Угрозы безопасности информации, которые могут быть нейтрализованы функционалом сертифицированной версии Deckhouse Platform		
№ п.п.	**Реализованная в СЗИ Deckhouse функция безопасности информации**	**Угроза безопасности, от которой Изделие обеспечивает защиту**
1.	изоляция контейнеров	УБИ.007: Угроза воздействия на программы с высокими привилегиями УБИ.012: Угроза деструктивного изменения конфигурации/среды окружения программ УБИ.116: Угроза перехвата данных, передаваемых по вычислительной сети УБИ.088: Угроза несанкционированного копирования защищаемой информации - изоляция блочных устройств УБИ.090: Угроза несанкционированного создания учетной записи пользователя УБИ.093: Угроза несанкционированного управления буфером УБИ.099: Угроза обнаружения хостов УБИ.117: Угроза перехвата привилегированного потока УБИ.118: Угроза перехвата привилегированного процесса
2.	проверка корректности конфигурации контейнеров	УБИ.109 Угроза перебора всех настроек и параметров приложения УБИ.115: Угроза перехвата вводимой и выводимой на периферийные устройства информации УБИ.023: Угроза изменения компонентов информационной (автоматизированной) системы
3.	выявление уязвимостей в образах контейнеров	УБИ.192 Угроза использования уязвимых версий программного обеспечения
4.	контроль целостности контейнеров и их образов	УБИ. 023 Угроза изменения компонентов информационной (автоматизированной) системы
5.	регистрация событий безопасности	УБИ.214: Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации
6.	ролевой метод управления доступом	УБИ. 067 Угроза неправомерного ознакомления с защищаемой информацией УБИ. 179 Угроза несанкционированной модификации защищаемой информации УБИ. 187 Угроза несанкционированного воздействия на средство защиты информации