

ПРОТОКОЛ № 14875/2023

проведения совместных испытаний средства защиты от несанкционированного доступа к информации «система аудита сетевого доступа к серверам баз данных и веб-приложениям «Гарда БД» версии 4.23.1 и программного комплекса «СУБД Tantor BE 15» версии 15.2.1.

г. Москва

03.10.2023

1 Предмет испытаний

1.1 В настоящем протоколе зафиксирован факт проведения в период с 25.09.2023 по 03.10.2023 совместных испытаний средства защиты от несанкционированного доступа к информации «система аудита сетевого доступа к серверам баз данных и веб-приложениям «Гарда БД» версии 4.23.1 (далее – «Гарда БД»), разработанного ООО «Гарда Технологии», и программного изделия «СУБД Tantor BE 15» версии 15.2.1, разработанного ООО «ТАНТОР ЛАБС».

2 Объект испытаний

2.1 Перечень компонентов, эксплуатировавшихся в ходе проведения данных испытаний представлен в Таблице 1.

Таблица 1 – Перечень пакетов, относящихся к ПО

Описание	Наименование	MD5	Источник
Файл программного пакета дистрибутива «Гарда БД»	CentOS-7-x86_64-Minimal-1804.iso	fabdc67ff3a1674a489953effa285dfd	Сторона разработчика ПО
Файл программного пакета дистрибутива «Гарда БД»	DBS.4.23.1.tar.gz	26eb1ee24039d848d99d456dc1ced897	Сторона разработчика ПО
Файл программного пакета дистрибутива «Гарда БД»	AGENT.2.13.34-1.tar.gz	25c8931b9d2841c00128dc3f06ff2a1d	Сторона разработчика ПО
Файл программного пакета дистрибутива «СУБД Tantor BE 15»	tantor-be-server-15_15.2.1_amd64.deb	3d46d41e4d46def8ed7f8c1aafe72f1d	Репозиторий ГК

3 Ход испытаний



3.1 В ходе проведения настоящих испытаний были выполнены проверки корректности совместного функционирования «Гарда БД» и «СУБД Tantor VE 15» в объеме, указанном в Приложении 1.

3.2 В ходе испытаний использовался тестовый стенд описанный в Приложении 3.

4 Результаты испытаний

4.1 «Гарда БД» корректно функционирует совместно с «СУБД Tantor VE 15».

5 Вывод

5.1 Система аудита сетевого доступа к серверам баз данных и веб-приложениям «Гарда БД» версии 4.23.1 и «СУБД Tantor VE 15» версии 15.2.1 совместимы, принимая во внимание информацию, содержащуюся в разделах 3, 4.

6 Состав рабочей группы и подписи сторон

6.1 Данный протокол составлен участниками рабочей группы:

Карпенко Д. И. – руководитель сектора отдела технологической совместимости департамента развития технологического сотрудничества ДВиС ООО «РусБИТех-Астра»;

Плотников Д. В. – инженер отдела технологической совместимости департамента развития технологического сотрудничества ДВиС ООО «РусБИТех-Астра».

ООО «РусБИТех-Астра»	
руководитель сектора отдела технологической совместимости департамента развития технологического сотрудничества ДВиС	
(должность)	
(подпись)	Карпенко Д. И. (фамилия, инициалы)



Перечень проверок совместимости «Гарда БД» и «СУБД Tantor BE 15»

№ п/п	Наименование проверки	Результат проверки
1.	Подключение к базе данных	Успешно
2.	Выполнение перехвата запросов к базе данных	Успешно
3.	Перехвата запросов к базе данных с фильтром «Аутентификация»	Успешно
4.	Перехвата запросов к базе данных с фильтром «Другое»	Успешно
5.	Перехвата запросов к базе данных с фильтром «Изменение»	Успешно
6.	Перехвата запросов к базе данных с фильтром «Пользователи»	Успешно
7.	Перехвата запросов к базе данных с фильтром «Права доступа»	Успешно
8.	Перехвата запросов к базе данных с фильтром «Создание»	Успешно
9.	Перехвата запросов к базе данных с фильтром «Удаление»	Успешно



Инструкция по интеграции «Гарда БД»с «СУБД Tantor BE 15»

1 Настройка «Гарда БД»:

1.1 выполнить действия:

1.2 Установить ОС, используя предоставленный образ диска CentOS-7-x86_64-Minimal-1804.iso, согласно документации.

1.3 Установить серверную часть ПО, согласно документации, указав в inventory-файле, в качестве IP-адреса — внешний IP-адрес сервера, в случае установки всего на один сервер.

1.4 Лицензировать серверную часть, согласно документации.

1.5 После установки, используя утилиту setup_sni, необходимо удалить устройство захвата, убедиться, что конфигурация «Агенты БД» активна и переустановить перехватчик.

1.6 В веб-интерфейсе необходимо перейти в раздел «Настройки» и добавить Анализатор в разделе «Анализаторы», указав в графе «IP-адрес управления» и «IP-адрес для агентов» - внешний IP-адрес сервера.

1.7 Подключить Агента, согласно документации.

1.8 В веб-интерфейсе необходимо перейти в раздел «Базы Данных» и указать там значения «Политики», в качестве протокола выбрать «PostgreSQL», в качестве IP-адреса — адрес сервера с СУБД Tantor BE 15 с портом 5432, в качестве анализатора выбрать ранее созданный. После чего необходимо нажать «Создать».

1.9 Перейти в раздел «Агенты», в качестве основного анализатора указать анализатор, созданный по инструкции выше.

1.10 В разделе «Агенты» перейти в подраздел «Мониторинг» и указать в графе Базы данных, созданную по инструкции выше.

2 Настройка «СУБД Tantor BE 15»:

2.1 выполнить действия:

2.2 В среду ОС установить ядро 5.4.0-110-generic (корректность функционирования агента зависит от версии ядра).

2.3 Установить СУБД Tantor BE 15.

2.4 Установить deb-пакет dbs_agent-2.13.34-1-debian-x64.deb, полученный из архива AGENT.2.13.34-1.tar.gz

2.5 Произвести настройку согласно документации.



Описание стенда

1. «СУБД Tantor BE 15» и агент «Гарда БД» запущенный в среде операционной системы специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (очередное обновление 1.7) с установленным оперативным обновлением безопасности БЮЛЛЕТЕНЬ № 2023-0426SE17 (оперативное обновление 1.7.4) на ядре 5.4.0-110-generic.

2. Сервер «Гарда БД» запущенная в среде альтернативной операционной системе.



Перечень используемых сокращений

- СУБД — система управления базами данных;
 «Гарда БД» - система аудита сетевого доступа к серверам баз данных и веб-приложениям «Гарда БД версии 4.23.1 ;
 IP-адрес — адрес устройства на сетевом уровне;
 ДВиС — дирекция внедрения и сопровождения;
 ОС — операционная система;
 ПО – программное обеспечение.

Идентификатор документа 8f36c10f-4c8a-4c01-8e0e-f2f1e10729d2

Документ подписан и передан через оператора ЭДО АО «ПФ «СКБ Контур»

Подписи отправителя:	 ООО "РУСБИТЕХ-АСТРА" Карпенко Дмитрий Иванович	 Не приложена при подписании	Доверенность: рег. номер, период действия и статус Сертификат: серийный номер, период действия 04AFBF780037B0108D4C0703DE 291A40B2 с 06.07.2023 10:09 по 06.07.2024 10:09 GMT+03:00	Дата и время подписания 04.10.2023 15:49 GMT+03:00 Подпись соответствует файлу документа
-------------------------	---	---	--	---