

Общество с ограниченной ответственностью
«Софт Плюс»

КРАТКОЕ ОПИСАНИЕ СИСТЕМЫ

Программы для ЭВМ

Система управления безопасной разработкой

Листов 11

2025

Содержание

1	Введение	3
1.1	Область применения.....	4
1.2	Краткое описание возможностей.....	4
2	Назначение и условия применения.....	4
2.1	Предмет автоматизации.....	4
2.2	Структура программного обеспечения.....	5
2.3	Варианты поставки Платформы заказчику.....	5
3	Подготовка к работе	6
4	Внедрение и обслуживание	6
4.1	Установка программного обеспечения Платформы	6
4.1.1	Установка на одну ноду с доступом к интернету.....	6
4.1.2	Установка на одну ноду в закрытом контуре	7
4.1.3	Развёртывание в среде kubernetes	7
4.2	Перечень оказываемых услуг в рамках сопровождения Системы	8
4.2	Требования к программному и аппаратному обеспечению при установке на одну ноду.....	8
4.3	Требования к программному обеспечению при установке в кластер kubernetes.....	10
4.4	Требования к техническому обеспечению.....	11

1 Введение

Программное обеспечение "Система управления безопасной разработкой" (далее – программное обеспечение, программа для ЭВМ, Система, ПЭВМ) правомерно введено в гражданский оборот на территории Российской Федерации, экземпляры программного обеспечения либо права использования программного обеспечения, услуги по предоставлению доступа к программному обеспечению свободно реализуются на всей территории Российской Федерации, отсутствуют ограничения, установленные в том числе иностранными государствами и препятствующие распространению или иному использованию программы для электронных вычислительных машин и базы данных на территории Российской Федерации или территориях отдельных субъектов Российской Федерации.

Сведения о программном обеспечении не составляют государственную тайну и программное обеспечение не содержит сведений, составляющих государственную тайну.

Исключительное право на программное обеспечение на территории всего мира и на весь срок действия исключительного права согласно свидетельству о государственной регистрации программы для ЭВМ № 2024684963 принадлежит ООО «СОФТ ПЛЮС».

Программное обеспечение не имеет принудительного обновления и управления из-за рубежа.

Гарантийное обслуживание, техническая поддержка и модернизация программного обеспечения в том числе модификация исходного текста программного обеспечения, осуществляются российской коммерческой организацией без преобладающего иностранного участия ООО «СОФТ ПЛЮС».

Технические средства хранения исходного текста и объектного кода программного обеспечения, а также технические средства компиляции исходного текста в объектный код программного обеспечения находятся на территории Российской Федерации.

Технические средства, необходимые для активации, выпуска, распространения, управления лицензионными ключами программного обеспечения находятся на территории Российской Федерации, контролируются российскими организациями.

Графический пользовательский интерфейс программного обеспечения реализован на русском языке.

1.1 Область применения

Платформа предназначена для сбора, ранжирования и управления информацией об уязвимостях и может быть интегрирована в SDLC заказчика. Является универсальным решением, которое агрегирует данные о безопасности из разных источников для работы с уязвимостями и ускоряет процесс тестирования безопасности, оптимизируя рабочий процесс SDLC.

Специалисты, которые проводят анализ информационных систем для обеспечения безопасности, выявления недостатков в системе безопасности, известные как “Синяя команда” (Blue Team), могут легко работать с выявленными проблемами, создавать задачи в СОЗО и отслеживать прогресс в реальном времени, а разработчики могут исправлять ошибки и обеспечивать безопасность продуктов.

