Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А.Бонч-Бруевича
Кафедра Защищенных систем связи

Опыт проведения всероссийских киберучений и летних научных студенческих школ

Красов А.В., Ушаков И.А.

Опыт проведения всероссийских киберучений и летних научных студенческих школ

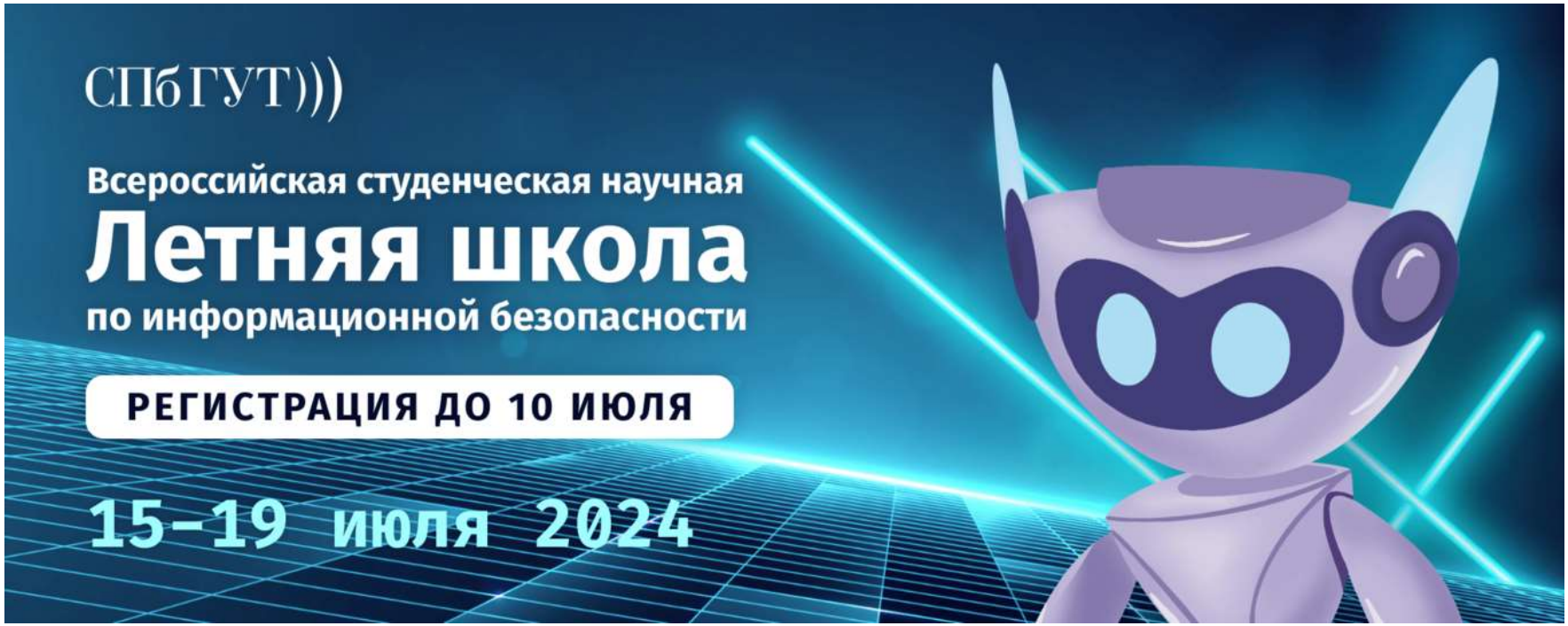
- ✓ Киберучения реализуется в рамках субсидии «Олимпиады» ФЦП «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации»;
- ✓ С 2021 года федеральный проект реализуется под руководством Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации (Минцифры России) через свои подведомственные образовательные организации: МТУСИ, СПбГУТ, ПГУТИ, СибГУТИ.
- ✓ Методическое руководство и сопровождение осуществляет Федеральное учебно-методическое объединение в системе высшего образования по укрупнённой группе специальностей и направлений подготовки 10.00.00 «Информационная безопасность» (ФУМО ВО ИБ).




