приложений администраторы могут выполнять следующие действия:

- Просматривать все приложения и сценарии,
- Добавлять приложение/сценарий,
- Редактировать приложение/сценарий,

- Удалять приложения/сценарии,
- Задавать внешний ID для приложения/сценария,
- Задавать сервер ЗС для одного приложения или нескольких.

4.6 Управление задачами администрирования

Работа sPACE основана на принципе минимальных привилегий, когда доступ к объектам администрирования предоставляется пользователям исключительно для выполнения задачи, к которой согласован наряд-допуск. Для выбора пользователями задач администрирования необходимо предварительно добавить их в Систему.

В рамках управления задачами администраторы могут:

- Просматривать все задачи,
- Добавлять задачу,
- Редактировать задачу,
- Удалять задачи.

4.7 Настройка и управление нарядами-допусками

Доступ к объектам администрирования осуществляется на основании наряда-допуска. Наряд-допуск (НД) – это задание на выполнение определенной задачи в рамках Системы, в котором содержится название задачи, срок действия наряда-допуска, инициирующее и согласующее лицо, обоснование и объекты администрирования.

В рамках настройки и управления нарядами-допусками администраторы могут выполнять следующие действия:

- Просматривать наряды-допуски и всю информацию о них,
- Добавлять наряд-допуск,
- Редактировать наряд-допуск,
- Согласовывать наряд-допуск (если администратор входит в группу согласования),
- Удалять наряды-допуски,
- Задавать внешний ID для наряда-допуска.

4.8 Настройка и управление сеансами привилегированного доступа

В рамках получения данных о сеансах привилегированного доступа в Системе администраторы могут выполнять следующие действия.

- Фильтровать сеансы по состоянию и по дате создания
- Просматривать таблицу сеансов,
- Просматривать информацию о сеансах,
- Удалять строки в таблице сеансов.

4.9 Настройка и управление серверами ЗС

Сервер Защищенной Среды — это выделенный сервер, на котором выполняется сеанс привилегированного доступа. Каждый сервер ЗСА поддерживает выполнение до 50 одновременных сеансов ПД. При увеличении числа привилегированных пользователей или увеличении количества задач по администрированию объектов администрирования может потребоваться настройка серверов ЗСА.

В рамках управления серверами ЗСА администраторы могут:

- Просматривать сервера ЗСА,
- Добавлять сервер ЗСА,
- Изменять настройки сервера ЗСА,
- Удалять сервера ЗСА

4.10 Просмотр системных настроек

Изменение системных настроек через интерфейс Системы не предусмотрено, но администратор может просматривать их в соответствующем разделе интерфейса.

4.11 Просмотр информации о статусе компонентов Системы

Администраторы могут выполнять следующие действия:

- Просматривать информацию о компонентах системы,
- Фильтровать таблицу статуса компонентов системы по различным параметрам,
- Обновлять таблицу статуса компонентов,
- Экспортировать таблицу компонентов системы в виде html-файла,
- Быстро узнавать о состоянии системы по индикатору «Светофор».

4.12 Просмотр информации о лицензии Системы

Лицензия системы учитывает максимально допустимые значения для количества ядер, хранилищ, одновременных сеансов, работающих пользователей и т. д. Администраторы могут выполнять следующие действия:

- Просматривать лицензию.
- Обновлять страницу лицензии,
- Скачивать запрос на лицензию,
- Загружать лицензию.

4.13 Управление агентами паролей

Агенты паролей служат для рандомизации паролей учётных записей. В рамках Системы реализованы следующие возможности, доступные администратору:

- Просмотр агентов паролей,
- Добавление нового агента паролей,
- Редактирование агента паролей,
- Удаление агентов паролей,
- Добавление внешних ID для агента паролей.

4.14 Управление встроенной системой внутреннего видеоаудита

Система «sPACE» позволяет осуществлять видеоаудит системы, для этого у нее есть специальный встроенный функционал, настройка которого производится в соответствующем разделе. Видеоаудит служит для записи скриншотов сеансов и действий пользователей. Внутренняя система видеоаудита (ВСАС) не требует дополнительной установки и поставляется вместе с Системой.

Для управления ВСАС администратору доступен следующий функционал:

- Просматривать параметры внутренней системы видеоаудита сеансов,
- Редактировать параметры ВСАС глобально,
- Настраивать параметры ВСАС для отдельного сервера ЗС.

4.15 Управление хранилищами ВСАС системы

Для управления хранилищами системы ВСАС, которые содержат скриншоты записанных сеансов, администратору доступен следующий функционал:

- Просмотр доступных хранилищ,
- Удаление строки в таблице хранилищ.

4.16 Управление сторонними системами видеоаудита

Помимо встроенной внутренней системы видеоаудита существует возможность добавить в sPACE сторонние системы видеоаудита. Для управления ими администратору доступен следующий функционал:

- Просмотр систем видеоаудита,
- Добавление системы видеоаудита,
- Редактирование системы видеоаудита,
- Удаление систем видеоаудита,
- Добавление типа систем видеоаудита,
- Редактирование типа систем видеоаудита,
- Добавление параметра типа системы видеоаудита,
- Удаление типов систем видеоаудита,
- Загрузка/скачивание шаблона типа системы видеоаудита.

4.17 Формирование отчетности по использованию Системы

Система sPACE позволяет формировать статистику по использованию системы на основе следующих данных:

- использование системы,
- суммарное количество сеансов за временной интервал,
- максимальное количество одновременных сеансов за определенный интервал времени.

Администратор может сформировать следующую отчетность:

- об использовании приложений, включая общее количество сеансов, число успешных и неуспешных сеансов,
- о количестве сеансов к объектам администрирования, включая число успешных и неуспешных сеансов,
- об использовании Системы пользователями, включая общее количество сеансов, а также число успешных и неуспешных сеансов,
- о суммарном количестве сеансов за час, сутки и месяц,
- о максимальном количестве одновременных сеансов за час, сутки, месяц.

4.18 Осуществление аудита сеансов

Для осуществления аудита сеансов реализован следующий функционал:

- Фильтрация сеансов по состоянию и по дате создания,
- Обновление таблицы сеансов,
- Просмотр детальной информации о каждом сеансе,
- Просмотр записи сеанса,
- Просмотр записи работающего сеанса в режиме онлайн,
- Скачивание скриншотов сеанса,
- Экстренное завершение работающего сеанса,
- Поиск по метаданным сеансов,
- Просмотр записи сеанса по данным Key Logger.

4.19 Осуществление аудита доступа пользователей к порталу

При необходимости администратор может получить всю информацию о пользовательских сессиях: кем они созданы, когда и с какого адреса производился доступ к порталу.

4.20 Осуществление аудита операций рандомизации

Для администратора Системы реализован следующий функционал:

- Фильтрация операций рандомизации по состоянию и по дате создания,
- Обновление таблицы операция рандомизации,
- Просмотр детальной информации о каждом сеансе рандомизации.