1.2 Краткое описание возможностей

ПЭВМ "Система управления безопасной разработкой" обладает следующими возможностями:

- Импорт результатов сканирования из сторонних инструментов ИБ
- Анализ и нормализация импортированных данных из сторонних инструментов ИБ
- Поиск, анализ и приоритизация уязвимостей в исходном коде, библиотеках и зависимостях
- Поддержка инструментов CI/CD для автоматизации проверки безопасности на этапах разработки, тестирования и развертывания
- Контроль соответствия заданным критериям качества ПО
- Управление запуском сканирований сторонних инструментов ИБ

2 Назначение и условия применения

2.1 Предмет автоматизации

ПЭВМ Система управления безопасной разработкой предоставляет возможность автоматизации следующих задач:

- Импорта результатов сканирования из сторонних инструментов ИБ
- Поиска, анализа и приоритизации уязвимостей в исходном коде, библиотеках и зависимостях
- Контроля соответствия заданным критериям качества ПО
- Управления процессами информационной безопасности
- Запуска сканирований сторонних инструментов ИБ

2.2 Структура программного обеспечения

В таблице 1 приведён список компонентов и их основные функции.

Таблица 1 — список компонентов и их основные функции

Компонент	Функция
v_engine	Основная механика приложения
v_background	Сервис выполнения фоновых задач
v_scheduling	Сервис назначения расписания фоновых задач
v_orchestration	Сервис оркестрации сканеров
v_docker_proxy ⁽¹⁾	Сервис доступа к сервису docker с ограничением возможностей
v_files	Сервис обмена файловыми данными между компонентами
v_deck	Сервис предоставляющий пользовательский интерфейс и ssl терминирование при необходимости
postgres ⁽²⁾	Реляционная СУБД PostgreSQL
redis ⁽²⁾	in-memory NoSQL база данных. Используется как в качестве кеша, так и для взаимодействия engine и background

Примечания:

1. Компонент v_docker_proxy используется только для варианта инсталляции на одну ноду.
2. Компоненты postgres и redis, как указано выше, обычно используются внешние. Но могут быть развёрнуты вместе с остальными. Для варианта инсталляции на одну ноду это опция по умолчанию.

2.3 Варианты поставки Платформы заказчику

Платформа предполагает развёртывание в инфраструктуре заказчика при помощи одного

из двух вариантов:

- инсталляция на одной физической или виртуальной машине (далее – ноде) при помощи дистрибутивного пакета, представляющего собой самораспаковывающийся архив с инсталлятором;
- развёртывание в среде kubernetes при помощи helm chart.

При инсталляции на одной машине при помощи дистрибутивного пакета так же есть два варианта инсталляции:

- установка с доступом в интернет;
- установка без доступом в интернет.

3 Подготовка к работе

Перед началом работы с ПЭВМ Система управления безопасной разработкой необходимо ознакомится с руководством администратора и руководством пользователя. В соответствии с описанными там опциями произвести настройку ПЭВМ Система управления безопасной разработкой с учетом вашего окружения и решаемых задач.

4 Внедрение и обслуживание

4.1 Установка программного обеспечения Платформы

4.1.1 Установка на одну ноду с доступом к интернету

Что бы начать инсталляцию, скачайте установщик на целевую машину: https://hexway.io/wp-content/uploads/12059/install_hw_vmp_en-US_0.64.0.run

Выполните команду с правами `root`:

```
bash ./install_hw_vmp_en-US_0.64.0.run
```

В процессе инсталляции необходимо принять пользовательское соглашение. Для этого нажмите Y.

После завершения установки вы получите следующее сообщение:

```
hexway Vampy is ready to use.  
UI accessible on http://0.0.0.0 or https://0.0.0.0  
Login as '<username>' password: '<password>'
```

Откройте интерфейс Платформы в браузере по адресу: `http://<ip-server>/` или `http://<your-domain-name>/`. Логин по умолчанию для администратора: `root@ro.ot`. Пароль смотрите в сообщении выше.

После окончания установки может потребоваться дополнительная настройка Платформы, которую можно произвести в файле `/opt/hw-vmp/config/user.ini`. В файле `/opt/hw-vmp/config/user-template.ini` перечислены все опции, которые можно использовать для настройки.