Всероссийская летняя школа по Информационной безопасности

ФУМО по УГСН 10.00.00 Информационной безопасности.

ФЦП Информационная безопасность



Всероссийская летняя школа по Информационной безопасности

В ВЛШ приняли участие 22 команды из 5 федеральных округов!

Всероссийская летняя школа по Информационной безопасности

День		
15.07.24 понедельник	СПбГУТ)))	Открытие летней школы
	positive technologies GIS ГАЗИНФОРМ СЕРВИС	
16.07.24 вторник	ASTRA LINUX®	
17.07.24 среда	Эшелон комплексная безопасность	
18.07.24 четверг	infotecs®	
19.07.24 пятница	ELTEX	
		Завершение летней школы

Всероссийская летняя школа по Информационной безопасности

$$\text{рейтинг} = \sum \frac{10}{\text{место в конкурсе}}$$

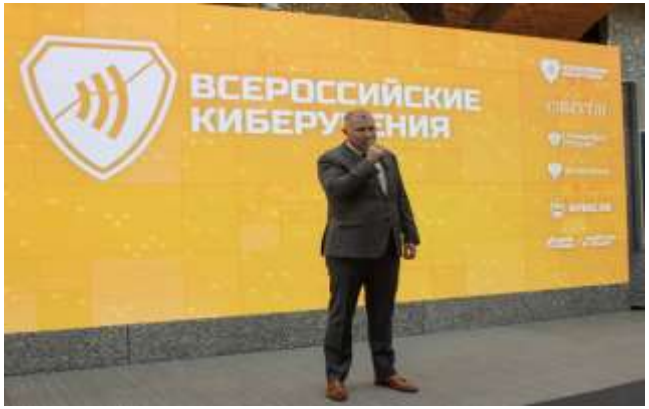
№	ВУЗ	На ква	РТ + ГИС				Astra Linux			НПО Эшелон		ИнфоТекс+ЗСС			Элтекс				Науч докл		Победитель ЛШ	
			балл	мес	балл	мес	тес	балл	мест	балл	мест	Отб(	балл	мест	Тес	отб(	балл	мест	балл	мест	мест	рейти
5	СПбГУТ им. проф. М.А.Бонч-Бруевича		32	1	вне конкурса		90,93	38	2	10	1	4	100(t3)	3	18	9	вне кон	0		11	1	24,24
2	Российский государственный университет нефти и газа (национальный исследовательский университет) имени И.М. Губкина		0	4	89(t2)	4	93,79	38	1	9(t1)	2	2	100(t4)	4	23	2	6	4	9	8	2	23,75
11	МГТУ им. Н.Э. Баумана		0	4	94	2	77,04	48	5	9(t2)	3	1	100(t1)	1	18	10	6	4	9	8	3	22,83
8	Северный (Арктический) федеральный университет		0	4	100	1	66,67	58	6	7(t1)	7	4	100(t2)	2	22	4	6	4	14	4	5	19,35
7	МТУСИ		0	4	89(t1)	3	90,93	37	4	6	9	5	0	17	15	15	0	16	18	1	4	17,74
13	Санкт-Петербургский государственный морской технический университет		9	3	49(t1)	9	74,44	0	16	3(2)	12	4	67	6	18	11	7,5	1		11	11	16,26
1	Вятский государственный университет		0	4	66	6	78,89	37	10	8(t2)	5	3	67	5	17	14	0	16	16	3	6	11,04
10	ФГБОУ ВО «КНИТУ»		0	4	54(t1)	7	90,19	38	3	7(t2)	8	5	52	11	22	3	5	7	12	5	7	10,89
6	ГУМРФ им. адмирала С. О. Макарова		0	4	34	14	56,67	0	20	3(t1)	11	4	50	7	19	7	7	2	10	7	14	10,87
17	ФГБОУ ВО "Уральский государственный экономический университет"		0	4	49(t2)	10	65,00	38	14	0	16	5	0	17	16	14	2	10	17	2	8	9,68
21	Петербургский колледж телекоммуникаций им. Э.Т.Кренкеля		0	4	31(t1)	15	80,46	38	8	2(t2)	15	4	50	8	21	6	6,5	3	5	10	12	9,08
18	ТУСУР		23	2	37	13	71,21	38	11	8(t1)	4	5	0	17	18	12	2	10		11	9	8,79
19	Санкт-Петербургский Политехнический Университет Петра Великого		0	4	77	5	70,00	38	12	8(t3)	6	4	33(t1)	9	16	14	0	16	11	6	10	8,15
3	Балтийский Федеральный Университет им. И. Канта		0	4	43	11	83,43	38	7	5	10	5	12	15	17	13	3	9		11	13	6,82
20	ИКТИБ ИТА ЮФУ		0	4	54(t2)	8	68,33	36	13	0	16	4	33(t2)	10	29	1	5	7	5	10	15	6,70
9	ФГБОУ ВО "ПГТУ"		0	4	31(t2)	16	79,63	38	9	2(t1)	14	5	32	12	22	5	2	10	8	9	16	6,33
15	ФГБОУ ВО Уфимский университет науки и технологий		0	4	39	12	70,55	0	18	0	16	5	0	17	19	8	2	10	9	8	18	5,69
16	ДонНТУ		0	4	22(t2)	18	62,22	33	15	3(t3)	13	5	14	14	19	12	2	10		11	17	5,59
14	КузГТУ		0	4	16	19	73,89	0	17	1	15	5	29	13	18	13	0	16		11	19	5,07
4	ГУАП		0	4	22(t1)	17	61,94	0	19	0	16	5	0	17	21	0	0	16		11	20	4,82
12	Дагестанский Государственный Технический Университет		0	4	0	20	21,67	0	21	0	16	5	0	17	20	8	1	15		11	21	4,77

