READY FOR ASTRA

АСТРА

СЕРТИФИКАТ СОВМЕСТИМОСТИ

№28045/2025

Настоящим сертификатом ООО «РусБИТех-Астра» подтверждает работоспособность
и корректность совместного функционирования
системы управления базами данных Tantor Special Edition (очередное обновление 16.8)
с программным обеспечением

Программный комплекс для обнаружения и предотвращения утечек информации «Кибер Протего» – 10.5

компании ООО «Киберпротект»
на основании результатов совместных испытаний,
указанных в протоколе № 28045/2025.
Протокол является неотъемлемой частью сертификата.

tantor × КИБЕРПРОТЕКТ

25 апреля 2025 года

Директор департамента
сопровождения и сервисов
ООО «РусБИТех-Астра»

Алексей Трубочев

ПРОТОКОЛ № 28045/2025

проведения совместных испытаний программного обеспечения "Программный комплекс для обнаружения и предотвращения утечек информации Кибер Протего" версии 10.5.0.632 и программного изделия СУБД "Tantor SE" версии 16.8.0

г. Москва 14.04.2025

1 Предмет испытаний

1.1 В настоящем протоколе зафиксирован факт проведения в период с 11.04.2025 по 14.04.2025 совместных испытаний программного обеспечения "Программный комплекс для обнаружения и предотвращения утечек информации Кибер Протего" версии 10.5.0.632, разработанного ООО "Киберпротект", и программного изделия СУБД "Tantor SE" версии 16.8.0, 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 дистрибутива

Описание	**Наименование дистрибутива**	**MD5**	**Источник**
Файл программного пакета дистрибутива "Программный комплекс для обнаружения и предотвращения утечек информации Кибер Протего"	CyberProtegoServerInstaller-astra.tar	d871d1ae1c83d4c997bc158c1f814889	Сторона разработчика ПО
Файл программного пакета дистрибутива "Программный комплекс для обнаружения и предотвращения утечек информации Кибер Протего"	protego-rus-10.5.0-astra1.x86_64.deb	428d43f32e184709936d5f6d85e3b09a	Сторона разработчика ПО

Файл программного пакета дистрибутива СУБД "Tantor SE"	tantor-se-server-16_16.8.0_amd64.deb	5f4bef5e80f5f6b9367f661e2a332e69	Сторона разработчика ПО

3 Ход испытаний

3.1 В ходе проведения настоящих испытаний были выполнены проверки корректности совместного функционирования СУБД "Tantor SE" и "Программный комплекс для обнаружения и предотвращения утечек информации Кибер Протего" в объеме, указанном в Приложении 1.

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

4 Результаты испытаний

4.1 "Программный комплекс для обнаружения и предотвращения утечек информации Кибер Протего" корректно функционирует совместно с СУБД "Tantor SE".

5 Вывод

5.1 "Программный комплекс для обнаружения и предотвращения утечек информации Кибер Протего" версии 10.5.0.632 и СУБД "Tantor SE" версии 16.8.0 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. – начальник сектора, ООО "РусБИТех-Астра";

Плотников Д. В. – инженер, ООО "РусБИТех-Астра".

Приложение 1 к Протоколу № 28045/2025

Перечень проверок совместимости "Программный комплекс для обнаружения и предотвращения утечек информации Кибер Протего" и СУБД "Tantor SE"

№ п/п	Наименование проверки	Результат проверки
1.	Инициализация соединения с СУБД "Tantor SE"	Успешно
2.	Функциональное тестирование	Успешно

Приложение 2 к Протоколу № 28045/2025

Инструкция по интеграции "Программный комплекс для обнаружения и предотвращения утечек информации Кибер Протего" с СУБД "Tantor SE"

1 Настройка "Программный комплекс для обнаружения и предотвращения утечек информации Кибер Протего":

1.1 выполнить действия:

1.2 Перед установкой ПО "Программный комплекс для обнаружения и предотвращения утечек информации Кибер Протего" необходимо выполнить установку и настройку СУБД "Tantor SE".

1.3 Установить ПО согласно официальной документации.

1.4 Во время установки веб-консоли "Кибер Протего", на этапе установки параметров инициализации подключения к СУБД "Tantor SE", указать тип базы данных "PostgreSQL".

1.5 В случае использования СУБД "Tantor SE" в качестве базы данных событий, необходимо находясь в веб-консоли "Кибер Протего" перейти в меню "Настройки", после чего вызвать меню "Базы данных" и указать параметры подключения к СУБД "Tantor SE". Например:

В качестве параметра "Имя сервера" указать адрес устройства на котором работает СУБД "Tantor SE";

В качестве параметра "Порт" указать порт, на котором работает СУБД "Tantor SE";

В качестве параметра "Тип подключения" выбрать параметр «POSTGRESQL»;

В качестве параметров "Имя пользователя" и "Пароль" указать логин и пароль роли СУБД "Tantor SE", имеющей право на создание базы данных и таблиц.

В качестве параметра "Имя базы данных" указать произвольное название для базы данных.

Предварительное создание базы данных не требуется.

2 Настройка СУБД "Tantor SE":

2.1 выполнить действия:

2.2 Установить СУБД "Tantor SE" согласно официальной документации.

2.3 Средствами утилиты "psql" задать привилегированному пользователю СУБД "Tantor SE" "postgres" пароль. Например:

```
/opt/tantor/db/16/bin/psql -U postgres
```

ALTER ROLE postgres WITH PASSWORD 'postgres';

2.4 Изменить конфигурационные файлы "/var/lib/postgresql/tantor-se-16/data/pg_hba.conf" и "/var/lib/postgresql/tantor-se-16/data/postgresql.conf" для подключения к СУБД извне. Например, для разрешения всех подключений:

Добавить в конфигурационный файл "pg_hba.conf" следующую запись:

host all all 0.0.0.0/0 scram-sha-256

Открыть конфигурационный файл postgresql.conf и привести параметр listen_addresses к значению listen_addresses = '*'

Приложение 3 к Протоколу № 28045/2025

Описание стенда

1. СУБД "Tantor SE" запущенная в среде операционной системы специального назначения "Astra Linux Special Edition" РУСБ.10015-01 (очередное обновление 1.7) с установленным оперативным обновлением безопасности БЮЛЛЕТЕНЬ № 2024-0830SE17 (оперативное обновление 1.7.6) на ядре 6.1.90-1 generic.

2. "Программный комплекс для обнаружения и предотвращения утечек информации Кибер Протего" запущенный в среде операционной системы специального назначения "Astra Linux Special Edition" РУСБ.10015-01 (очередное обновление 1.7) с установленным оперативным обновлением безопасности БЮЛЛЕТЕНЬ № 2024-0830SE17 (оперативное обновление 1.7.6) на ядре 6.1.90-1 generic.

3. Агент "Программного комплекса для обнаружения и предотвращения утечек информации Кибер Протего" запущенный в среде операционной системы специального назначения "Astra Linux Special Edition" РУСБ.10015-01 (очередное обновление 1.7) с установленным оперативным обновлением безопасности БЮЛЛЕТЕНЬ № 2024-0830SE17 (оперативное обновление 1.7.6) на ядре 6.1.90-1 generic.

Приложение 4 к Протоколу № 28045/2025

Перечень используемых сокращений

СУБД – система управления базами данных;

ПО – программное обеспечение.