Approved by order _____

from _ _ _ September 2024 year No. ____ _

Regulations for conducting all-Russian Cyber Drill for university students

This Regulation establishes the procedure and conditions for conducting all Russian Cyber Drill Students (hereinafter referred to as Competitions) in the field of information security (hereinafter referred to as the Regulation) among students of higher education institutions of the Russian Federation.

1. General provisions

1.1. These Regulations define the rules of conduct, conditions and procedure for participation in the all Russian Cyber Drills for students of higher education institutions of the Russian Federation (hereinafter referred to as Competitions).

1.2. The organizers of the Competition are the Ural Federal University organize and the Ural Cybersecurity Community (hereinafter referred to as the Organizer).

1.3. The Regulation defines the goals, procedure for organizing and conducting Competitions for students of higher educational institutions.

1.4. This Competition Regulation is available for free, all information on how to join and the forms with information about the conditions and procedure for conducting Competitions, can be found on the website: ucsbattle.ru.

1.5. The Organizer reserves the right to change the rules of the Competition at its sole discretion unilaterally and make changes to the Regulations with the publication of these changes on the website. Such changes take effect from the moment they are published on the website.

1.6. The competition is a public event held to demonstrate attacking techniques and methods for investigating cyber-attacks based on various types of services and infrastructure types.

1.7. Only residents and students of higher education institutions of the Russian Federation can participate in the Competition.

1.8. From each university two teams may participate:

- Red Team – the attacking team.
- Blue Team – the investigating team.

1.9. The number of participants in one team is 4-5people.

1.10. Competitions are held in accordance with the legislation of the Russian Federation and the requirements of these Regulations.

1.10. Competitions are held at : Ekaterinburg, UrFU campus (md-n. Novokolovskii, st. Universiade 7).

1.11. The competition is held in five stages:

Stage 1: registration for the competition is open **from July 29, 2024 to September 9, 2024**;

Stage 2: passing the qualifying stage in the period **from September 10, 2024 to September 22, 202.4**;

Stage 3: activity of the attacking team (Red Team) - October 24, 2024;

Stage 4: activity of the investigating team (Blue Team) – October 25, 2024;

Stage 5: Summing up the results and awarding the winners – October 26, 2024.

1.12. Dates and times of the Competition: October 24, 2024 from 10: 00 to 23: 00, October 25, 2024 from 10: 00 to 23: 00, October 26, 2024 from 10:00 to 14:00 local time.

1.13. The competition is held virtually using cyber polygon, which is a set of virtual machines containing vulnerabilities and configuration errors to detect the tactics and techniques of attackers, as well as an information security event monitoring system for subsequent incident investigation and recovery of attackers' actions.

1.14. The competition will be held within the framework of the forum "Forum of the Future".

1.15. The Rules are determined by the Competition Procedure (clause 5).

1.16. This Regulation is mandatory for all participants of the Competition.

1.17. Participation in the Competition is free of charge.

1.18. Personal expenses of participants for participating in the Competition are not compensated by the Organizer.

2. Goals and objectives of the Competition

2.1. Objectives of the Competition:

- increase the level of theoretical knowledge of participants and improve their practical skills in the field of information security;
- formation of participants' system-integrated vision for information security problems;
- formation of participants' understanding of the nature of information security threats, skills of practical implementation of measures to protect against them.
- orientation of participants to receive education and further employment in the field of Information Technology and computer security.
- identification and support of talented and creative active youth;
- getting acquainted and building further cooperation with high-tech teams participating in the Competition.

2.2. Objectives of the Competition:

- participants receive practical knowledge and consolidate theoretical knowledge obtained in classes in educational institutions and from other sources;
- assessment of the participants ' competencies, their ability to navigate in a non-standard situation;
- preparation for participation in all-Russian and international competitions and Olympiads on information security.

3. The procedure for registration in Competitions

3.1. Registration of participants of the Competition begins **on July 29, 2024 and lasts until September 9, 2024 inclusive.**

3.2. Registration of participants is carried out by filling out the application form within the time limits specified in clause 3.1. of the Regulations on the website: ucsbattle.ru .

