МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
И.о. директора института
перспективной инженерии канд.
техн. наук, доцент Порохня А.А.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ
Безопасность жизненного цикла

Направление подготовки	09.04.04 Программная инженерия
Направленность (профиль)	Разработка, мониторинг и управление жизненным циклом инженерных систем
Год начала обучения	2026
Форма обучения	очная
Реализуется в семестре	3

Введение

Назначение: ФОС предназначен для объективной оценки уровня сформированности компетенций.

ФОС является приложением к программе дисциплины «Безопасность жизненного цикла».

Разработчик Е.Н. Новикова, к.ф.-м.н., доцент, заведующий межинститутский базовой кафедрой департамента цифровых, робототехнических систем и электроники.

Проведена экспертиза ФОС.

Председатель Новикова Е.Н., межинститутской базовой кафедры департамента цифровых, робототехнических систем и электроники института перспективной инженерии

Члены комиссии:

Азаров И.В., и.о. директора департамента цифровых, робототехнических систем и электроники института перспективной инженерии

Николаев Е. И., доцент департамента цифровых, робототехнических систем и электроники института перспективной инженерии

Представитель организации-работодателя:

Руководитель группы разработки А.А. Шипулин, ООО «Стилсофт».

Экспертное заключение: ФОС по дисциплине позволяет оценить уровень сформированности компетенций. Приступить к апробации.

Срок действия ФОС определяется сроком реализации образовательной программы.

1. **Описание критериев оценивания компетенции на различных этапах их формирования, описание шкал оценивания**

Уровни сформированности компетенций, индикаторов	Дескрипторы			
	Минимальный уровень не до- стигнут (Неудовлетвори-тельно) 2 балла	Минимальный уровень (удовлетвори-тельно) 3 балла	Средний уро- вень (хорошо) 4 балла	Высокий уро- вень (отлично) 5 баллов
ПК-8 - Способен интегрировать практики безопасности на всех этапах ЖЦ, включая статический и динамический анализ кода, анализ уязвимостей зависимостей, безопасность контейнеров и облачной инфраструктуры, обеспечивая непрерывное соответствие требованиям безопасности				
ИД-1$_{ПК-8}$ Внедряет инструменты статического анализа безопасности (SAST) в процесс разработки для автоматического выявления уязвимостей на этапе pull request'ов	Не знает инструментов SAST, не может объяснить принципы работы. Не выполняет лабораторные работы.	Знает Semgrep/Bandit, может запустить вручную. Понимает отчет, но не настраивает автоматизацию	Интегрирует SAST в CI/CD, настраивает базовые правила. Автоматизирует запуск, но не блокирует MR/PR.	Настраивает продвинутые правила SAST (кастомные), интегрирует в MR/PR с автоматической блокировкой слияния при HIGH-уязвимостях.
ИД-5пк-8 Сканирует конфигурации инфраструктуры как кода (IaC) на соответствие политикам безопасности и лучшим практикам	Не знает инструменты анализа IaC (Checkov/tfsec). Не выполняет лабораторные работы.	Знает Checkov, может запустить вручную. Понимает отчет, но не интегрирует в CI/CD.	Интегрирует Checkov в CI/CD, проверяет Terraform-код на соответствие CIS.	Разрабатывает кастомные политики для Checkov, интегрирует в terraform plan с блокировкой деплоя при нарушениях.
ИД-6пк-8 Интегрирует инструменты безопасности в CI/CD-пайплайны, настраивая автоматические шлюзы качества (quality gates)	Не понимает концепцию Quality Gates. Не может настроить остановку пайплайна	Понимает концепцию, но настраивает только простые проверки (например, наличие артефактов).	Настраивает Quality Gates на основе результатов SAST/SCA (блокировка при HIGH-уязвимостях).	Настраивает многоступенчатые Quality Gates на основе CVSS, Exploitability, Severity Score. Интегрирует с дефект-трекером.
ИД-7пк-8 Мониторит состояние безопасности контейнеров и инфраструктуры в рантайме, выявляя инциденты и аномальное поведение	Не знает инструменты runtime-безопасности (Falco). Не может выявить аномалии	Знает Falco, может установить и запустить базовые правила	Настраивает политики Falco для обнаружения запуска шелла или монтирования sensitive path.	Настраивает кастомные политики Falco, интегрирует с SIEM, настраивает автоматическую реакцию на инциденты.
ИД-8пк-8 Обеспечивает непрерывное соответствие (continuous compliance) через автоматизированный сбор доказательств и	Не знает OPA/Rego. Не может написать простую политику	Знает OPA, может запустить Conftest с готовыми политиками.	Пишет простые политики Rego (например, запрет latest-тегов).	Пишет сложные политики Rego для Cloud Custodian, настраивает автоматическую генерацию отчетов для аудита (152-ФЗ, ФСТЭК).

