

Положение о проведении Всероссийского соревнования по безопасной разработке

1. Общие положения

1.1. Настоящее Положение определяет цель, порядок организации и проведения, условия и порядок участия в соревновании по безопасной разработке (далее – Соревнование).

1.2. Организатором Соревнования является Уральский федеральный университет (далее – Организатор).

1.3. Соорганизатором Соревнования является ООО «УЦСБ» (далее – Соорганизатор).

1.4. Организатор оставляет за собой право изменять правила Соревнования по собственному усмотрению в одностороннем порядке и вносить изменения в Положение с публикацией этих изменений на сайте Соревнования. Такого рода изменения вступают в силу с момента их публикации на сайте.

1.5. Соревнование представляет собой мероприятие, проводимое с целью демонстрации навыков безопасной разработки, поиска уязвимостей и внедрения инструментов безопасности в процесс разработки программного обеспечения (ПО).

1.6. Участниками Соревнования могут быть учащиеся вузов (направлений подготовки бакалавриата, специалитета и магистратуры) и ссузов Российской Федерации.

1.7. Для участия в отборочном этапе от каждого вуза и ссуза возможно неограниченное количество команд. В очный финал приглашаются 15 команд-лидеров по результатам онлайн-отбора.

1.8. Количество участников одной команды – от 3 до 5 человек со следующим распределением ролей:

- Appsec инженер (настраивает CI/CD, встраивает инструменты безопасности в пайплайн, защищает GitLab, Nexus и другие внутренние сервисы, внедряет SSDLC);
- Devsecops инженер (ищет уязвимости, исправляет код, анализирует результаты сканеров, настраивает политики сканеров);
- Аналитик безопасной разработки/архитектор (распределяет задачи и управляет ресурсами, формирует архитектуру безопасности, защищает результаты).

Необходимо в каждой команде иметь по одному представителю каждой роли, то есть для команды 3 человека – на каждой роли по одному человеку, в команде из 4-х человек может быть два человека на любой из ролей, в команде из 5-ти человек на двух любых ролях может быть по два человека.

1.9. Максимальное количество команд, которые будут допущены до Соревнования по итогам отборочного этапа – 15 команд. Организатор оставляет за собой право увеличить количество команд, прошедших в финал, для которых не требуется организация проживания.

1.10. Соревнования проводятся в соответствии с законодательством Российской Федерации и требованиями настоящего Положения.

1.11. Соревнования проводятся по адресу: г. Екатеринбург, Кампус УрФУ (мкр-н Новокольцовский, ул. Универсиады 7).

1.12. Соревнования проводятся в четыре этапа:

Этап 1: регистрация команд — с 12.10.2026 по 23.10.2026.

Этап 2: выполнение заданий онлайн-отбора — 24-25 октября 2026 года.

Этап 3: проверка заданий отборочного этапа — с 26.10.2026 по 30.10.2026.

Этап 4: объявление результатов и публикация списков финалистов — 31.10.2026.

Этап 5: очный финал соревнования — 26-27 ноября 2026 года (г. Екатеринбург).

Этап 6: подведение итогов и награждение — 27.11.2026.

1.13. Соревнования проводятся на базе виртуального полигона, представляющего собой набор виртуальных машин, которые содержат уязвимости и ошибки конфигурации с целью отработки навыков поиска уязвимостей, а также систему GitLab и Nexus для отработки навыков внедрения инструментов безопасной разработки.

1.14. Участие в Соревнованиях является бесплатным. Организатор обеспечивает проживание участников (кроме участников из Екатеринбурга и Свердловской области) и питание для всех участников в дни проведения Соревнования. Расходы на проезд до места проведения Соревнования и обратно покрываются направляющей стороной.

2. Цели и задачи Соревнования.

2.1. Цели проведения Соревнования:

- повышение уровня теоретических знаний участников и совершенствование их практических навыков в области безопасной разработки;
- формирование у участников системно-целостного видения проблем обеспечения безопасности разработки ПО;
- формирование у участников представлений о природе возникновения уязвимостей, навыков практической реализации мероприятий защиты от них;
- ориентация участников на получение образования и дальнейшее трудоустройство в сфере информационных технологий и компьютерной безопасности;
- знакомство и выстраивание дальнейшего сотрудничества с технологическими компаниями-участниками Соревнования.

