

ПРОТОКОЛ № 30547/2025

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 1.8)

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 1.8) с установленным оперативным обновлением безопасности БЮЛЛЕТЕНЬ № 2025-0811SE18 (оперативное обновление 1.8.3) (далее – Astra Linux SE 1.8.3), 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 1.8.3 в объеме, указанном в Приложении 1.

3.2 Перечень используемых репозиторий 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 1.8) 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)

Перечень проверок совместимости ПО и Astra Linux SE 1.8.3

Таблица 1.1 - Результаты проверок ПО

Перечень проверок	Версия ядра		Статус механизмов безопасности в процессе выполнения проверки		
	6.1.141-1-generic	6.12.34-1-generic	ЗПС	МКЦ	МРД
Установка ПО	Успешно	Успешно	Неактивен	Активен	Активен
Эксплуатация ПО	Успешно	Успешно	Неактивен		
Удаление ПО	Успешно	Успешно	Неактивен		
Эксплуатация ПО. Уровень конфиденциальности 1-3	Не проводилась	Не проводилась	Неактивен		

Инструкция по установке и удалению ПО

1 Используемые репозитории в Astra Linux SE 1.8.3:

- deb https://dl.astralinux.ru/astra/frozen/1.8_x86-64/1.8.3/main-repository/ 1.8_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 директорию /opt/bi.zone/siem/collector и /opt/bi.zone/siem/correlator соответственно.

2.3 Скопировать минимальную конфигурацию в директорию 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.

Перечень используемых сокращений

Astra Linux SE 1.8.3 - операционная система специального назначения "Astra Linux Special Edition" РУСБ.10015-01 (очередное обновление 1.8) с установленным оперативным обновлением безопасности БЮЛЛЕТЕНЬ № 2025-0811SE18 (оперативное обновление 1.8.3);

PKC3 - Документ из состава эксплуатационной документации Astra Linux SE 1.8.3, Руководство по KC3. Часть 1;

KC3 - комплекс средств защиты;

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.