генерацию отчетов				
ПК-11 - Способен проводить анализ угроз кибербезопасности для автономных систем, проектировать и внедрять меры защиты на уровнях канала связи, бортового ПО, наземной инфраструктуры управления и цепочек поставок, обеспечивая целостность, конфиденциальность и доступность системы.				
ИД-1пк-11 Проводит анализ угроз кибербезопасности для автономных систем с использованием методологии STRIDE	Не знает методологию STRIDE, не может назвать типы угроз. Не строит DFD-диаграммы	Знает основные типы угроз STRIDE. Составляет простую модель угроз по шаблону.	Самостоятельно строит DFD-диаграмму, применяет STRIDE ко всем элементам.	Разрабатывает детальную модель угроз и нарушителя, оценивает риски по DREAD, предлагает меры защиты.
ИД-2пк-11 Проектирует меры защиты для каналов связи автономных систем на основе анализа уязвимостей протоколов (MAVLink, DDS)	Не знает протоколы MAVLink/DDS, их уязвимости. Не может проанализировать трафик.	Знает основные уязвимости (отсутствие шифрования, подмена пакетов). Может проанализировать трафик в Wireshark.	Настраивает аутентификацию и шифрование в MAVLink 2.0 (Signing) или DDS Security.	Проводит глубокий анализ защищенности, моделирует атаки (replay, MITM), настраивает комплексную защиту каналов связи.
ИД-3пк-11 Внедряет механизмы защиты бортового ПО, включая безопасную загрузку, изоляцию процессов и контроль целостности	Не знает концепции Secure Boot, изоляции процессов в ROS 2.	Знает базовые механизмы (SROS 2, AppArmor). Может включить готовые политики.	Настраивает SROS 2 для изоляции узлов, контролирует целостность компонентов.	Настраивает мандатный контроль доступа (SELinux), интегрирует с Secure Boot, разрабатывает политики безопасности для бортового ПО.
ИД-4пк-11 Обеспечивает безопасность цепочки поставок для автономных систем, анализируя уязвимости компонентов и зависимостей прошивок	Не знает инструменты SBOM и SCA. Не может выявить CVE в зависимостях.	Знает SBOM (CycloneDX, SPDX), может сгенерировать отчет.	Формирует SBOM для прошивки PX4/ArduPilot, выявляет CVE с помощью Trivy/Syft.	Разрабатывает политику управления уязвимостями для парка устройств, автоматизирует мониторинг цепочки поставок.
ИД-5пк-11 Внедряет механизмы безопасных массовых OTA-обновлений (по воздуху) бортового ПО, обеспечивающие надежность доставки, целостность, подлинность прошивок и защиту от отката версий	Не знает архитектуру OTA-обновлений, механизмы подписи и rollback protection.	Знает базовую архитектуру OTA, может сгенерировать подпись (Cosign/GPG) вручную.	Настраивает пайплайн подписанных OTA-обновлений, реализует верификацию подписи на симуляторе устройства.	Настраивает A/B-разделы, канареечные обновления, защиту от отката (rollback protection), автоматизирует rollout обновлений на парк устройств.

ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕРКИ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
3 семестр			
1	DevSecOps	Как называется подход, интегрирующий практики безопасности в DevOps-культуру на всех этапах жизненного цикла?	ПК-8 (ИД-1)
2	Shift Left	Как называется концепция, означающая «сдвиг безопасности влево» (перенос проверок безопасности на ранние этапы разработки)?	ПК-8 (ИД-1)
3	Semgrep, CodeQL (любой из них)	Назовите один из инструментов статического анализа безопасности кода (SAST).	ПК-8 (ИД-1)
4	False Positive	Как термин обозначает ситуацию, когда SAST-инструмент ошибочно помечает безопасный код как уязвимый?	ПК-8 (ИД-1)
5	Quality Gate	Как называется автоматический шлюз качества в CI/CD, который блокирует пайплайн при обнаружении критических уязвимостей?	ПК-8 (ИД-6)
6	CVSS	Какая система используется для оценки критичности уязвимостей (от 0 до 10)?	ПК-8 (ИД-6)
7	Checkov, tfsec (любой из них)	Назовите инструмент для статического анализа конфигураций инфраструктуры как кода (IaC).	ПК-8 (ИД-5)

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
3 семестр			
8	Trivy, Grype (любой из них)	Назовите инструмент для сканирования уязвимостей в Docker-образах.	ПК-8 (ИД-7)
9	Falco	Какой инструмент используется для runtime-безопасности контейнеров и обнаружения аномального поведения?	ПК-8 (ИД-7)
10	Pod Security Standards (PSA)	Как в Kubernetes называются стандарты безопасности подов (документ, определяющий политики baseline/restricted)?	ПК-8 (ИД-7)
11	SBOM (Software Bill of Materials)	Как называется документ, содержащий список всех компонентов и зависимостей программного продукта?	ПК-8 (ИД-8)
12	SPDX, CycloneDX (любой из них)	Назовите один из форматов представления SBOM.	ПК-8 (ИД-8)
13	Syft	Какой инструмент используется для генерации SBOM из контейнеров и файловых систем?	ПК-8 (ИД-8)
14	Cosign	Какой инструмент из экосистемы Sigstore используется для подписи и верификации артефактов?	ПК-8 (ИД-8)
15	Rego	На каком языке пишутся политики для Open Policy Agent (OPA)?	ПК-8 (ИД-8)
16	Conftest	Какой инструмент позволяет проверять конфигурационные файлы	ПК-8 (ИД-8)

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
3 семестр			
		(Kubernetes, Terraform) с помощью политик OPA?	
17	Cloud Custodian	Какой инструмент предназначен для автоматического отслеживания и исправления нарушений политик в облачных средах?	ПК-8 (ИД-8)
18	OWASP ZAP	Назовите инструмент для динамического анализа безопасности веб-приложений и API (DAST).	ПК-8
19	SCA (Software Composition Analysis)	Как называется процесс анализа сторонних библиотек и зависимостей на наличие известных уязвимостей?	ПК-8
20	OWASP Dependency-Check, Snyk (любой из них)	Назовите инструмент для анализа уязвимостей зависимостей (SCA).	ПК-8
21	SolarWinds, log4shell, 3CX (один пример)	Приведите один пример известной атаки на цепочку поставок программного обеспечения (supply chain attack).	ПК-8
22	152-ФЗ	Какой федеральный закон Российской Федерации регулирует вопросы защиты персональных данных?	ПК-8
23	ФСТЭК России	Какой орган государственной власти РФ осуществляет регулирование в области защиты государственной тайны и безопасности критической информационной инфраструктуры?	ПК-8

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
3 семестр			
24	STRIDE	Какая методология анализа угроз включает в себя следующие категории: Spoofing, Tampering, Repudiation, Information Disclosure, DoS, Elevation of Privilege?	ПК-11
25	DFD (Data Flow Diagram)	Какой тип диаграммы строится на первом этапе методологии STRIDE для идентификации элементов системы?	ПК-11
26	Spoofing	Какой тип угрозы в методологии STRIDE соответствует подмене субъекта или объекта (например, подмена GPS-сигнала дрона)?	ПК-11
27	Tampering	Какой тип угрозы в методологии STRIDE соответствует несанкционированному изменению данных (например, подмена телеметрии)?	ПК-11
28	Information Disclosure	Какой тип угрозы в методологии STRIDE соответствует несанкционированному раскрытию конфиденциальной информации (например, перехват телеметрии)?	ПК-11
29	Denial of Service (DoS)	Какой тип угрозы в методологии STRIDE соответствует нарушению доступности системы (например, глушение канала управления дроном)?	ПК-11