2.2. Задачи проведения Соревнования:

- получение участниками практических знаний и закрепление теоретических, полученных на занятиях в учебных заведениях и из иных источников;
- оценка компетенций участников, их умения ориентироваться в нестандартной ситуации;
- подготовка к участию во всероссийских и международных соревнованиях и олимпиадах по информационной безопасности и безопасной разработке.

3. Порядок регистрации в Соревновании

3.1. Регистрация участников Соревнования начинается с 12.10.2026 и длится по 16.10.2026 включительно.

3.2. Регистрация участников осуществляется посредством заполнения формы заявки в сроки, указанные в п. 3.1 Положения на сайте: <https://devsecops-contest.ru>

3.3. Участники самостоятельно организуются в команды. Регистрация команды Соревнования осуществляется одним участником команды посредством заполнения электронной формы заявки на сайте, указанном в п. 3.2 Положения.

3.4. При регистрации команда обязана предоставить полную, достоверную и не нарушающую законодательство Российской Федерации информацию об участниках. Объем предоставляемой информации определяется в форме для регистрации.

3.5. Заявка на участие от команды считается принятой, если участник заполнил все поля электронной формы регистрации, согласился с условиями Положения о конкурсе, дал согласие на обработку персональных данных, ознакомился с политикой конфиденциальности персональных данных, нажал кнопку «Зарегистрироваться» и получил звонок-подтверждение от менеджера проекта.

3.6. Отборочный этап Соревнования проводится онлайн в период с 17.10.2026 по 18.10.2026 на сайте <https://devsecops-contest.ru/>

3.7. В рамках онлайн-отбора участникам предоставляется доступ к тестовому приложению (артефакту), содержащему уязвимости. Задача команды провести анализ, найти максимальное количество уязвимостей и предложить варианты их устранения.

3.8. Решение тестового задания каждая команда должна отправить до 18.10.2026 23:59 по времени Екатеринбурга на сайте <https://devsecops-contest.ru/> вкладка «Отчет»

3.9 Отчет должен быть оформлен в формате PDF и сдан от имени команды через платформу конкурса.

- Структура отчета на каждую уязвимость должна включать:
- Название и тип уязвимости (с указанием ID из OWASP Top 10 / CWE).
- Оценку критичности (по шкале CVSS).
- Пошаговое описание воспроизведения (Steps to reproduce) и доказательство эксплуатации (PoC: скриншоты, логи, исходный код эксплойта).
- Рекомендации по исправлению (на уровне кода или конфигурации).

3.10. Все выполненные задания отборочного этапа проходят проверку Организатором до 23:59 25.10.2026.

3.11. Команды, прошедшие отборочный этап, размещаются на главной странице сайта <https://devsecops-contest.ru/> не позднее 26.10.2026.

3.12. Команды, не прошедшие отборочный этап, не допускаются к участию в очном финале Соревнования.

3.13. Команда из 3-4 человек допускается к участию в очном финале, если готовы приехать в полном составе. Для команд из 5-ти человек допускается участие в составе 4-х человек. Возможна замена участника, в случае если 2 участника из 4 не смогут приехать на очный финал. Информацию о замене участника капитан команды отправляет Организаторам соревнований не позднее 23 октября 2026 года. Подтверждение участия

команды в очном этапе Соревнования осуществляется путем звонка менеджера проекта капитану команды.

4. Порядок участия в Соревновании

4.1. Организация Соревнования

4.1.1. Полное расписание дня Соревнования утверждается Организатором и размещается на официальном сайте Соревнования: <https://ucsbattle.ru/> не позднее 7 дней до их проведения. Дополнительная программа Соревнования отправляется на электронные почты участников, указанные при регистрации.

4.1.2. Инструкция для подключения к стендам соревнования и необходимые доступы для участников, в том числе ссылки на вступление во все чаты Соревнования, предоставляются Организатором перед проведением Соревнования.