4.1.2 Установка на одну ноду в закрытом контуре

Описать инсталляцию

Что бы начать инсталляцию, скачайте установщик на целевую машину: https://hexway.io/wp-content/uploads/12059/install_offline_hw_vmp_en-US_0.64.0.run

Выполните команду с правами `root`:

```
bash ./install_offline_hw_vmp_en-US_0.64.0.run
```

В процессе инсталляции необходимо принять пользовательское соглашение. Для этого нажмите Y.

После завершения установки вы получите следующее сообщение:

```
hexway Vampy is ready to use.  
UI accessible on http://0.0.0.0 or https://0.0.0.0  
Login as '<username>' password: '<password>'
```

Откройте интерфейс Платформы в браузере по адресу: `http://<ip-server>/` или `http://<your-domain-name>/`. Логин по умолчанию для администратора: `root@ro.ot`. Пароль смотрите в сообщении выше.

После окончания установки может потребоваться дополнительная настройка Платформы, которую можно произвести в файле `/opt/hw-vmp/config/user.ini`. В файле `/opt/hw-vmp/config/user-template.ini` перечислены все опции, которые можно использовать для настройки.

4.1.3 Развёртывание в среде kubernetes

Перед началом развёртывания в среде kubernetes требуется получить:

- `kubectl` и `helm` установленные на локальной машине;
- конфигурацию kubernetes кластера для доступа к ней через `kubectl`.

Шаги развёртывания:

1. Для получения `helm chart` выполните:

```
helm pull oci://registry.hexway.io/charts/vampy --version 0.64.0 --untar
```
2. Откройте файл `vampy/values.yaml` для изучения имеющихся опций.

3. Измените значения требуемых опций в этом же файле или, предпочтительно создайте новый файл.
4. Примените шаблон helm при помощи, например, такой команды:
`helm install vampu --values vampu/values.yaml --values my.yml`

4.2 Перечень оказываемых услуг в рамках сопровождения Системы

Техническая поддержка пользователей Системы по вопросам установки, переустановки, администрирования и эксплуатации осуществляется по электронной почте. В рамках технической поддержки Системы оказываются следующие услуги:

- помощь в установке Системы;
- помощь в настройке и администрировании;
- помощь в установке обновлений Системы;
- устранение неисправностей, выявленных в ходе эксплуатации;
- помощь в поиске и устранении проблем в случае некорректной установки обновления Системы;
- пояснение функционала модулей Системы, помощь в эксплуатации;
- предоставление актуальной документации по установке/настройке/работе Системы;
- общие консультации по выбору серверного программного обеспечения для обеспечения более высокой производительности работы Системы.

Неисправности, выявленные в ходе эксплуатации Системы, могут быть исправлены следующими способами:

- автоматическая перезагрузка компонентов Системы;
- обновление компонентов Системы;
- работа специалиста службы технической поддержки по запросу пользователя.

Техническая поддержка Системы предоставляется в соответствии с действующими правилами компании и осуществляется специалистами ООО «СОФТ ПЛЮС».

4.2 Требования к программному и аппаратному обеспечению при установке на одну ноду

При инсталляции на одной машине требуется:

- подготовить машину, удовлетворяющую минимальным системным требованиям;
- установить на неё одну из поддерживаемых ОС;
- установить на неё требуемое ПО.

Минимальные системные требования:

- RAM: 4GB
- CPU: 2 core
- Скорость диска: 100 IOps
- Место на диске: 20GB

Платформа поддерживает установку на следующие операционные системы:

- CentOS 8
- RHEL 8
- RedOS 7.3
- Ubuntu 20.04
- Ubuntu 22.04
- Ubuntu 24.04
- Debian 11
- Debian 12
- Astra Linux Орёл 1.7
- другие ОС, совместимые с указанными выше.

Примечание: некоторые дистрибутивы Linux в минимальной установке могут не включать некоторые из следующих утилит: curl, find, groupadd, tar, gzip, useradd, xargs. Однако эти утилиты используются в инсталляторе и скриптах обслуживания. В случае использования стандартных установок проблем с этими утилитами не возникает. Поэтому, мы рекомендуем использовать стандартную серверную версию указанных выше ОС или установить указанные утилиты.