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
3 семестр			
30	Elevation of Privilege	Какой тип угрозы в методологии STRIDE соответствует повышению привилегий (например, получение контроля над полетным контроллером)?	ПК-11
31	DREAD	Какая методология используется для количественной оценки рисков (оценка ущерба, воспроизводимости, эксплуатируемости и т.д.)?	ПК-11
32	MAVLink	Как называется протокол связи, наиболее часто используемый для телеметрии и управления БПЛА?	ПК-11
33	Отсутствие шифрования, подмена пакетов, replay-атаки (один из вариантов)	Назовите одну из основных уязвимостей протокола MAVLink версии 1.	ПК-11
34	Signing (подпись пакетов)	Какой механизм безопасности был добавлен в протокол MAVLink версии 2 для защиты от подмены пакетов?	ПК-11
35	DDS (Data Distribution Service)	Какой протокол используется в ROS 2 для обеспечения обмена данными между узлами в распределенной системе?	ПК-11
36	DDS Security	Как называется подсистема ROS 2, обеспечивающая аутентификацию, шифрование и контроль доступа для DDS?	ПК-11

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
3 семестр			
37	Wireshark	Какой инструмент позволяет анализировать сетевой трафик протоколов MAVLink и DDS для выявления уязвимостей?	ПК-11
38	Replay Attack	Как называется тип атаки, при которой злоумышленник перехватывает и повторно передает легитимные команды управления дроном?	ПК-11
39	Man-in-the-Middle (MITM)	Как называется тип атаки, при которой злоумышленник внедряется в канал связи между дроном и наземной станцией?	ПК-11
40	Secure Boot	Как называется механизм, обеспечивающий проверку подлинности загрузчика и ядра операционной системы при старте бортового компьютера?	ПК-11
41	SROS 2	Как называется набор инструментов для обеспечения безопасности ROS 2 (изоляция узлов, аутентификация, шифрование)?	ПК-11
42	AppArmor, SELinux (любой из них)	Назовите один из механизмов мандатного контроля доступа (MAC), используемый для изоляции процессов в Linux.	ПК-11
43	OTA (Over-The-Air)	Как называется технология удаленной доставки и установки прошивок на устройства без физического подключения?	ПК-11

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
3 семестр			
44	Rollback protection	Как называется механизм защиты от установки старой уязвимой версии прошивки после выхода обновления?	ПК-11
45	A/B-разделы (A/B partitions)	Какая архитектура обновления предполагает наличие двух разделов (активного и резервного) для обеспечения атомарной установки и отката?	ПК-11
46	Canary update (канареечное обновление)	Как называется стратегия обновления, при которой новая прошивка сначала выкатывается на малую часть парка устройств (например, 5-10%)?	ПК-11
47	GPG (GNU Privacy Guard) или Cosign	Какой инструмент используется для криптографической подписи прошивок перед отправкой на устройства?	ПК-11
48	QGroundControl	Как называется популярная наземная станция управления (GCS) с открытым исходным кодом, используемая для настройки и управления БПЛА на прошивке PX4?	ПК-11
49	PX4 (или ArduPilot)	Назовите одну из популярных open-source прошивок для автопилотов БПЛА.	ПК-11
50	Gazebo	Какой симулятор наиболее часто используется для SITL-тестирования	ПК-11

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
3 семестр			
		БПЛА и робототехнических систем вместе с ROS и PX4?	
51	Б	Что означает концепция «Shift Left» в DevSecOps? А) Перенос тестирования на этап production Б) Сдвиг проверок безопасности на ранние этапы разработки В) Увеличение количества этапов в пайплайне Г) Замена ручного тестирования автоматическим	ПК-8
52	А, В	Какие инструменты относятся к SAST (статическому анализу безопасности)? (Выберите все верные) А) Semgrep Б) OWASP ZAP В) CodeQL Г) Trivy	ПК-8
53	В	Что такое Quality Gate в CI/CD? А) Автоматическое создание отчета о тестировании Б) Ручное подтверждение деплоя в production В) Условие (шлюз), блокирующее пайплайн при нарушении пороговых значений Г) Кэширование артефактов между запусками	ПК-8

