

Положение о проведении всероссийских соревнований «Киберучения в УрФУ» в области информационной безопасности

Настоящее положение устанавливает порядок и условия проведения всероссийских соревнований «Киберучения в УрФУ» (далее – Соревнований) в области информационной безопасности среди учащихся вузов и ссузов Российской Федерации и стран СНГ.

I. Общие положения

1.1. Настоящее Положение определяет цели, порядок организации и проведения, условия и порядок участия в Соревнованиях.

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

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

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

1.5. Соревнования представляют собой очное мероприятие, проводимое с целью демонстрации атакующих техник и методов расследования кибератак на базе различного рода сервисов и типов инфраструктур.

1.6. Участниками Соревнований могут быть учащиеся вузов (направлений подготовки бакалавриата, специалитета, базового высшего образования) и ссузов Российской Федерации и стран СНГ очной формы обучения.

1.7. От каждого вуза и ссуза возможно неограниченное количество команд по двум направлениям:

- Red Team – атакующая команда;
- Blue Team – расследующая команда.

1.8. Количество участников одной команды – от 4 до 5 человек.

1.9. Максимальное количество команд, которые будут допущены до Соревнований по итогам отборочного этапа – 15 атакующих команд, 15 расследующих команд. Организатор оставляет за собой право уменьшить количество команд, допущенных к очному этапу, по итогам отборочного этапа, при этом количество атакующих и расследующих команд должно быть равным друг другу.

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. Новоколыцковский, ул. 100-летия Уральского университета, стр. 5).

1.12. Соревнования проводятся в семь этапов:

Этап 1: регистрация команд на соревнования с **12.10.2026 по 25.10.2026.**

Этап 2: выполнение заданий отборочного этапа с **26.10.2026 по 1.11.2026.**

Этап 3: проверка заданий отборочного этапа с **27.10.2026 по 2.11.2026.**

Этап 4: оглашение результатов отборочного этапа – **2.11.2026 по 9.11.2026.**

Этап 5: активность команды атакующих (Red Team) – **26.11.2026.**

Этап 6: активность команды расследующих (Blue Team) – **27.11.2026.**

Этап 7: подведение итогов и награждение победителей – **27.11.2026.**

1.13. Соревнования проводятся на базе виртуального киберполигона, представляющего собой набор виртуальных машин, которые содержат уязвимости и ошибки конфигурации с целью отработки тактик и техник атакующих, а также систему мониторинга событий информационной безопасности в целях последующего расследования инцидентов и восстановления действий атакующих.

1.14. Участие в Соревнованиях является бесплатным. Организатор обеспечивает проживание участников и питание в дни проведения Соревнований. Расходы на проезд до места проведения Соревнований и обратно покрываются направляющей стороной.

1.15. Организаторы оставляют за собой право изменения сроков проведения Соревнований. При этом, Организатор обязуется уведомить участников о таких изменениях на сайте Соревнований или путем отправки соответствующего уведомления на электронную почту участников.

2 Цели и задачи Соревнований

2.1. Цели проведения Соревнований:

- повышение уровня теоретических знаний участников и совершенствование их практических навыков в области информационной безопасности;
- формирование у участников системно-целостного видения проблем обеспечения информационной безопасности;
- ориентация участников на получение образования и дальнейшее трудоустройство в сфере информационных технологий и компьютерной безопасности;
- выявление и поддержка талантливой молодежи.

2.2. Задачи проведения Соревнований:

- 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.

3 Порядок регистрации в Соревнованиях

3.1. Регистрация участников Соревнований начинается с **12.10.2026** и длится по **25.10.2026 включительно**.

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

3.3. Участники самостоятельно организовываются в команды. Регистрация команд Соревнований осуществляется одним участником команды посредством заполнения единой 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 Соревнований проводится онлайн в период с **26.10.2026 по 1.11.2026 г.** Тестовые задания команды получают с помощью рассылки электронных писем на e-mail капитана команды, указанный при регистрации.

3.7. После получения тестового задания каждая команда должна отправить решение до **1.11.2026 23:59 по времени Екатеринбурга** на электронный адрес Организаторов: friend@urfu.ru

3.8. В электронном письме с решением отборочного задания команда обязана указать: порядок решения задания, ответ на задание, название команды, ФИО каждого участника команды.

3.9. Все выполненные задания отборочного этапа проходят проверку Организатором в течение пяти календарных дней после завершения этапа выполнения заданий.

3.10. После формирования списка команд, допущенных к участию в очном этапе, менеджеры проекта подтверждают участие таких команд посредством телефонного звонка.

3.10. Команды, должны подтвердить очное участие не позднее 3 дней после получения звонка от менеджера проекта.

3.11. Если команда, ранее допущенная к очному этапу, отказалась от участия в очном этапе, к участию в очном этапе приглашается команда следующая по списку допущенных команд.

3.12. Итоговый список команд, допущенных к участию в очном этапе, размещается на главной странице сайта <https://ucsbattle.ru/> не позднее **9.11.2026**.

3.13. Команда допускается к участию, если не менее 80% ее Участников подтвердили свое участие.

