ПРОТОКОЛ № 30548/2025

проведения совместных испытаний программного обеспечения "BI.ZONE SIEM" версии 0.18.0 и операционной системы специального назначения "Astra Linux Special Edition" РУСБ.10015-01 (очередное обновление 1.7)

г. Москва 25.09.2025

1 Предмет испытаний

1.1 В настоящем протоколе зафиксирован факт проведения совместных испытаний в период с 24.09.2025 по 25.09.2025 программного обеспечения "BI.ZONE SIEM" версии 0.18.0 (далее – ПО), разработанного ООО "БИЗон", и операционной системы специального назначения "Astra Linux Special Edition" РУСБ.10015-01 (очередное обновление 1.7) с установленным оперативным обновлением безопасности БЮЛЛЕТЕНЬ № 2025-0319SE17 (оперативное обновление 1.7.7) (далее – Astra Linux SE 1.7.7), разработанной ООО "РусБИТех-Астра".

2 Объект испытаний

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

Таблица 1 – Дистрибутив и документация ПО

Описание	**Наименование**	**MD5**	**Источник**
Файл архива, содержащий файлы ПО	bz-siem.0.18.0.linux.amd64.tar.gz	959f6b7e6955b9c71b0eac4e8a895773	Сторона разработчика ПО
Файл архива, содержащий файлы конфигурации ПО	siem_min_conf.zip	bf2536f72dc2b6dad535abd44d1fc468	Сторона разработчика ПО
Официальное руководство по эксплуатации ПО в электронном формате	bz-siem.pdf	–	Сторона разработчика ПО

3 Ход испытаний

3.1 В ходе проведения настоящих испытаний были выполнены проверки ПО в среде Astra Linux SE 1.7.7 в объеме, указанном в Приложении 1.

3.2 Перечень используемых репозиториев приведен в Приложении 2.

3.3 Предоставленный на испытания дистрибутив ПО не содержит электронную цифровую подпись для функционирования в среде операционной системы с активным режимом ЗПС.

3.4 Проверка корректности функционирования ПО с уровнем конфиденциальности 1-3 механизма мандатного разграничения доступа не проводилась по причине отсутствия поддержки ПО соответствующей функциональности ОС. Информация об отсутствии упомянутой поддержки была заявлена стороной разработчика ПО.

4 Вывод

4.1 "BI.ZONE SIEM" версии 0.18.0 функционирует в среде операционной системы специального назначения "Astra Linux Special Edition" РУСБ.10015-01 (очередное обновление 1.7) уровень защищенности "базовый" и признано совместимым, принимая во внимание информацию, содержащуюся в разделе 3.

5 Состав рабочей группы и подписи сторон

5.1 Данный протокол составлен участниками рабочей группы:

Васюков А. В. – Начальник отдела разработки решений для сбора и анализа информации о событиях безопасности, ООО "БИЗон";

Еремин Е. О. – Ведущий аналитик систем сбора и анализа информации о событиях безопасности, ООО "БИЗон".

ООО "БИЗон"

Начальник отдела разработки решений для сбора и анализа информации о событиях безопасности

(должность)

(подпись)

Васюков А. В.

(фамилия, инициалы)

Приложение 1 к Протоколу № 30548/2025

Перечень проверок совместимости ПО и Astra Linux SE 1.7.7

Таблица 1.1 - Результаты проверок ПО

Перечень проверок	**Версия ядра**								**Статус механизмов безопасности в процессе выполнения проверки**		
	5.4.0-202-generic	**5.4.0-202-hardened**	**5.10.233-1-generic**	**5.10.233-1-hardened**	**5.15.0-127-generic**	**5.15.0-127-hardened**	**5.15.0-127-lowlatency**	**6.1.124-1-generic**	**ЗПС**	**МКЦ**	**МРД**
Установка ПО	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Неактивен	Активен	Активен
Эксплуатация ПО	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Неактивен		
Удаление ПО	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Неактивен		
Эксплуатация ПО. Уровень конфиденциальности 1-3	Не проводилась	Не проводилась	Не проводилась	Не проводилась	Не проводилась	Не проводилась	Не проводилась	Не проводилась	Неактивен		

Приложение 2 к Протоколу № 30548/2025

Инструкция по установке и удалению ПО

1 Используемые репозитории в Astra Linux SE 1.7.7:

- deb https://dl.astralinux.ru/astra/frozen/1.7_x86-64/1.7.7/repository-base/ 1.7_x86-64 main contrib non-free

2 Установка ПО:

2.1 Распаковать архивы bz-siem.0.18.0.linux.amd64.tar.gz и siem_min_conf.zip

2.2 Выполнить копирование исполняемых файлов bz-collector и bz-correlator в директории /opt/bi.zone/siem/collector и /opt/bi.zone/siem/correlator соответственно.

2.3 Скопировать минимальную конфигурацию в директории siem из состава siem_min_conf.zip в директорию /etc/bi.zone/siem.

2.4 Создать директории /var/log/bi.zone/siem/collector и /var/log/bi.zone/siem/correlator, выдать на них права записи для пользователя, запускающего SIEM.

3 Удаление ПО:

3.1 Удалить директории /opt/bi.zone/siem, /etc/bi.zone/siem, /var/log/bi.zone/siem.

Приложение 3 к Протоколу № 30548/2025

Перечень используемых сокращений

Astra Linux SE 1.7.7 – операционная система специального назначения "Astra Linux Special Edition" РУСБ.10015-01 (очередное обновление 1.7) с установленным оперативным обновлением безопасности БЮЛЛЕТЕНЬ № 2025-0319SE17 (оперативное обновление 1.7.7);

РКСЗ - Документ из состава эксплуатационной документации Astra Linux SE 1.7.7, Руководство по КСЗ. Часть 1;

ОС — операционная система;

ЗПС – замкнутая программная среда;

МКЦ – мандатный контроль целостности;

МРД – мандатное управление доступом;

ПО – программное обеспечение "BI.ZONE SIEM" версии 0.18.0.