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
3 семестр			
54	А, Б, В	Какие инструменты используются для статического анализа конфигураций IaC? (Выберите все верные) А) Checkov Б) tfsec В) TFLint Г) OWASP ZAP	ПК-8
55	Б	Что такое SBOM (Software Bill of Materials)? А) Инструмент для подписи артефактов Б) Спецификация всех компонентов и зависимостей ПО В) Политика безопасности контейнеров Г) Отчет о статическом анализе кода	ПК-8
56	А, Г	Какие форматы используются для представления SBOM? (Выберите все верные) А) SPDX Б) JSON В) YAML Г) CycloneDX	ПК-8
57	А	Какой инструмент из экосистемы Sigstore используется для подписи и верификации артефактов?	ПК-8

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
3 семестр			
		А) Cosign Б) Syft В) Grype Г) Falco	
58	Г	На каком языке пишутся политики для Open Policy Agent (OPA)? А) YAML Б) Python В) HCL Г) Rego	ПК-8
59	А	Какой инструмент используется для runtime-безопасности контейнеров и обнаружения аномалий? А) Falco Б) Trivy В) Checkov Г) Semgrep	ПК-8
60	Б, В	Какие инструменты предназначены для сканирования уязвимостей в Docker-образах? (Выберите все верные) А) Semgrep Б) Trivy	ПК-8

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
3 семестр			
		В) Grype Г) OWASP ZAP	
61	А, Б	Какие стандарты безопасности подов (Pod Security) существуют в Kubernetes? (Выберите все верные) А) baseline Б) restricted В) privileged Г) isolated	ПК-8
62	В	Какой инструмент используется для генерации SBOM из контейнеров и файловых систем? А) Cosign Б) Falco В) Syft Г) Checkov	ПК-8
63	Б	Какой инструмент предназначен для автоматического отслеживания и исправления нарушений политик в облачных средах? А) OPA Б) Cloud Custodian В) Conftest	ПК-8

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
3 семестр			
		Г) Falco	
64	Б	Какой федеральный закон РФ регулирует вопросы защиты персональных данных? А) 187-ФЗ Б) 152-ФЗ В) 273-ФЗ Г) 149-ФЗ	ПК-8
65	А, В	Какие типы анализа безопасности относятся к динамическим (DAST)? (Выберите все верные) А) Сканирование веб-приложения через OWASP ZAP Б) Анализ исходного кода Semgrep В) Fuzzing API-эндпоинтов Г) Анализ Docker-образа Trivy	ПК-8
66	А	Что означает аббревиатура SCA в контексте безопасности? А) Software Composition Analysis Б) Static Code Analysis В) Security Compliance Audit Г) Secure Container Architecture	ПК-8

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
3 семестр			
67	В, Г	Какие инструменты используются для анализа уязвимостей зависимостей (SCA)? (Выберите все верные) А) Semgrep Б) Falco В) OWASP Dependency-Check Г) Snyk	ПК-8
68	А	Какой государственный орган РФ осуществляет регулирование в области безопасности критической информационной инфраструктуры (КИИ)? А) ФСТЭК России Б) Минцифры России В) Роскомнадзор Г) Минобороны России	ПК-8
69	А	Что такое ложное срабатывание (false positive) в SAST? А) Инструмент ошибочно помечает безопасный код как уязвимый Б) Инструмент пропускает реальную уязвимость В) Инструмент не может завершить сканирование Г) Инструмент генерирует пустой отчет	ПК-8
70	Б	Какая система используется для оценки критичности уязвимостей по	ПК-8

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
3 семестр			
		шкале от 0 до 10? А) STRIDE Б) CVSS В) DREAD Г) OWASP	
71	В, Г	Какие инструменты позволяют проверять конфигурации Kubernetes с помощью политик OPA? (Выберите все верные) А) Cloud Custodian Б) Checkov В) Conftest Г) Gatekeeper	ПК-8
72	А	Как называется подход, при котором безопасность интегрируется в DevOps-культуру на всех этапах жизненного цикла? А) DevSecOps Б) GitOps В) FinOps Г) NoOps	ПК-8
73	Б	Какой механизм безопасности был добавлен в протокол MAVLink версии 2 для защиты от подмены пакетов?	ПК-11