4 Порядок участия в Соревнованиях

4.1. Организация Соревнований

4.1.1. Точное расписание дней Соревнования утверждается Организатором и направляется командам на электронные почты не позднее 3 дней до их проведения.

4.1.2. Подключение к киберполигону осуществляется через VPN-сервер. Инструкция для подключения и необходимые доступы для участия, в том числе ссылки на вступление во все чаты Соревнований, предоставляются Организатором в день проведения Соревнований.

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 карточке конкретного задания.

4.2. Ограничения

4.2.1. Запрещается:

- присвоение ответов других команд своей команде,
- проведение атак типа «отказ в обслуживании»,
- смена паролей скомпрометированных пользователей в инфраструктуре,
- исправление уязвимостей,
- отключения агентов мониторинга событий информационной безопасности
- использование систем искусственного интеллекта (ИИ), включая генеративные модели и ИИ-ассистенты, при выполнении заданий отборочного и очного этапов Соревнований, в том числе для поиска и формирования решений, генерации и анализа программного кода, подготовки ответов и отчетов, за исключением инструментов, прямо предоставленных или разрешенных Организатором
- и другие преднамеренные воздействия, приводящие к:
- нарушению работоспособности Киберполигона,
- невозможности реализации атак,
- невозможности расследования атак.

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

4.3. Порядок участия для атакующих команд

4.3.1. Целью атакующих команд является проведение атак на объекты киберполигона через выполнение предоставленных на Платформе заданий, представляющих собой требования к реализации конкретных техник в соответствии с матрицей MITRE ATT&CK.

4.3.2. Разрешается атаковать только сервисы киберполигона, расположенные по адресам, предоставленным Организатором.

4.3.3. Задания приближены к реальным сценариям и подразделяются на два типа:

- реализация недопустимых событий,
- задания на OSINT и киберразведку.

4.3.4. По итогам реализации цепочки атаки (kill-chain) команда разрабатывает отчет о том, какие тактики и техники использовались на разных этапах (в соответствии с матрицей

MITRE ATT&CK), а также использованные инструменты. В части получения определенных чувствительных данных при использовании тактик и техник в соответствии с заданием – указанные данные (флаги) – отражаются в отчете.

4.3.5. Для сдачи задания по реализации недопустимого события необходимо оформить отчет по шаблону, предоставленному на Платформе.

4.3.6. Отчеты по реализованным недопустимым событиям проверяются глобальным SOC.

4.3.7. Распределение баллов за выполненные задания фиксировано и прописано в задании.

4.4. Порядок участия для расследующих команд

4.4.1. Целью расследующих команд является расследование атак на объекты Киберполигона.

4.4.2. Задания приближены к реальным сценариям и могут быть выданы по двум типам:

- расследование действий команд Атакующих,
- выполнение единичных заданий, не связанных с действиями Атакующих.

4.4.3. В случае нехватки данных (например, неспособность команды Атакующих реализовать сценарий атаки) – представителям команды расследования будут предоставлены образы виртуальных машин, содержащих следы действий злоумышленников, приближенных к реальным сценариям угроз.

4.4.4. Для сдачи заданий по расследуемому недопустимому событию необходимо оформить отчет по шаблону, предоставленному на платформе.

4.4.5. Отчеты по расследуемым недопустимым событиям проверяются глобальным SOC.

4.4.6. Защитникам предоставляются следующие классы средств защиты для выявления атак: система для управления событиями информационной безопасности (SIEM); средства анализа сетевого трафика (NTA); система статического и динамического анализа файлов на вредоносность (Sandbox). Использование иных средств защиты согласовывается с Организатором отдельно.

5. Оценка команд

5.1. Команды оцениваются по 100-балльной шкале в соответствии с требованиями, указанными в п.5.2. и 5.3. Положения.

5.2. Команда атакующих оценивается по следующим условиям:

- достижение целей сценария Соревнований,
- использование тактик и техник, которые были не обнаружены XDR, то есть выполнен обход средств защиты информации.

5.3. Команда расследующих оценивается по следующим условиям:

- достижение целей сценария Соревнований,
- максимально полное покрытие тактик и техник, использованных злоумышленниками в ходе расследования.

5.4. Весовые коэффициенты, соответствующие каждой цели и выраженные в баллах, будут озвучены на Соревнованиях **26.11.2026**.

6. Призы и порядок их получения

6.1. Призы предоставляются Организатором Соревнований.

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

6.3. Победители Соревнований награждаются дипломами и призами.

6.4. Дипломы победителей Соревнований подписываются председателем оргкомитета.

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

6.6. Призы победителям и призерам определяются Организатором и Соорганизатором соревнований не менее чем за 14 дней до проведения очного этапа Соревнований.

6.7. Выдача призов командам-победителям осуществляется на торжественном награждении **27.11.2026.**

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

7. Заключительные положения

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

7.2. Регистрация Участника в порядке, предусмотренном разделом 4 настоящего Положения, означает его безоговорочное согласие со всеми условиями и правилами Соревнований, 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 Соревнований, подлежат разрешению путем переговоров.

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

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