4.1.3. В Соревнованиях предусмотрен командный зачет. За каждое правильно решенное задание баллы получает команда в целом, а не каждый отдельный участник. Результат одного из участников является результатом всей команды.

4.1.4. За выполненное задание Организатор начисляет баллы, указанные в п. 5.2 Положения

4.1.5 Задания отборочного тура и очного финала выполняются на оборудовании Участников. Организатор не осуществляет выдачу оборудования для участия в Соревнованиях.

4.2. Ограничения

4.2.1. Запрещается:

- присвоение ответов других команд своей команде;
- смена паролей в инфраструктуре;
- отключение агентов мониторинга событий информационной безопасности;
- иные преднамеренные воздействия, приводящие к:
 - нарушению работоспособности стендов;
 - невозможности реализации заданий;
 - невозможности оценки результатов.

4.2.2. При выявлении нарушений участник Организатор вправе применить меры в виде штрафов, таких как вычет баллов с командного счета или дисквалификация команды.

4.3. Порядок участия в очном финале

4.3.1. Командам предоставляется GitLab с проектом, в который загружен open-source ПО и Nexus.

4.3.2. В рамках очного финала командам предоставляется GitLab с проектом (open-source ПО) и Nexus.

Командам необходимо выполнить следующие задачи:

1. Провести хардеринг GitLab и Nexus. Результаты подтвердить техническим отчетом о внесенных изменениях в конфигурации.
2. Настроить CI/CD пайплайн, встроив в него инструменты безопасной разработки (SAST, DAST, SCA) на соответствующих этапах.

3. Провести кастомизацию политик сканеров: настроить правила так, чтобы критически снизить количество ложных срабатываний (False Positive) без пропуска реальных уязвимостей (False Negative).
4. Найти, описать и устранить уязвимости в ПО, подготовив отчет по результатам проделанных работ.
5. Подготовить презентацию с описанием архитектуры безопасности и обоснованием внедренных процессов.

4.3.3. Дополнительное задание: участникам предоставляется развернутое ПО. Задача команды — провести тестирование на проникновение и аудит кода методами «черного» и «серого» ящика (учетные записи для серого ящика предоставляются Организатором). По результатам подготовить отчет.

4.3.4. По итогам реализации заданий команда разрабатывает отчет о том, какие инструменты и техники использовались на разных этапах.

4.3.5 Для выполнения заданий на этапе онлайн-отбора и очном финале допускается использование командой искусственного интеллекта.

4.3.6 Для защиты задания необходимо подготовить презентацию о проделанной работе.

4.3.7 Презентации команд проверяются жюри Соревнования.

5. Оценка команд

5.1. Команды оцениваются по 100-балльной шкале. Итоговый балл складывается из четырех модулей по 25 баллов каждый.

5.2. Детализация критериев оценки:

Модуль 1. Application Security (25 баллов)

Оценивается качество аудита и поиска уязвимостей в предоставленном ПО.

10 баллов — за количество и критичность найденных уязвимостей. Учитываются только уникальные уязвимости. Дубликаты внутри команды не суммируются. Критические и высокоуровневые уязвимости имеют приоритет.

10 баллов — за качество доказательной базы (PoC). Балл начисляется за каждый предоставленный рабочий эксплойт / скрипт / пошаговый гайд, подтверждающий уязвимость. Уязвимости без PoC не оцениваются.

5 баллов — за качество рекомендаций по исправлению (Remediation). Оценивается глубина проработки: от общих фраз («исправить код») до конкретных патчей, примеров безопасного кода или настроек WAF/конфигураций.

Модуль 2. DevSecOps и Хардеринг (25 баллов)

Оценивается настройка инфраструктуры и CI/CD (основное задание финала).

10 баллов — за хардеринг GitLab и Nexus. Жюри проверяет отчет и конфигурации на соответствие лучшим практикам (отключение лишних сервисов, настройка прав доступа, шифрование, аудит логов).

