# **Домашнее задание**

|  |  |
| --- | --- |
| Дисциплина | «Разработка защищенных программных систем» |
| Тема | «Средства защиты DevOps инфраструктуры» |
| Форма проверки | **Самопроверка. Студент выполняет задание и самостоятельно проверяет его.**  *Совет: выполняйте домашнее задание сразу после изучения темы.* |
| Имя преподавателя |  |
| Время выполнения | 1.5–2 часа |
| Цель задания | Научиться работать со средствами защиты контейнеризации. |
| Инструменты для выполнения ДЗ | Docker, Kubernetes — в качестве инфраструктуры; Hadolint — для проверки Dockerfile, Trivy — для сканирования образов контейнеров на уязвимости, kube-bench — для сканирования конфигурации кластера Kubernetes. |
| Правила приёма работы | 1. Для выполнения задания создайте Google Документ и вносите в него информацию по каждому этапу.  2. Прикрепите ссылку на Google Документ.  **Важно:** убедитесь в том, что доступ по ссылке открыт.  Название файла должно содержать фамилию и имя студента, номер ДЗ (ДЗ по теме 5). |
| Чеклист самопроверки | **Задание считается выполненным, если** **реализованы следующие пункты:**   * скриншот вывода kube-bench о состоянии кластера Kubernetes, * скриншот вывода Hadolint о проверке Dockerfile до его правок и после, * скриншот отчёта Trivy о найденных уязвимостях образа, * \* скриншот окна браузера с веб-интерфейсом Pygoat.   **Задание не выполнено, если** **не реализован хотя бы один из пунктов:**   * скриншот вывода kube-bench о состоянии кластера Kubernetes, * скриншот вывода Hadolint о проверке Dockerfile до его правок и после, * скриншот отчёта Trivy о найденных уязвимостях образа. |
| Дедлайн | *Срок сдачи домашнего задания — 7 дней после вебинара. Рекомендуем выполнять домашнее задание сразу после вебинара.* |

**Задание**

К заданию приложен [архив с репозиторием приложения Pygoat](https://disk.360.yandex.ru/d/NWFpWF7TP71wCQ). Скачайте и распакуйте его.

1. В корне репозитория расположен Dockerfile, который содержит инструкции для сборки образа контейнера с этим приложением. С помощью Hadolint (<https://github.com/hadolint/hadolint>) выполните сканирование Dockerfile и исправьте ошибки в файле.
2. Соберите образ контейнера.
3. С помощью Trivy (<https://github.com/aquasecurity/trivy>) выполните сканирование образа на уязвимости.
4. Запустите кластер Kubernetes и с помощью kube-bench (<https://github.com/aquasecurity/kube-bench>) выполните сканирование кластера на соответствие CIS Benchmark.
5. Запустите контейнер Pygoat в Docker.
6. \*Запустите приложение Pygoat в кластере Kubernetes.