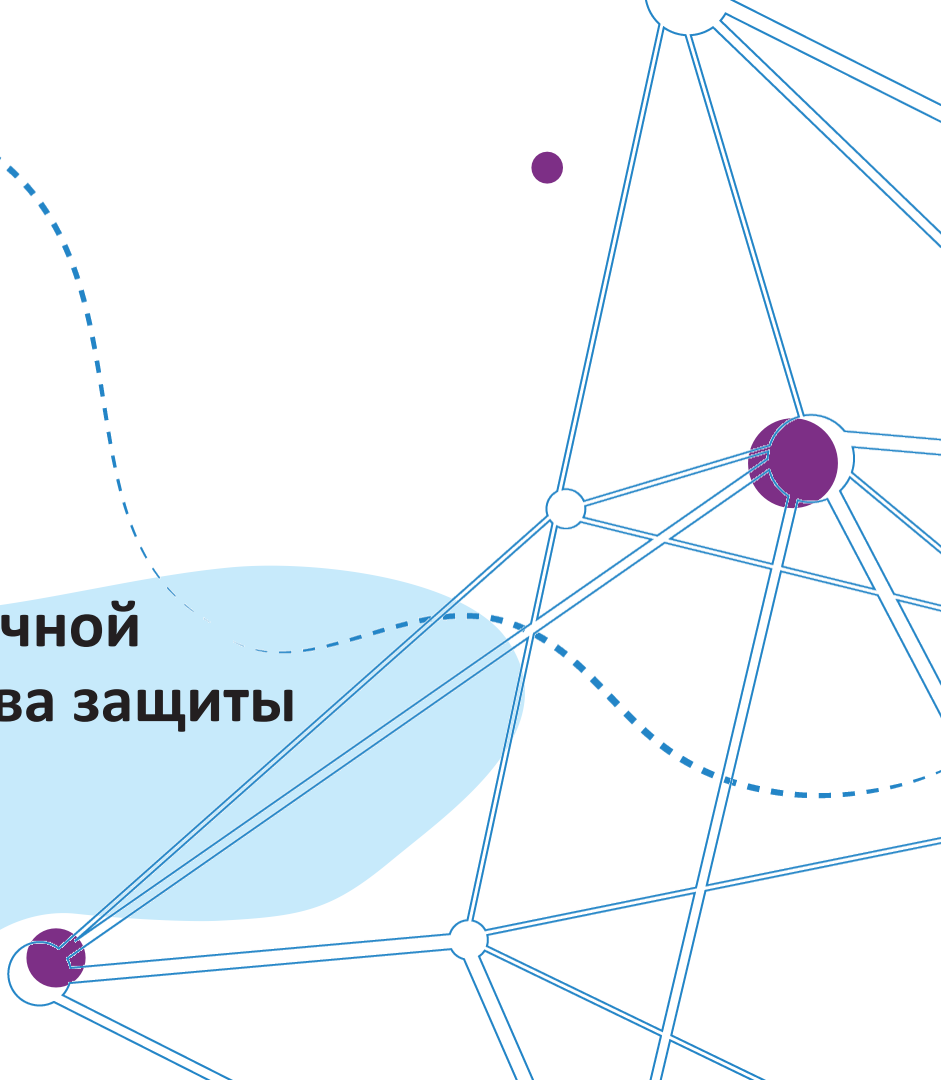
Space
создаем
реальность

Совместное применение облачной платформы SpaceVM и средства защиты информации vGate R2



Основное предназначение

- Средство защиты информации vGate R2 от компании ООО «Код Безопасности» предназначено для формирования единого контура защиты виртуализации в среде SpaceVM

- Контроль рабочего места администратора, сервера управления и хоста гипервизора обеспечивает целостную защиту приложений от атак со стороны виртуальной инфраструктуры

Задачи решаемые SpaceVM и vGate

vGate R2 (версии 4.9) и SpaceVM (версия 6.2.1) совместно могут применяться для организации защиты информации при создании информационных систем и аттестации следующих объектов:

