ИНФОРМАЦИОННОЕ СООБЩЕНИЕ
о повышении безопасности средств защиты информации, в состав которых разработчики включают средства контейнеризации или образы контейнеров

Изготовители при разработке средств защиты информации от несанкционированного доступа включают в их состав средства контейнеризации или образы контейнеров, применение которых влияет на эффективность использования и безопасность таких средств защиты информации (далее — средства, средства в контейнерном исполнении), связанные с наличием в средствах контейнеризации избыточных полномочий, отсутствием учета и инвентаризации образов контейнеров и программного обеспечения, входящего в состав образов контейнеров, а также контроля целостности образов контейнеров.

В целях повышения безопасности средств в контейнерном исполнении изготовителям при разработке и сертификации необходимо:

1. В случае если средство контейнеризации не входит в состав средства в контейнерном исполнении и используется в качестве среды его функционирования, такое средство контейнеризации должно быть сертифицировано на соответствие Требованиям к средствам контейнеризации, утвержденным приказом ФСТЭК России от 4 июля 2022 г. № 118.

2. Разработчик средства должен провести инвентаризацию образов контейнеров, входящих в средство, а также программного обеспечения из состава образов контейнеров. Перечень образов контейнеров должен быть приведен в проектной документации на средство, оформленный в табличной форме и в машиночитаемом формате в соответствии с приложениями к настоящему порядку, при представлении в ФСТЭК России заявки на сертификацию в соответствии с пунктом 20 Положения о системе сертификации средств защиты информации, утвержденного приказом ФСТЭК России от 3 апреля 2018 г. № 55.

3. В средстве должна обеспечиваться целостность образов контейнеров и исполняемых файлов, содержащихся в контейнерах средства. При этом как минимум средство должно обеспечить контроль целостности образов

контейнеров и исполняемых файлов, содержащихся в контейнерах средства, при установке или по требованию (периодически в ходе эксплуатации средства).

Контроль целостности образов контейнеров и исполняемых файлов, осуществляется средством самостоятельно, с использованием средства контейнеризации или сертифицированного средства контроля целостности. Методика проверки контроля целостности должна быть приведена в эксплуатационной документации средства.

4. Разработчик средства в контейнерном исполнении должен обеспечить совместимость программного обеспечения, входящего в состав образов контейнеров, с хостовыми операционными системами, указанными в эксплуатационной документации средства в качестве среды функционирования.

5. Средство в контейнерном исполнении должно обеспечить запуск контейнеров с полномочиями, минимально необходимыми для функционирования средства на уровне процессов хостовой операционной системы. Избыточные полномочия компонентов, выявленные при проведении сертификации средства, должны быть устранены.

6. Средство контейнеризации с функцией централизованного управления контейнерами (далее — оркестратор), должно обеспечить управление доступом между компонентами средства (контейнерами, микросервисами, иными ресурсами, характерными для выбранного типа оркестратора), компонентами среды функционирования, внешними по отношению к средству компонентами в соответствии с заданными разработчиком средства правилами.

Заданные разработчиком средства правила должны содержать список действий, разрешенных при взаимодействии компонентов средства (контейнеров, микросервисов, иных ресурсов, характерных для выбранного типа оркестратора) между собой, компонентами среды функционирования, внешними по отношению к средству компонентами.

Избыточные разрешающие правила доступа к компонентам средства, выявленные при проведении сертификации средства, должны быть устранены.

Правила доступа, содержащие список действий, разрешенных при взаимодействии компонентов средства между собой и компонентами среды функционирования, должны быть описаны в документации средства.

Первый заместитель директора В.Лютиков

Приложение № 1

Табличная форма перечня образов контейнеров

№ п/п	Наименование образа контейнера	Назначение	Перечень программного обеспечения входящего в состав образа контейнера	Принадлежность контейнеров, создаваемых из этого образа, к поверхности атаки и (или) к контейнерам, реализующим функции безопасности

Приложение № 2

Пример перечня образов контейнеров в табличной форме

№ п/п	Наименование образа контейнера	Назначение	Перечень программного обеспечения входящего в состав образа контейнера	Принадлежность контейнеров, создаваемых из этого образа, к поверхности атаки и (или) к контейнерам, реализующим функции безопасности
1	manager	Принятие решений о предоставлении доступа	romashka_manager, postgres	функция безопасности
2	gateway	Фильтрация поступающих запросов	romashka_gateway, nginx	функция безопасности, поверхность атаки

Приложение № 3

Форма перечня образов контейнеров в машиночитаемом формате

Перечень образов контейнеров в машиночитаемом формате представляется в нотации JSON[1] в виде JSON-объекта, содержащего поля, описанные в Таблице 1.