3.3. Participants organize themselves into teams of four to five people. Registration of teams of the Competition is carried out by one team member by filling in a single application form, specified in clause 3.2. of the Regulations.

3.4. When registering, the team is obliged to provide complete, reliable and non-infringing information about the participants. The amount of information provided is determined in the registration form.

3.5. A team is considered eligible to pass the qualifying stage for participation in the Competition if the participant has filled in all the fields of the electronic registration form, agreed to the terms of the Competition Regulations, consented to the processing of personal data, read the Privacy Policy of Personal Data, clicked the "Register" button and received confirmation of registration to the email address specified by them.

3.6. The qualifying stage of the Competition is held online **from September 10, 2024 to September 22, 2024** by sending emails to registered participants on the dates specified**.** The registered participants will be notified through e-mail on the specified dates.

3.7. After receiving the e-mail, each team must send the decision **by September 22, 2024 to the** Organizers' email address: friend@urfu.ru

3.8. In the email with the solution of the qualifying task, the team must indicate: the order of solving the task, the answer to the task, the name of the team, and the full name of each team member.

3.9. All completed tasks of the qualifying stage are checked by the Organizer within 10 working days. After the verification is completed, the Organizer sends a confirmation letter of participation in the Competition to the email addresses specified by the participants.

3.10. The winners of the qualifying stage will be announced on the main page of the site ucsbattle.ru **on September 26, 2024**

3.10. Teams that will not pass the qualifying stage will not be allowed to participate in the Competition.

3.11. A team is allowed to participate if at least 80% of its Participants confirmed their participation seven days before the Competition by means of a survey sent by the Organizer to the email address of a private participant. The captain is obliged to find a replacement for private owners who have not confirmed their participation and inform the Organizer (the curator of registration on the part of the company – Tatiana, friend@urfu.ru).

4. Order of participation in Competitions

5.1. Organization of Competitions

5.1.1. Competition Timing:

October 24, 2024:
9:00 - 9:30 – Opening of the event;

9:30 - 10:00 – Description of the Competition rules for both sides.
10:00 - 23:00 – Work of the attacking teams (Red Team).

October 25, 2024:
10:00 - 23:00 – Work of the investigating teams (Blue Team).

October 26, 2024:
10:00 - 12:00 – Summing up the results of the Competition;
12:00 - 13:00 – Awarding ceremony of the winners.

5.1.2. You can connect to the cyber polygon via a VPN server. Instructions for activation and necessary accesses for participation, including links to join all chats of the Competition, are provided by the Organizer one day before the event by sending an email to the email address of a private participant.

5.1.3. The Competition includes a team competition. For each correctly solved task, points are awarded to the team, and not to each individual employee. The result of one of the private traders is the result of the entire to teem.

5.1.4. For the completed the task, the Organizer awards the points specified in the specific task card.

5.2. Restrictions

5.2.1. It is prohibited to:

- Assign responses from other Teams to your own Team.
- conducting denial-of-service attacks.
- changing passwords of compromised users in the infrastructure.
- fixing vulnerabilities.
- disabling information security event monitoring agents
- and other deliberate actions that lead to:
    - Disruption of the Cyber Polygon's performance.
    - failure to implement attacks.
    - failure to investigate attacks.

5.2.2. If violations of participation are detected, the Organizer has the right to apply penalties, such as deduction of points from the team account or disqualification of the team.

5.3. Participation procedure for Attacking Teams

5.3.1. The purpose of the following commands is to conduct attacks on objects of the cyber polygon through the execution of tasks provided on the Platform, which represent requirements for the implementation of specific techniques in accordance with the MITRE ATT&CK matrix.

5.3.2. Only the Cyber polygon services located at the addresses provided by the Organizer are allowed to be attacked.

5.3.3. Tasks are close to real-world scenarios and are divided into two types:

- implementation of invalid events.
- OSINT and cyber intelligence missions.

5.3.4. Based on the results of the implementation of the kill-chain, the team develops a report on, what tactics and techniques were used at different stages (in accordance with MITRE the MITRE ATTACK matrix), as well as the tools used. In terms of obtaining certain sensitive data when using tactics and techniques in accordance with the task, the specified data (flags) are reflected in the report.