Государственные информационные системы (ГИС)
- до 1 класса защищённости включительно (Приказ ФСТЭК России от 11 февраля 2013 г. № 17)

Информационные системы персональных данных (ИСПДн)
- до 1 уровня защищенности персональных данных включительно (Приказ ФСТЭК России от 18 февраля 2013 г. № 21)

Объекты критической информационной инфраструктуры (КИИ)
- до 1 категории значимости включительно (Приказ ФСТЭК России от 25 декабря 2017 г. № 239)

Автоматизированные системы (АС)
- до класса защищенности 1Г включительно (Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации» (Гостехкомиссия России, 1992))

Схема применения SpaceVM и vGate

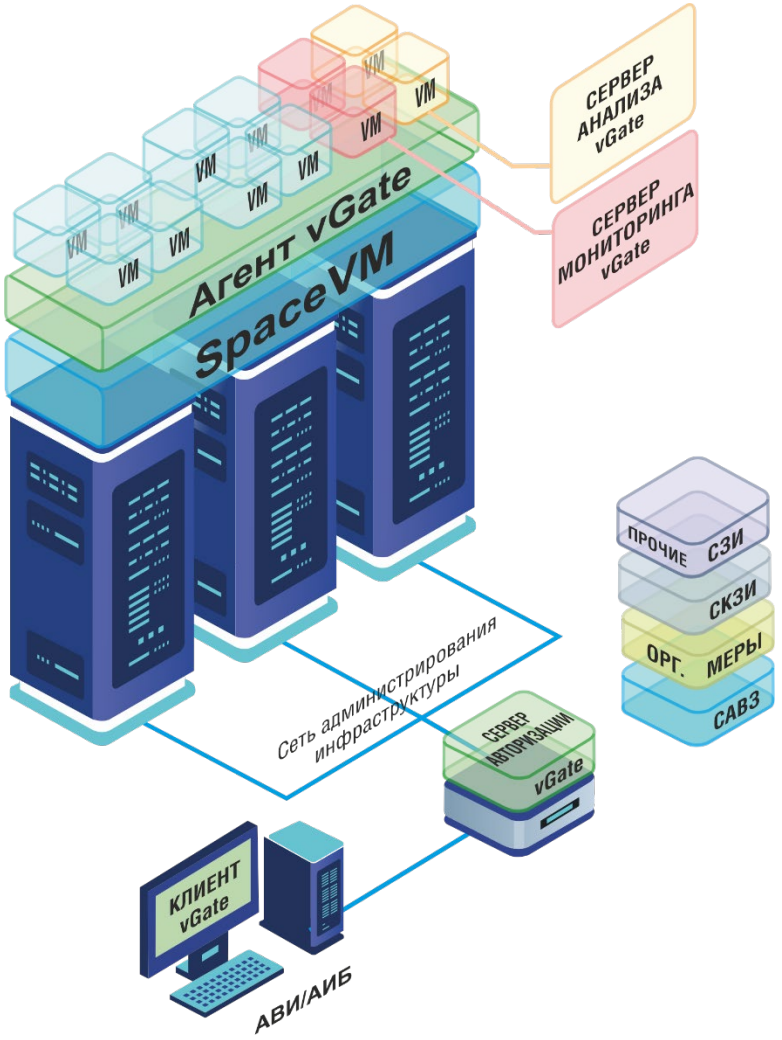
СЕВЕР АВТОРИЗАЦИИ vGate
Устанавливается на специально выделенный для него компьютер который может использоваться в качестве рабочего места АВИ/АИБ

КЛИЕНТ vGate
Устанавливается на рабочее место АВИ/АБИ (если рабочее место АИБ во внешнем периметре сети администрирования), серверы сервисных служб (DNS, AD и т. д.)

