Положение о проведении всероссийских киберучений для студентов вузов

Настоящее положение устанавливает порядок и условия проведения Всероссийских студенческих киберучений (далее – Соревнований) в области информационной безопасности (далее – Положение) среди учащихся вузов Российской Федерации.

1. Общие положения

1.1. Настоящий Регламент определяет правила проведения, условия и порядок участия во всероссийских киберучениях студентов вузов Российской Федерации (далее – Соревнования).

1.2. Организаторами Соревнований является Уральский федеральный университет и сообщество кибербезопасности Ural Cyber Securitty (далее – Организатор).

1.3. Положение определяет цели, порядок организации и проведения Соревнований для студентов высших учебных заведений.

1.4. Данное Положение о Соревнованиях является публичным предложением, воспользоваться которым возможно путем присоединения к условиям, предусмотренным в настоящем Положении и формулярах с информацией об условиях и порядке проведения Соревнований, с которыми можно ознакомиться на сайте Соревнований: ucsbattle.ru.

1.5. 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. Такого рода изменения вступают в силу с момента их публикации на сайте.

1.6. Соревнование представляет собой очное мероприятие, проводимое с целью демонстрации техник атакующих и методов расследования кибератак на базе различного рода сервисов и типов инфраструктур.

1.7. Участниками Соревнований могут быть только резиденты и учащиеся вузов Российской Федерации.

1.8. От каждого вуза возможно участие двух команд:

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

1.9. Количество участников одной команды – 4-5 человек.

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

1.10. Соревнования проводится по адресу: Екатеринбург, кампус УрФУ (мкр-н. Новокольцовский, ул. Универсиады 7).

1.11. Соревнования проводятся в четыре этапа:

Этап 1: прохождение отборочного этапа в период с **с 19 октября 2023 г. по 20 ноября 2023 г.**

Этап 2: активность команды атакующих (Red Team) – 5 декабря 2023 г.;

Этап 3: активность команды расследующих (Blue Team) – 6 декабря 2023 г.;

Этап 4: подведение итогов и награждение победителей – 7 декабря 2023 г.

1.12. Даты и время проведения Соревнований: 5 ноября 2023 г. с 10:00 до 23:00, 6 ноября 2023 г. с 10:00 до 23:00, 7 ноября 2023 г. с 10:00 до 14:00 по местному времени.

1.13. Соревнования проводится 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. Соревнования состоится в рамках форума «Форум будущего».

1.15. Правила определяются Порядком проведения Соревнований (п. 5).

1.16. Настоящее Положение является обязательным для исполнения всеми участниками Соревнований.

1.17. Участие в Соревнованиях является бесплатным.

1.18. Личные расходы участников на участие в Соревнованиях Организатором не компенсируются.

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;
- формирование у участников представления о природе возникновения угроз информационной безопасности, навыков практической реализации мероприятий защиты от них;
- ориентация участников на получение образования и дальнейшее трудоустройство в сфере Информационных Технологий и компьютерной безопасности;
- выявление и поддержка талантливой и творчески активной молодежи;
- знакомство и выстраивание дальнейшего сотрудничества с технологичными командами-участниками Соревнований.

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;
- подготовка к участию во всероссийских и международных соревнованиях и олимпиадах по информационной безопасности.

3. Порядок регистрации в Соревнованиях

3.1. Регистрация участников Соревнования начинается **19 октября 2023 г. и длится до 17 ноября 2023 г.**

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

3.3. Участники самостоятельно организовываются в команды из четырех-пяти человек. Регистрация команд Соревнований осуществляется одним участником команды посредством заполнения единой формы заявки, 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. Команда считается допущенной для прохождения отборочного этапа для участия в Соревнованиях, 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 подтверждение регистрации на указанный им адрес электронной почты.

3.6. Отборочный этап Соревнований проводится онлайн в период **с 19 октября 2023 г. по 20 ноября 2023 г.** с помощью рассылки электронных писем на e-mail зарегистрированных участников в указанные даты.