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
3 семестр			
		А) Шифрование всего трафика Б) Подпись пакетов (Signing) В) Сжатие данных Г) Двухфакторная аутентификация	
74	А, В, Д	Какие типы угроз включает методология STRIDE? (Выберите все верные) А) Spoofing (подмена) Б) Injection (внедрение) В) Tampering (изменение данных) Г) XSS (межсайтовый скриптинг) Д) Denial of Service (отказ в обслуживании)	ПК-11
75	Б	Какой тип угрозы в методологии STRIDE соответствует перехвату и повторной передаче легитимных команд? А) Tampering Б) Repudiation (отказ от действий) В) Information Disclosure Г) Elevation of Privilege	ПК-11
76	В	Какой тип диаграммы строится на первом этапе методологии STRIDE для идентификации элементов системы?	ПК-11

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
3 семестр			
		А) UML-диаграмма классов Б) BPMN-диаграмма процессов В) DFD (Data Flow Diagram) Г) ER-диаграмма	
77	А	Какая методология используется для количественной оценки рисков на основе параметров: Damage, Reproducibility, Exploitability, Affected users, Discoverability? А) DREAD Б) CVSS В) STRIDE Г) OWASP Risk Rating	ПК-11
78	Б, Г	Какие протоколы связи наиболее часто используются в автономных системах (БПЛА) и робототехнике? (Выберите все верные) А) HTTP Б) MAVLink В) FTP Г) DDS	ПК-11
79	Б	Какая подсистема ROS 2 обеспечивает аутентификацию, шифрование и контроль доступа?	ПК-11

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
3 семестр			
		А) ROS 2 Bridge Б) DDS Security В) ROS 2 Launch Г) RViz	
80	Б, В	Какие атаки наиболее характерны для протокола MAVLink без защиты? (Выберите все верные) А) SQL-инъекция Б) Replay-атака В) Подмена пакетов Г) XSS	ПК-11
81	А	Как называется популярная наземная станция управления (GCS) с открытым исходным кодом для БПЛА на прошивке PX4? А) QGroundControl Б) Mission Planner В) DroneKit Г) ArduPilot GCS	ПК-11
82	В	Какой инструмент позволяет анализировать сетевой трафик протоколов MAVLink и DDS для выявления уязвимостей? А) Nmap	ПК-11

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
3 семестр			
		Б) Metasploit В) Wireshark Г) Burp Suite	
83	А	Как называется механизм, обеспечивающий проверку подлинности загрузчика и ядра ОС при старте бортового компьютера? А) Secure Boot Б) Trusted Boot В) Measured Boot Г) Safe Boot	ПК-11
84	В	Какой набор инструментов используется для обеспечения безопасности ROS 2 (изоляция узлов, аутентификация, шифрование)? А) ROS 2 Security Kit Б) ROS 2 Guard В) SROS 2 Г) ROS 2 Shield	ПК-11
85	А, Г	Какие механизмы мандатного контроля доступа (MAC) используются в Linux для изоляции процессов? (Выберите все верные) А) AppArmor Б) iptables	ПК-11

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
3 семестр			
		В) fail2ban Г) SELinux	
86	Б	Что означает аббревиатура OTA в контексте обновлений прошивок? А) On-Time Activation Б) Over-The-Air В) Open Trust Architecture Г) One-Time Authentication	ПК-11
87	Г	Как называется механизм защиты от установки старой уязвимой версии прошивки после выхода обновления? А) Secure Boot Б) Code Signing В) A/B Update Г) Rollback protection	ПК-11
88	Б	Какая архитектура обновления предполагает наличие двух разделов (активного и резервного) для атомарной установки? А) Canary update Б) A/B-разделы В) Rolling update Г) Blue-Green update	ПК-11

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
3 семестр			
89	А	Как называется стратегия обновления, при которой новая прошивка сначала выкатывается на малую часть парка устройств (например, 5-10%)? А) Canary update Б) A/B update В) Full rollout Г) Staged update	ПК-11
90	Б, В	Какие инструменты используются для криптографической подписи прошивок перед отправкой на устройства? (Выберите все верные) А) Trivy Б) Cosign В) GPG Г) Syft	ПК-11
91	В	Какая популярная open-source прошивка используется для автопилотов БПЛА (наряду с PX4)? А) Betaflight Б) iNav В) ArduPilot Г) Cleanflight	ПК-11