АГЕНТ vGate
Устанавливается на гипервизор SpaceVM

СЕРВЕР МОНИТОРИНГА vGate
Устанавливается на виртуальную машину

СЕРВЕР АНАЛИЗА vGate
Устанавливается на виртуальную машину



Основные компоненты vGate:

vGate имеет WEB интерфейс для централизованного управления

СЕРВЕР АВТОРИЗАЦИИ vGate

Устанавливается на специально выделенный для него компьютер который может использоваться в качестве рабочего места АИБ

- Аутентификация пользователей и компьютеров
- Разграничение доступа к средствам управления виртуальной инфраструктурой
- Регистрация событий безопасности
- Хранение данных (учетной информации, журналов аудита и конфигурации vGate)
- Репликация данных (при наличии резервного сервера)
- Синхронизация настроек серверов авторизации
- Автоматическое развертывание агентов vGate на защищаемых серверах

КЛИЕНТ vGate

Рабочее место АВИ, рабочее место АИБ (если рабочее место АИБ во внешнем периметре сети администрирования), серверы сервисных служб (DNS, AD и т. д.)

- Идентификация и аутентификация пользователя.
- Идентификация и аутентификация компьютера.
- Контроль целостности компонентов клиента vGate.
- Выбор уровня сессии при работе с конфиденциальными ресурсами (при включенном контроле уровня сессий).
- Регистрация событий безопасности

СЕРВЕР МОНИТОРИНГА vGate

Устанавливается на виртуальную машину

- Сбор и корреляция событий виртуальной инфраструктуры

СЕРВЕР АНАЛИЗА vGate

Устанавливается на виртуальную машину

- Анализ сетевого трафика виртуальных машин в рамках функции "Контроль прикладных протоколов"

АГЕНТ vGate

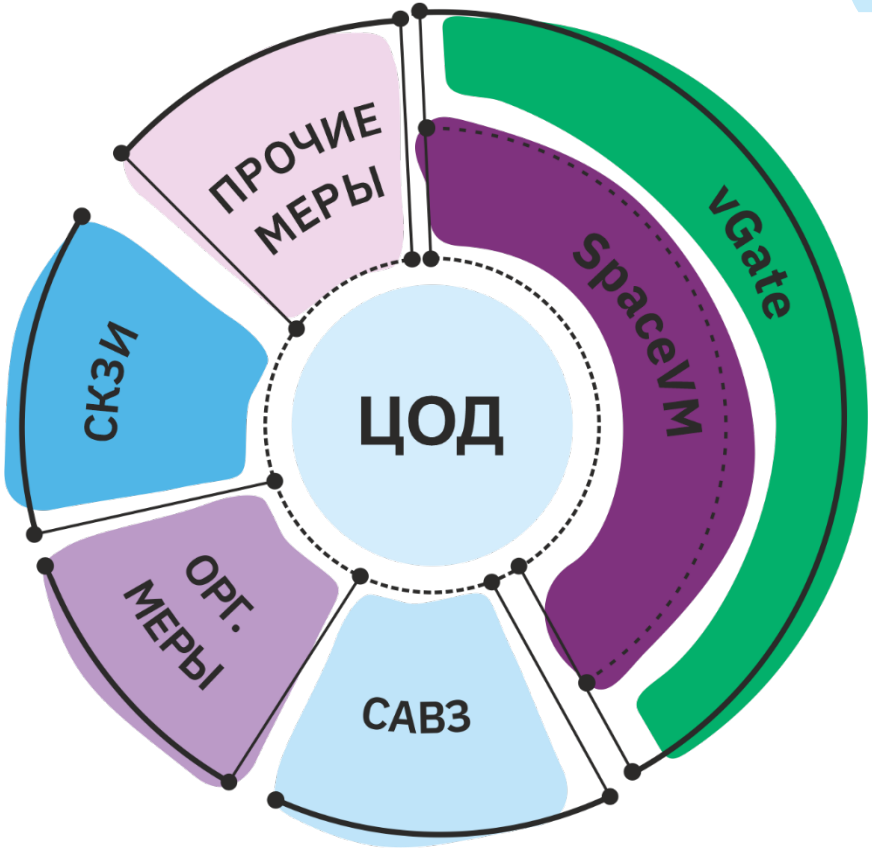
Устанавливается на гипервизор SpaceVM

- Защита серверов виртуализации KVM
- Контроль целостности и доверенная загрузка ВМ
- Защита от НСД внутри сети администрирования
- Регистрация событий безопасности