10 баллов — за внедрение инструментов в CI/CD. Оценивается корректность интеграции SAST/DAST/SCA, настройка триггеров (например, блокировка merge request при наличии Critical уязвимостей).

5 баллов — за кастомизацию политик (Tuning). Оценивается способность команды настроить сканеры: снижение уровня шума (False Positive) при сохранении полноты сканирования. Штрафные баллы снимаются, если команда просто отключила сканер или критические алерты.

Модуль 3. Аналитика и процессы SSDLC (25 баллов)

Оценивается методологическая часть работы команды.

15 баллов — за разработку руководства по безопасной разработке (Secure Coding Guidelines) и регламентов. Оценивается применимость документов на практике, учет специфики предоставленного open-source ПО, наличие чек-листов для разработчиков.

10 баллов — за выстраивание процесса реагирования на инциденты ИБ. Оценивается наличие описанного SLA, маршрутизации уведомлений от сканеров к разработчикам и трекинга исправлений.

Модуль 4. Защита проекта перед жюри (25 баллов)

Оценивается презентация и ответы на вопросы.

10 баллов — за техническую глубину презентации. Насколько полно раскрыта архитектура внедренного SSDLC, обоснован выбор конкретных инструментов и политик.

10 баллов — за ответы на вопросы жюри. Оценивается эрудиция участников, умение аргументированно защищать принятые технические решения и отвечать на каверзные вопросы.

5 баллов — за тайминг, слаженность команды и качество визуальных материалов. Презентация должна занять строго отведенное время (до 10 минут), выступать должны все заявленные роли (Appsec, DevSecOps, Team Lead).

5.3 За дополнительное задание по проведению тестирования на проникновение начисляется вплоть до 10 баллов.

6. Призы и порядок их получения

6.1. Призы предоставляются Организатором Соревнования.

6.2. Призовые места в зависимости от баллов распределяются по трем командам-победителям от большего к меньшему количеству баллов – 1 место, 2 место, 3 место.

6.3. Дипломы победителей Соревнования подписываются председателем Оргкомитета.

6.4. В каждом призовом месте победителем может стать только одна команда участников.

6.5. Призы победителям и призерам определяются Организатором и Соорганизатором Соревнования не менее чем за 14 дней до проведения очного этапа Соревнования.

6.6. Выдача призов командам-победителям осуществляется на торжественном награждении 27.11.2026.

6.8. Информация об итогах Соревнования размещается в сети на официальном сайте Соревнования: <https://ucsbattle.ru/> в течение трех рабочих дней после завершения Соревнования.

7. Заключительные положения

7.1. Соревнования организованы в соответствии с законодательством Российской Федерации (применимое право).

7.2. Регистрация и участие в порядке, предусмотренном разделом 4 настоящего Положения, означает его безоговорочное согласие со всеми условиями и правилами Соревнования, указанными в Положении.

7.3. Во всем, что не урегулировано Положением, стороны руководствуются действующим законодательством Российской Федерации.

7.4. Все споры и разногласия, которые возникают в связи с организацией и проведением Соревнования, подлежат разрешению путем переговоров.

7.5. Если по какой-либо причине настоящие Соревнования в любой части не могут проводиться так, как было запланировано, включая причины, вызванные заражением вредоносным программным обеспечением, поломками в сети Интернет, хакерскими атаками, манипуляциями, несанкционированным вмешательством, фальсификацией, техническими неполадками или любой другой причиной, неконтролируемой Организатором Соревнования, которая искажает или затрагивает исполнение, безопасность, целостность или адекватность проведения Соревнования, Организатор может по своему единоличному усмотрению временно приостановить проведение Соревнования. В этом случае сроки проведения Соревнования будут соразмерно увеличены на срок приостановления проведения Соревнования.

7.6. Организатор Соревнования оставляет за собой право на изменение условий настоящего Положения и порядка проведения Соревнования, а также на отказ от его проведения. При этом Организатор Соревнования обязуется уведомить участников об указанных действиях путем размещения актуальной версии Положения на сайте Соревнования или путем отправки соответствующего уведомления.