			% решенных заданий	% решенных заданий	Тестирование	Практическое задание	Число заданий (10)	1-4 ИнфоТекс; 5 не проходной	% решенных заданий зал.ИнфоТекс; син.ЗСС (макс 73)	Тест	место по отбору

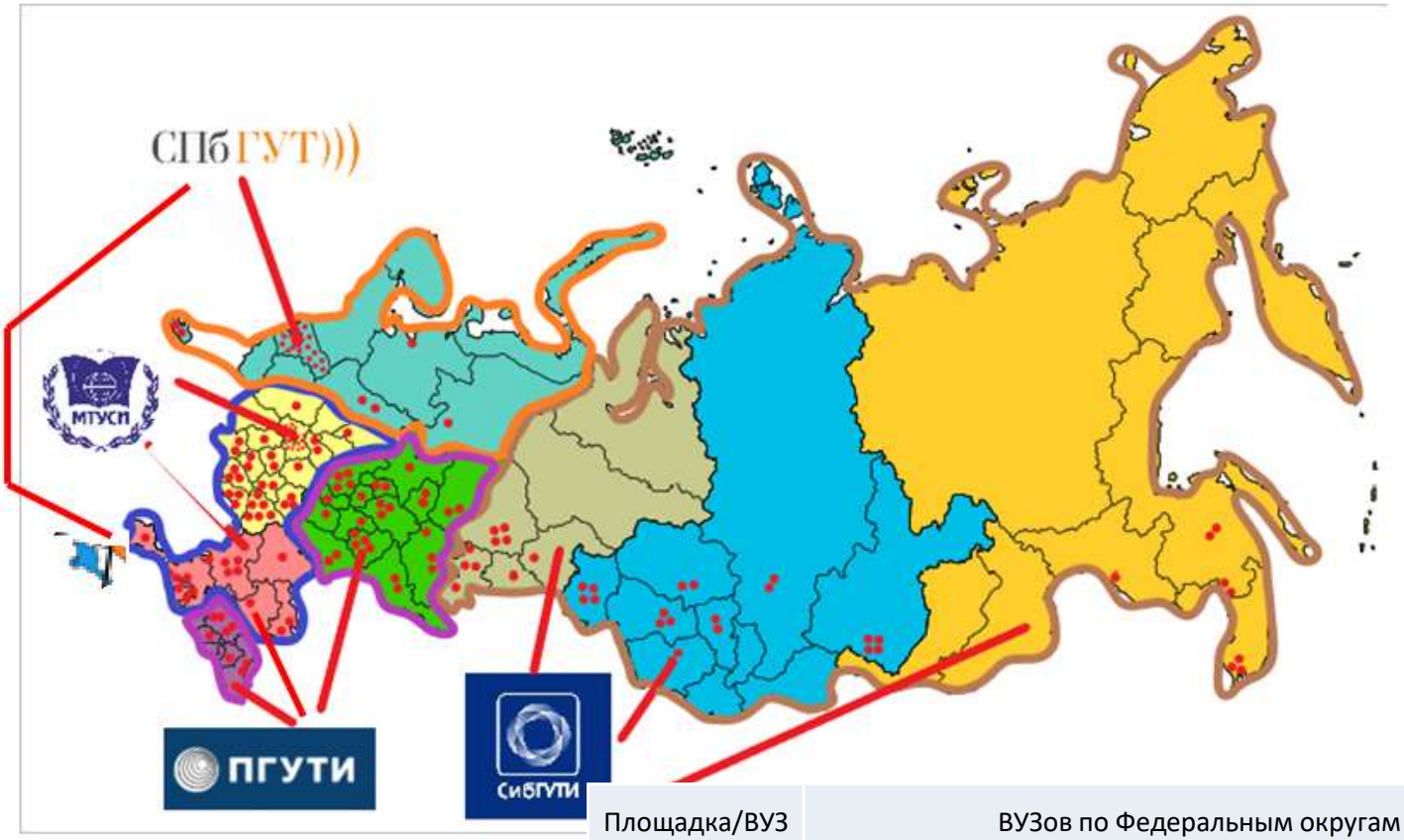
СПбГУТ им. проф. М.А.Бонч-Бруевича в номинации ГИС выступал вне конкурса, т.к. студенты работали по совместительству в компании ГазИнформСервис

Опыт проведения всероссийских киберучений и летних научных студенческих школ

- 1-й этап (Отборочный)
  - Заочный формат
  - Исследование сетевого трафика
  - Исследования дампа оперативной памяти
- 2-й этап (Региональный)
  - Очный формат
  - Цифровая криминалистика
- 3-й этап (Всероссийский)
  - Очный формат
  - Цифровая криминалистика



Опыт проведения всероссийских киберучений и летних научных студенческих школ



Площадка/ВУЗ	ВУЗов по Федеральным округам						Кол-во ВУЗов на площадке
МТУСИ	Центральный	55					55
СПбГУТ	Северо-Западный	22	СПбГУТ принимает финал очного всероссийского этапа 16 команд ВПО и 2 команды СПО		Южный	18	40
ПГУТИ	Приволжский	29	Северо-Кавказский	8	Южный	16	53
СибГУТИ	Сибирский	19	Дальневосточный	8	Уральский	10	37
					Итого:		185

Опыт проведения всероссийских киберучений и летних научных студенческих школ

Опыт проведения всероссийских киберучений и летних научных студенческих школ

Отборочный этап (типовой сценарий)

Рис.1 - Подбор пароля по протоколу SSH

Рис.2 - Управление Linux-системой при помощи шелла

Опыт проведения всероссийских киберучений и летних научных студенческих школ

- Атака должна быть видна в трафике.
- Компьютерная атака должна быть комплексной, включать несколько этапов.
- Эмуляция успешных и безуспешных (отвлекающих) атак.
- IP-адресация включает внешние IP-адреса.
- Обязательно самостоятельное прорешивание задания.
- Формирование заданий с учетом возможностей средств анализа трафика.
- Для усложнения задания можно использовать обфускацию скриптов, протоколы с шифрованием, простую стеганографию в сетевых протоколах.