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
3 семестр			
92	Б, Г	Какие симуляторы наиболее часто используются для SITL-тестирования БПЛА и робототехнических систем? (Выберите все верные) А) Unity Б) Gazebo В) Unreal Engine Г) Webots	ПК-11
93	А	Какой тип угрозы в STRIDE соответствует перехвату телеметрии (раскрытие конфиденциальной информации)? А) Information Disclosure Б) Tampering В) Spoofing Г) Elevation of Privilege	ПК-11
94	Г	Какой тип угрозы в STRIDE соответствует повышению привилегий (например, получение контроля над полетным контроллером)? А) Denial of Service Б) Repudiation В) Tampering Г) Elevation of Privilege	ПК-11

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
3 семестр			
95	А, В	Какие уязвимости отсутствуют в протоколе MAVLink версии 1 и были частично исправлены в версии 2? (Выберите все верные) А) Отсутствие шифрования Б) Уязвимость переполнения буфера В) Отсутствие аутентификации пакетов Г) Уязвимость инъекции команд	ПК-11
96	Б	Как называется атака типа Man-in-the-Middle (MITM) применительно к каналу связи дрона? А) Подмена GPS-сигнала Б) Внедрение в канал связи между дроном и наземной станцией В) Глушение канала управления Г) Перехват телеметрии без модификации	ПК-11
97	В	Какой инструмент используется для генерации SBOM из контейнеров? А) Trivy Б) Cosign В) Syft Г) Falco	ПК-8
98	А, Г	Какие типы политик безопасности подов (Pod Security Standards)	ПК-8

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
3 семестр			
		существуют в Kubernetes? (Выберите все верные) А) baseline Б) secure В) audit Г) restricted	
99	Б	Какой инструмент позволяет проверять конфигурационные файлы (Kubernetes, Terraform) с помощью политик OPA из командной строки? А) Gatekeeper Б) Conftest В) Checkov Г) Falco	ПК-8
100	А	Что означает аббревиатура КИИ в российском законодательстве? А) Критическая информационная инфраструктура Б) Комплексная информационная инфраструктура В) Корпоративная информационная инфраструктура Г) Компьютерная информационная инфраструктура	ПК-8

Описание шкалы оценивания

В рамках рейтинговой системы успеваемость студентов по каждой дисциплине оценивается в ходе текущего контроля и промежуточной аттестации. Рейтинговая система оценки знаний студентов основана на использовании совокупности контрольных мероприятий по проверке пройденного материала, оптимально расположенных на всем временном интервале изучения дисциплины. Принципы рейтинговой системы оценки знаний студентов основываются на требованиях, описанных в Положении об организации образовательного процесса на основе рейтинговой системы оценки знаний студентов в ФГАОУ ВО «СКФУ».

Критерии оценивания компетенций

Оценка «отлично» (5 баллов) — высокий уровень сформированности

Обучающийся демонстрирует высокий уровень сформированности компетенций ПК-8 и ПК-11:

По ПК-8 (безопасность жизненного цикла):

1. Самостоятельно настраивает многоступенчатые Quality Gates на основе CVSS-оценок и эксплуатируемости уязвимостей.
2. Кастомизирует правила SAST (Semgrep/CodeQL) под специфику проекта (включая инженерные системы на C++/Python), интегрирует их в MR/PR с автоматической блокировкой слияния.
3. Разрабатывает кастомные политики для Checkov/tfsec и интегрирует их в этап terraform plan с блокировкой деплоя при нарушениях.
4. Настраивает runtime-безопасность (Falco) с кастомными политиками, интегрирует с SIEM и настраивает автоматическую реакцию на инциденты.
5. Разрабатывает сложные политики Rego для Open Policy Agent (OPA) и Cloud Custodian, настраивает автоматическую генерацию отчетов для аудита (включая требования 152-ФЗ, ФСТЭК).

По ПК-11 (безопасность автономных систем):

1. Проводит комплексный анализ угроз с использованием методологии STRIDE, разрабатывает детальную модель нарушителя, оценивает риски по DREAD.
2. Настраивает шифрование и аутентификацию каналов связи (DDS Security в ROS 2, MAVLink 2.0 Signing), моделирует атаки (replay, MITM) и предлагает меры защиты.
3. Настраивает мандатный контроль доступа (SELinux/AppArmor) для бортового ПО, интегрирует с Secure Boot.
4. Внедряет безопасные OTA-обновления с A/B-разделами, канареечными (canary) обновлениями, защитой от отката (rollback protection) и автоматизированным rollout на парк устройств.
5. Формирует SBOM для прошивок (PX4/ArduPilot) и управляет уязвимостями цепочки поставок.