Установите docker engine (<https://docs.docker.com/engine/install/>), включая docker compose plugin (<https://docs.docker.com/compose/install/linux/>) на вашу машину (устанавливается по умолчанию, если пользуетесь инструкцией по предыдущей ссылке).

Примечания:

- `docker from snap` на данный момент не поддерживается.
- `docker -compose` версии 1.x не поддерживается.
- `docker` установленный из пакетного менеджера вашего дистрибутива ОС может работать, а может не работать. Поэтому, мы рекомендуем устанавливать `docker` с `docker.com` если это возможно, однако, для некоторых ОС это вызывает сложности. См. ниже что бы узнать об известных проблемах и возможных путях их решения.
- `docker-compose standalone` поддерживается, но не рекомендуется. Используйте его только в том случае, если нет возможности установить `docker compose` именно как `plugin` к `docker`.

Известные проблемы при использовании `docker` и `docker compose plugin` из репозитория ОС, вместо `docker.com`:

- В репозиториях многих ОС есть только `docker-compose 1.x` который не поддерживается Платформой. Для установки `docker compose plugin` воспользуйтесь инструкцией со страницы `Install the plugin manually` (<https://docs.docker.com/compose/install/standalone/>), но обратите внимание, на пометки for **all users**. Если плагин будет установлен только текущего пользователя, даже если это будет `root`, запустить платформу корректно невозможно.
- В репозиториях некоторых ОС `docker` после установки не стартует автоматически или не создаёт `docker socket`. В этих случаях его нужно запустить вручную.

4.3 Требования к программному обеспечению при установке в кластер `kubernetes`

Для установки в кластер `kubernetes` для промышленной эксплуатации необходимо подготовить кластер, включающий не менее трёх рабочих нод для обеспечения высокой доступности. Требования к кластеру указаны ниже:

- `Kubernetes`: 1.29+
- `CNI`: любой
- `CRI`: любой
- `Linux Kernel`: 5.13+
- Внешний `Postgresql` версии 16+ (опционально, но рекомендуется)
- Внешний `Redis` версии 7.x (опционально, но рекомендуется)

- Внешнее хранилище, обеспечивающее доступ в режиме ReadWriteMany для постоянного хранения данных.

Примечания:

- PostgreSQL и Redis могут быть развернуты как часть Платформы, однако, рекомендуется использовать управляемые провайдером СУБД или кластера развернутые заказчиком самостоятельно.

4.4 Требования к техническому обеспечению

В таблице 2 указано минимальное количество реплик для промышленной эксплуатации. Точное количество реплик определяется нагрузкой у конкретного заказчика.

Таблица 2 — минимальное количество реплик для промышленной эксплуатации

Компонент	Количество реплик	Request	Limits
v_engine	3	500m / 512Mi	2 / 2Gi
v_background	3	500m / 512Mi	2 / 2Gi
v_scheduling	3	500m / 512Mi	2 / 2Gi
v_orchestration	3	500m / 512Mi	2 / 2Gi
v_docker_proxy	1 ⁽¹⁾	50 / 128Mi	2 / 2Gi
v_files	3	500m / 512Mi	1 / 1Gi
v_deck	3	50 / 128Mi	2 / 2Gi
postgres	1 ⁽²⁾	500m / 512Mi	2 / 2Gi
redis	1 ⁽²⁾	50m / 128Mi	2 / 2Gi

Примечания:

1. Компонент v_docker_proxy используется только для варианта инсталляции на одну ноду.
2. Компоненты postgres и redis, как указано выше, обычно используются внешние. Но могут быть развернуты вместе с остальными. Для варианта инсталляции на одну ноду это опция по умолчанию. В случае использования внешних БД postgres и redis для них требуется быстрое хранилище. Объем и характеристики сервера и хранилища зависят от объема данных, которые предполагается обрабатывать.

3. В случае инсталляции на одну ноду все компоненты имеют только одну реплику.