Акционерное общество «Инфозащита», ИНН/КПП 7719672244/770201001
129110, г. Москва, ул. Большая Переяславская, д. 46, стр. 2, этаж 4, помещ. I, ком. 8
+7 (495) 786-34-93, info@itprotect.ru, www.itprotect.ru

itprotect

Исх. № ИЗ-25/1121 от 27.08.2025 г.

**Информационное письмо**

АО «Инфозащита» информирует Вас о том, что 04.06.2025 в Банк данных угроз безопасности информации (bdu.fstec.ru), ведение которого осуществляется ФСТЭК России, внесены изменения и добавлены следующие угрозы безопасности информации:

- УБИ.227 Угроза модификации (подмены) образов контейнеров;
- УБИ.226 Угроза внедрения вредоносного программного обеспечения в контейнеры;
- УБИ.225 Угроза нарушения изоляции контейнеров;
- УБИ.224 Угроза нарушения целостности (подмены) контейнеров;
- УБИ.223 Угроза несанкционированного доступа к контейнерам, предоставляющего пользователям расширенные привилегии.

Перечисленные угрозы заключаются в возможности использования уязвимостей информационных (автоматизированных) систем, построенных с применением технологий контейнеризации.

В случае, если в информационных (автоматизированных) системах (ОКИИ, ИСПДн, ГИС и иных информационных и автоматизированных системах) не используются технологии контейнеризации, АО «Инфозащита» предлагает ответственным за обеспечение безопасности информационных (автоматизированных) систем рассмотреть приведенное в Приложении № 1 к настоящему информационному письму Заключение по результатам анализа угроз безопасности информации. Заключение по результатам анализа угроз безопасности информации может быть приложено к разработанным ранее в организации моделям угроз безопасности информации в качестве свидетельства рассмотрения указанных выше угроз.

В случае использования технологий контейнеризации в информационных (автоматизированных) системах организации, АО «Инфозащита» предлагает ответственным за обеспечение безопасности ПДн, а также ответственным за организацию обработки ПДн рассмотреть приведенное в Приложении № 2 к настоящему информационному письму дополнение к разработанным ранее Моделям угроз.

С уважением,

Генеральный директор А. В. Соколов

Акционерное общество «Инфозащита», ИНН/КПП 7719672244/770201001
129110, г. Москва, ул. Большая Переяславская, д. 46, стр. 2, этаж 4, помещ. I, ком. 8
+7 (495) 786-34-93, info@itprotect.ru, www.itprotect.ru

itprotect

**Приложение № 1**

## ЗАКЛЮЧЕНИЕ
## по результатам анализа угроз безопасности информации

АО «Инфозащита», рассмотрев следующие угрозы, включенные 04.06.2025 в Банк данных угроз безопасности информации (bdu.fstec.ru), ведение которого осуществляется ФСТЭК России в соответствии с подпунктом 21 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16.08.2004 №1085:

- УБИ.223 Угроза несанкционированного доступа к контейнерам, предоставляющего пользователям расширенные привилегии;
- УБИ.224 Угроза нарушения целостности (подмены) контейнеров;
- УБИ.225 Угроза нарушения изоляции контейнеров;
- УБИ.226 Угроза внедрения вредоносного программного обеспечения в контейнеры;
- УБИ.227 Угроза модификации (подмены) образов контейнеров,

считает, что в случае, если в информационной (-ых) системе (-ах) не используются технологии контейнеризации, то вышеперечисленные угрозы являются неприменимыми к данной (-ым) системе (-ам) и, следовательно, являются неактуальными.

Генеральный директор А. В. Соколов

Акционерное общество «Инфозащита», ИНН/КПП 7719672244/770201001
129110, г. Москва, ул. Большая Переяславская, д. 46, стр. 2, этаж 4, помещ. I, ком. 8
+7 (495) 786-34-93, info@itprotect.ru, www.itprotect.ru



**Приложение № 2**

## ЗАКЛЮЧЕНИЕ
## по результатам анализа угроз безопасности информации

АО «Инфозащита», рассмотрев следующие угрозы, включенные 04.06.2025 в Банк данных угроз безопасности информации (bdu.fstec.ru), ведение которого осуществляется ФСТЭК России в соответствии с подпунктом 21 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16.08.2004 №1085:

- УБИ.223 Угроза несанкционированного доступа к контейнерам, предоставляющего пользователям расширенные привилегии;
- УБИ.224 Угроза нарушения целостности (подмены) контейнеров;
- УБИ.225 Угроза нарушения изоляции контейнеров;
- УБИ.226 Угроза внедрения вредоносного программного обеспечения в контейнеры;
- УБИ.227 Угроза модификации (подмены) образов контейнеров,

считает, что в случае, если в информационной (-ых) системе (-ах) используются технологии контейнеризации, то необходимо выполнить анализ актуальности вышеперечисленных угроз.

В качестве исходных данных для анализа актуальности вышеперечисленных угроз используются:

- характеристика и потенциал актуальных нарушителей безопасности информации (источников угроз);
- актуальные способы реализации угроз;
- возможные негативные последствия от реализации (возникновения) угроз безопасности информации.

1. В случае, если в качестве актуальных источников угроз не определены «Внешний нарушитель со средним потенциалом» или «Внутренний нарушитель со средним потенциалом», то следующие угрозы признаются невозможным с формулировкой «Отсутствует нарушитель, способный реализовать угрозу»:

- УБИ.224 Угроза нарушения целостности (подмены) контейнеров;
- УБИ.226 Угроза внедрения вредоносного программного обеспечения в контейнеры;
- УБИ.227 Угроза модификации (подмены) образов контейнеров.

2. Следующие угрозы признаются невозможным с формулировкой «Отсутствуют способы реализации угрозы» в случае, если в качестве актуальных способов реализации угроз не определены:

- «Использование уязвимостей:
  - УБИ.225 Угроза нарушения изоляции контейнеров;
  - УБИ.227 Угроза модификации (подмены) образов контейнеров;

- «Использование уязвимостей» или «Внедрение вредоносного ПО»:
  - УБИ.223 Угроза несанкционированного доступа к контейнерам, предоставляющего пользователям расширенные привилегии;
  - УБИ.226 Угроза внедрения вредоносного программного обеспечения в контейнеры;
- «Использование уязвимостей» или «Установка программных и (или) аппаратных закладок»:
  - УБИ.224 Угроза нарушения целостности (подмены) контейнеров.

3. В случае, если в качестве возможных негативных последствий от реализации (возникновения) угроз безопасности информации не определены последствия связанные с нарушением конфиденциальности информации, то угроза «УБИ.225 Угроза нарушения изоляции контейнеров» признаются невозможной с формулировкой «Отсутствуют негативные последствия от реализации (возникновения) угрозы».

Возможные угрозы безопасности информации признаются актуальными в случае наличия сценариев их реализации и включаются в перечень актуальных угроз.

Генеральный директор А. В. Соколов