Облачная платформа SpaceVM и средство защиты информации vGate R2 совместно с комплексом организационных и технических мер

Обеспечивает:

- конфиденциальность информации
- целостность информации
- доступность информации



Применяется в :

ГИС

КИИ

ИСПДн

АС

Организационные и технические меры

СРЕДСТВА АНТИВИРУСНОЙ ЗАЩИТЫ

- АРМ
- Сервера
- Периметральные средства защиты информации (МЭ, прокси серверы, и т.д.)
- Мобильные технические средства
- Иные точки доступа в информационную систему, подверженные внедрению (заражению) вредоносными компьютерными программами (вирусами) через съемные машинные носители информации или сетевые подключения, в том числе к сетям общего пользования (вложения электронной почты, веб- и другие сетевые сервисы)

СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ (СКЗИ)

- Применение наложенных средств шифрования может применяться в зависимости от требований к ИС
- Защита информации обеспечивается путем защиты каналов связи от несанкционированного физического доступа (подключения) к ним и (или) применения в соответствии с законодательством Российской Федерации средств криптографической защиты информации или иными методами

ОРГАНИЗАЦИОННЫЕ МЕРЫ

- Организационно-распорядительные документы оператора по защите информации
- Защита информации от утечки по техническим каналам в соответствии со Специальными требованиями и рекомендациями по технической защите конфиденциальной информации (СТР-К)
- Организация контролируемой зоны
- Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены исключающие несанкционированный физический доступ
- Размещение устройств вывода (отображения, печати) информации для исключения возможности несанкционированного просмотра выводимой информации
- Защита от внешних воздействий в соответствии с требованиями законодательства Российской Федерации (пожарная безопасность, температурно-влажностной режим и т.д.)
- Отключение переферийных устройств на рабочих местах

ПРОЧИЕ НАЛОЖЕННЫЕ СЗИ

- СОВ – система обнаружения вторжений
- Средства антиспам
- DLP - Data Leak Prevention, предотвращение утечек информации
- Резервирование технических средств
- Применение отказоустойчивых технических средств
- Применение средств межсетевого экранирования

Сценарий применения SpaceVM в ИСПДн

ИСПДн	vGate	SpaceVM	САВЗ	Орг. меры	СКЗИ	Прочие СЗИ
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)	+	+				
II. Управление доступом субъектов доступа к объектам доступа (УПД)	+	+		организационно-распорядительные документы АИБ		
III. Ограничение программной среды (ОПС)	+			организационно-распорядительные документы АИБ	МЭ, VLAN, VPN	
IV. Защита машинных носителей персональных данных (ЗНИ)	+	+		организационно-распорядительные документы АИБ		применение СЗИ от НСД Dallas Lock 8.0-К
V. Регистрация событий безопасности (РСБ)	+	+				
VI. Антивирусная защита (АВЗ)			Kaspersky Endpoint Security			
VII. Обнаружение вторжений (СОВ)						применение СОВ на уровне сети: ViPNet IDS, Континент или на уровне узла: СОВ Dallas Lock
VIII. Контроль (анализ) защищенности персональных данных (АНЗ)	+			организационно-распорядительные документы АИБ		
IX. Обеспечение целостности информационной системы и персональных данных (ОЦЛ)	+	+		организационно-распорядительные документы АИБ		
X. Обеспечение доступности персональных данных (ОДТ)	+	+		организационно-распорядительные документы АИБ		
XI. Защита среды виртуализации (ЗСВ)	+	+	Kaspersky Endpoint Security			
XII. Защита технических средств (ЗТС)				организационно-распорядительные документы АИБ		
XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)	+	+			Континент, ViPNet	применение средств межсетевого экранирования
XIV. Выявление инцидентов и реагирование на них (ИНЦ)		+		организационно-распорядительные документы АИБ		
XV. Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ)		+		организационно-распорядительные документы АИБ		

АЛЕКСЕЙ Мензовитый

Директор по продукту SpaceVM

a.menzovity@spacevm.org