Таблица 1. Требования к полям корневого объекта перечня образов контейнеров в машиночитаемом формате.

Имя поля	Тип	Описание	Требования к наличию
bomFormat	JSON строка	Спецификация формата документа. Должно содержать значение «CycloneDX».	Обязательно
specVersion	JSON строка	Версия спецификации документа. Должно содержать значение «1.6».	Обязательно
serialNumber	JSON строка	Уникальный серийный номер документа, сгенерированный Разработчиком в соответствии с RFC-4122 [2]. Например, «urn:uuid:3e671687-395b-41f5-a30f-a58921a69b79»	Опционально
version	Целое число	Версия документа. Первоначальное значение — 1. При модификациях должна увеличиваться на 1.	Обязательно
metadata	JSON объект	Дополнительная информация о перечне и продукте. Требования к заполнению полей объекта описаны в таблице 2.	Обязательно
components	Массив объектов JSON	Список образов контейнеров, входящих в состав средства. Требования к заполнению полей объектов описаны в таблице 5.	Обязательно

Таблица 2. Требования к полям объекта, описывающего дополнительную информацию о перечне и продукте.

Имя поля	Тип	Описание	Требования к наличию
timestamp	JSON строка	Дата и время формирования перечня в формате ГОСТ Р 7.0.64-2018 (ИСО 8601:2004). Например, «2022-04-25T09:30:00Z»	Обязательно
component	JSON объект	Информация о продукте. Требования к заполнению полей объекта описаны в таблице 3.	Обязательно

1ISO/IEC 21778:2017 Информационная технология. Синтаксис обмена данными JSON

2RFC 4122 «A Universally Unique IDentifier (UUID) URN Namespace» https://www.rfc-editor.org/info/rfc4122

Таблица 3. Требования к полям объекта, описывающего информацию о продукте.

Имя поля	Тип	Описание	Требования к наличию
type	JSON строка	Описывает тип продукта. Допускается использовать следующие значения: application, framework, library, operating-system, device-driver, firmware. Данное поле является обязательным для совместимости со спецификацией CycloneDX, выбор типа компонента осуществляется по усмотрению разработчика.	Обязательно
name	JSON строка	Название продукта.	Обязательно
version	JSON строка	Версия продукта. Длина строки не должна превышать 1024 символа.	Обязательно
manufacturer	JSON объект	Информация об изготовителе продукта. Требования к заполнению полей объекта описаны в таблице 4.	Обязательно

Таблица 4. Требования к полям объекта, описывающего информацию об изготовителе продукта.

Имя поля	Тип	Описание	Требования к наличию
name	JSON строка	Название организации — изготовителя продукта.	Обязательно

Таблица 5. Требования к полям объекта, описывающего образ контейнера.

Имя поля	Тип	Описание	Требования к наличию
type	JSON строка	Описывает тип компонента. Должно содержать значение «container».	Обязательно
name	JSON строка	Наименование образа контейнера.	Обязательно
version	JSON строка	Версия компонента.	Обязательно
purl	JSON строка	Опциональный идентификатор компонента в формате Package URL [3].	Опционально

3«Package Uniform Resource Locator Specification» https://github.com/package-url/purl-spec

properties	Массив объектов JSON	Массив объектов, описывающих свойства компонента. Требования к заполнению полей объектов описаны в таблице 6. Среди элементов массива обязательно должны присутствовать объекты со свойствами GOST:attack_surface и GOST:security_function.	Обязательно
components	Массив объектов JSON	Список программного обеспечения, входящего в состав образа контейнера. Требования к заполнению полей объектов описаны в таблице 7.	Обязательно

Таблица 6. Требования к полям объекта, описывающего свойства компонентов.

Имя поля	Тип	Описание	Требования к наличию
name	JSON строка	Название свойства компонента.	Обязательно
value	JSON строка	Значение свойства компонента. Если поле name имеет значение GOST:attack_surface, то поле value должно содержать одно из трёх значений: yes — в случае, если подпрограммы (функции) компонента реализуют программный интерфейс, который непосредственно доступен потенциальному нарушителю или входные данные которого потенциальный нарушитель способен гарантированно сформировать определенным образом. indirect — в случае, если подпрограммы (функции) компонента реализуют программный интерфейс, на входные данные которого потенциальный нарушитель способен целенаправленно повлиять, но это влияние существенно ограничено теми или иными факторами. no — в противном случае. Если поле name имеет значение GOST:security_function, то поле value должно содержать одно из трёх значений: yes — если функции компонента непосредственно реализуют функции безопасности средства защиты информации (например принимают решение по возможности доступа субъекта к объекту; принимают решение о принадлежности анализируемого объекта к классу (например вредоносного ПО, вредоносного трафика);	Обязательно