5.3.5. To complete the task of implementing an invalid event, you must issue a report using the template provided on the Platform.

5.3.6. Reports on implemented invalid events are checked by the global SOC.

5.3.7. The distribution of points for completed tasks is fixed and specified in the task.

5.4. Participation procedure for investigating teams

5.4.1. The purpose of investigating teams is to investigate attacks on Cyber polygon facilities.

5.4.2. Tasks are close to real-world scenarios and are divided into two types:

- investigation of the actions of attacking teams;
- performing individual tasks that are not related to the actions of Attackers.

5.4.3. If there is a lack of data (for example, the Attacking team is unable to implement an attack scenario)– , representatives of the investigation team will be provided with virtual machine images containing traces of malicious actions that are close to real-world threat scenarios.

5.4.4. To submit tasks related to an investigated invalid event, you must submit a report based on the template provided on the platform.

5.4.5. Reports on investigated invalid events are checked by the global SOC.

5.4.6. Defenders are provided with the following classes of security tools for detecting attacks: a system for managing information security events (SIEM); network traffic analysis tools (NTA); a system for static and dynamic analysis of files for malware (Sandbox). The use of other means of protection is agreed with the Organizers separately.

6. Team evaluation

6.1. Teams are evaluated on a 100-point scale in accordance with the requirements specified in clauses 6.2 and 6.3 of the Regulations.

6.2. The attacking team is evaluated according to the following criteria:

- achieving the goals of the Competition scenario;
- using tactics and techniques that were not detected by XDR, that is, bypassing information security tools.

6.3. The investigating team is evaluated according to the following criteria:

- achieving the goals of the Competition scenario;
- maximum coverage of the tactics and techniques used by the attackers during the investigation.

6.4. The weight coefficients corresponding to each goal and expressed in points will be announced at the Competition on December 5, 2023.

7. Prizes and how to get them

7.1. Prizes are provided by the Competition Organizer.

7.2. Depending on the number of points, prizes are distributed among three winning teams from more to less points – 1st place, 2nd place, and 3rd place.

7.3. The winners of the Competition are awarded with diplomas and prizes.

7.4. Diplomas of the winners of the Competition are signed by the chairman of the organizing committee.

7.5. In each prize place, only one team of participants can become the winner.

7.6. Teams from private owners are eligible for the following prizes:

- travel to the conference;
- course of training;
- souvenir.

7.7. Prizes will be awarded to the winning teams at the awards ceremony **on October 26, 2024 at 12:00.**

7.8. The organizer of the Competition is not responsible for the distribution of the prize among the team members. The prize is distributed among the team members independently, without the participation of the Competition Organizer.

7.9. Information about the results of the Competition is posted online on the official website of the Competition: ucsbattle.ru в within three business days after the end of the Competition.

8. **Final provisions**

8.1. The competition is organized in accordance with the legislation of the Russian Federation (applicable law).

8.2. Registration of a Participant in accordance with the procedure provided for in Section 4 of these Regulations means that the Participant unconditionally agrees to all the conditions and rules of the Competition specified in the Regulations.

8.3. In everything that is not regulated by the Regulation, the parties are guided by the current legislation of the Russian Federation.

8.4. All disputes and disagreements that arise in connection with the organization and conduct of the Competition are subject to negotiation.

8.5. If, for any reason, this Competition in any part cannot be conducted as planned, including reasons caused by malware infection, Internet problems, defects, manipulation, unauthorized interference, falsification, technical problems, or any reason beyond the control of the Competition Organizer that distorts or affects the performance, safety, integrity or proper conduct of the Competition, the Organizer may, at its sole discretion, temporarily suspend the Competition. In this case, the duration of the Competition will be proportionally extended for the duration of the suspension of the Competition.

8.6. The Organizer of the Competition reserves the right to change the terms of this Regulation and the procedure for holding the Competition, as well as to refuse to hold it. At the same time, the Organizer of the Competition undertakes to notify the Participants about these actions by posting the current version of the Regulations on the Competition Website or by sending a corresponding notification.