3.7. После получения электронного письма каждая команда должна отправить решение **до 20 ноября 2023 г.** 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 10 рабочих дней. После осуществления проверки письмо с подтверждением участия в Соревнованиях направляется Организатором на указанные участниками адреса электронной почты.

3.10. Команды, непрошедшие отборочный этап, не допускаются к участию в Соревнованиях.

3.11. Команда допускается к участию, если не менее 80% ее Участников подтвердили свое участие за семь дней до Соревнований путем опроса, направленного Организатором на адрес электронной почты участника. Капитан обязан найти замену участникам, которые не подтвердили свое участие, и сообщить об этом Организатору (куратору регистрации со стороны компании – Татьяна, friend@urfu.ru).

4. Порядок участия в Соревнованиях

5.1. Организация Соревнований

5.1.1. Тайминг Соревнований:

5 декабря 2023 г.:
9:00 – 9:30 – Открытие мероприятия;

9:30 – 10:00 – Описание правил Соревнований для обеих сторон;
10:00 – 23:00 – Работа атакующих команд (Red Team).
6 декабря 2023 г.:
10:00 – 23:00 – Работа расследующих команд (Blue Team).
7 декабря 2023 г.:
10:00 – 12:00 – Подведение итогов Соревнований;
12:00 – 13:00 – Торжественное награждение победителей.

5.1.2. 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 за день до мероприятия путем отправки письма на адрес электронной почты участника.

5.1.3. 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.

5.1.4. За выполненное задание Организатор начисляет баллы, указанные в карточке конкретного задания.

5.2. Ограничения

5.2.1. 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
- и другие преднамеренные воздействия, приводящие к:
    - нарушению работоспособности Киберполигона;
    - невозможности реализации атак;
    - невозможности расследования атак.

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

5.3. Порядок участия для атакующих команд

5.3.1. 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.

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

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

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

5.3.4. 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.

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

5.3.6. Отчеты по реализованным недопустимым событиям проверяются глобальным SOC.

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

5.4. Порядок участия для расследующих команд

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

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

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

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

5.4.4. Для сдачи заданий по расследованному недопустимому событию необходимо оформить отчет по шаблону, предоставленному на платформе.

5.4.5. Отчеты по расследованным недопустимым событиям проверяются глобальным SOC.

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

6. Оценка команд

6.1. Команды оцениваются по 100-балльной шкале в соответствии с требованиями, указанными в п.6.2. и 6.3. Положения.

6.2. 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.

6.3. Команда расследующих оценивается по следующим условиям:

- достижение целей сценария Соревнований;

- максимально полное покрытие тактик и техник, использованных злоумышленниками в ходе расследования.

6.4. Весовые коэффициенты, соответствующие каждой цели и выраженные в баллах, будут озвучены на Соревновании 5 декабря 2023 г.

7. Призы и порядок их получения

7.1. Призы предоставляются Организатором Соревнований.

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

7.3. Победители Соревнований награждаются дипломами и призами.

7.4. Дипломы победителей Соревнований подписываются председателем оргкомитета.

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

7.6. Команды из числа участников вправе претендовать на следующие призы:

- поездка на конференцию;
- курс обучения;
- сувенирная продукция.

7.7. Выдача призов командам-победителям осуществляется на торжественном награждении **7 декабря 2023 г. в 12:00.**

7.8. Организатор Соревнований не несет ответственности за распределение приза между участниками команды. Приз распределяется между участниками команды самостоятельно, без участия Организатора Соревнований.

7.9. Информация об итогах Соревнований размещается в сети на официальном сайте Соренований https://ucsbattle.ru в течение трёх рабочих дней после завершения Соревнований.

8. Заключительные положения

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

8.2. Регистрация Участника в порядке, предусмотренном разделом 4 настоящего Положения, означает его безоговорочное согласие со всеми условиями и правилами Соревнований, указанными в Положении.

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

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

8.5. 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 проведения 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.

8.6. 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.