		формируют и осуществляют запись сведений о событиях в журнал; управляют функционалом безопасности ядра ОС и процессора, предоставляющим возможности виртуализации и т. п.). indirect — если функции компонента участвуют в реализации функций безопасности средства защиты информации, взаимодействуя с компонентами, реализующими функции безопасности средства защиты информации (например, осуществляя различные виды обработки/подготовки данных, выделение структур данных из массива байт, выполнение вычислений над значениями аргументов функции и т. п.), но при этом не принимают непосредственных решений о запуске, остановке, изменении режимов и параметров работы компонентов, реализующих функции безопасности. no — если функции компонента не участвуют в реализации функций безопасности средства защиты информации. Если поле name имеет значение GOST:provided_by, то поле value должно содержать название сертифицированного средства защиты информации, из состава которого заимствован данный компонент, при условии, что изготовитель указанного средства обеспечивает поддержку безопасности этого компонента.	

Таблица 7. Требования к полям объекта, описывающего программного обеспечения, входящее в состав образа контейнера.

Имя поля	Тип	Описание	Требования к наличию
type	JSON строка	Описывает тип компонента. Допускается использовать следующие значения: application, framework, library, container, platform, operating-system, device, device-driver, firmware, file, machine-learning-model, data, cryptographic-asset. Данное поле является обязательным для совместимости со спецификацией CycloneDX, выбор типа компонента осуществляется по усмотрению разработчика.	Обязательно
name	JSON строка	Наименование компонента.	Обязательно
version	JSON строка	Версия компонента.	Обязательно
purl	JSON строка	Опциональный идентификатор компонента в формате Package URL.	Опционально
properties	Массив объекто в JSON	Массив объектов, описывающих свойства компонента. Требования к заполнению полей объектов описаны в таблице 6. Среди элементов массива обязательно должны присутствовать объекты со свойствами GOST:attack_surface и GOST:security_function.	Обязательно
components	Массив объекто в JSON	Список подкомпонентов данного компонента. Допускается перечислять подкомпоненты как в массиве components родительского компонента, так и в массиве components корневого объекта перечня. Требования к заполнению полей объектов описаны в таблице 7.	Опционально

В JSON-объектах допускается наличие дополнительных полей, соответствующих спецификации CycloneDX, с информацией, заполняемой по желанию заявителя.

Приложение № 4

Пример заполнения перечня образов контейнеров


```
{
 "bomFormat": "CycloneDX",
 "specVersion": "1.6",
 "version": 1,
 "metadata": {
  "timestamp": "2024-11-25T00:00:00Z",
  "component": {
   "type": "application",
   "name": "Самый лучший межсетевой экран",
   "version": "72.15",
   "manufacturer": { "name": "ООО «Ромашка»" }
  }
 },
 "components": [
  {
   "type": "container",
   "name": "manager",
   "version": "3.0.0",
   "properties": [
    { "name": "GOST:attack_surface",    "value": "no" },
    { "name": "GOST:security_function", "value": "yes"},
   ],
   "components": [
    {
     "type": "library",
     "name": "romashka_manager",
     "version": "0.07",
     "properties": [
      { "name": "GOST:attack_surface",    "value": "no" },
      { "name": "GOST:security_function", "value": "yes"}
     ],
    },
    {
     "type": "library",
     "name": "postgres",
     "version": "16.4",
     "properties": [
      { "name": "GOST:attack_surface",    "value": "no" },
      { "name": "GOST:security_function", "value": "no"}
     ],
    }
   ]
  },
  {
   "type": "container",
   "name": "gateway",
   "version": "2.31.0",
   "properties": [
    { "name": "GOST:attack_surface",    "value": "yes" },
    { "name": "GOST:security_function", "value": "yes"}
   ],
   "components": [
    {
     "type": "application",
     "name": "romashka_gateway",
     "version": "0.07",
     "properties": [
      { "name": "GOST:attack_surface",    "value": "no" },
      { "name": "GOST:security_function", "value": "yes"}
```

```
        ],
       },
       {
        "type": "application",
        "name": "nginx",
        "version": "1.24.4",
        "properties": [
          { "name": "GOST:attack_surface",    "value": "yes" },
          { "name": "GOST:security_function", "value": "no"},
          { "name": "GOST:provided_by",       "value": "CertifiedDistribution"}
        ],
       }
     ]
    }
  ]
}
```