Лабораторные работы и тестирование: все лабораторные работы выполнены в полном объеме, тестовые задания решены без ошибок, сквозной проект защищен с демонстрацией всех реализованных механизмов.

Оценка «хорошо» (4 балла) — средний уровень сформированности

Обучающийся демонстрирует средний уровень сформированности компетенций:

По ПК-8:

1. Уверенно интегрирует SAST/SCA/DAST в CI/CD-пайплайн, настраивает базовые Quality Gates (блокировка при HIGH-уязвимостях).
2. Пишет простые политики Rego для OPA/Conftest (например, запрет latest-тегов, требования к labels).
3. Анализирует отчеты об уязвимостях и предлагает корректирующие меры.
4. Настраивает базовые политики Falco (обнаружение запуска шелла в контейнере).

По ПК-11:

Самостоятельно применяет методологию STRIDE, строит DFD-диаграммы и формулирует актуальные угрозы для БПЛА/робота.

1. Настраивает базовую аутентификацию в ROS 2 (SROS 2) или подпись MAVLink.
2. Организует подписанные OTA-обновления с использованием Cosign.
3. Формирует SBOM для прошивок и выявляет CVE с помощью Trivy/Syft.

Лабораторные работы: выполнены в полном объеме, но есть незначительные замечания (неоптимальная конфигурация, неполный анализ угроз). Тестовые задания решены с небольшими ошибками.

Оценка «удовлетворительно» (3 балла) — минимальный уровень сформированности

Обучающийся демонстрирует минимальный уровень сформированности компетенций:

По ПК-8:

1. Знает базовые инструменты безопасности (Semgrep, Trivy, OWASP ZAP), может запустить их в ручном режиме.
2. Интерпретирует готовые отчеты об уязвимостях, но не настраивает автоматическую блокировку пайплайна.
3. Понимает концепцию Quality Gates, но настраивает только простые проверки (например, наличие артефактов).
4. Знает OPA/Rego на теоретическом уровне, но не может написать политику самостоятельно.

По ПК-11:

1. Знает основные угрозы для автономных систем (подмена GPS, перехват телеметрии).
2. Составляет простую модель угроз по шаблону (с помощью преподавателя).
3. Понимает необходимость шифрования каналов связи, но не может настроить его самостоятельно.
4. Знает архитектуру OTA-обновлений, но не может организовать подписанные обновления.

Лабораторные работы: выполнены частично, с помощью преподавателя. Тестовые задания решены на 50-70% правильно.

Оценка «неудовлетворительно» (2 балла) — минимальный уровень не достигнут

Обучающийся не демонстрирует сформированности компетенций:

По ПК-8:

1. Не знает инструменты SAST/DAST/SCA, не может объяснить принципы Shift Left и Compliance as Code.
2. Не способен настроить Quality Gates или написать политики Rego.
3. Лабораторные работы не выполнены или выполнены с грубыми ошибками.

По ПК-11:

1. Не знает методологию анализа угроз (STRIDE), не ориентируется в протоколах MAVLink/DDS.
2. Не способен выполнить анализ защищенности каналов связи или предложить меры защиты.
3. Не понимает архитектуру OTA-обновлений.

Лабораторные работы и тестирование: лабораторные работы не сданы, тестовые задания решены менее чем на 50% правильно, сквозной проект не защищен.

Шкала перевода баллов в оценку

Суммарный балл (процент выполнения)	Оценка	Уровень сформированности
90-100%	5 (отлично)	Высокий
75-89%	4 (хорошо)	Средний
60-74%	3 (удовлетворительно)	Минимальный
менее 60%	2 (неудовлетворительно)	Не достигнут

Итоговое заключение

Оценка по дисциплине «Безопасность жизненного цикла» выставляется на основе:

Результатов выполнения 18 лабораторных работ (включая сквозной проект) — 50% итоговой оценки.

Результатов тестового контроля (50 вопросов) — 30% итоговой оценки.

Качества защиты сквозного проекта (презентация, демонстрация, ответы на вопросы) — 20% итоговой оценки.