Опыт проведения всероссийских киберучений и летних научных студенческих школ

Отборочный этап

Участники

Подготовительный этап

1

1) Получение зашифрованного архива
2) Подготовка рабочего места

WinRAR

Решение задания

2

1) Получение пароля от архива
2) Решение задания

Организаторы

3

1) Отправка отчета
2) Проверка задания
3) Составление рейтинга

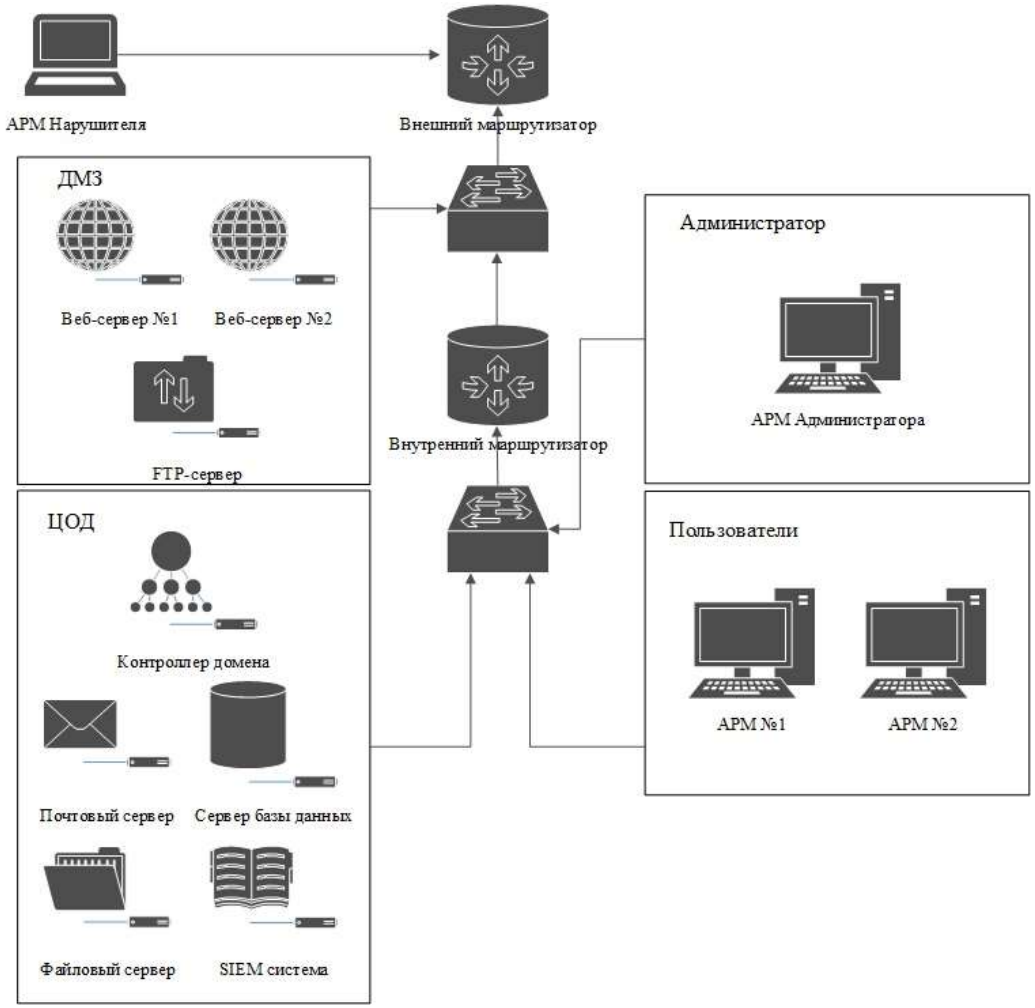
Опыт проведения всероссийских киберучений и летних научных студенческих школ

Отборочный этап (Критерии оценки)

- Дата и время проведения компьютерных атак (далее - КА).
- IP-адрес атакующего.
- IP-адрес жертвы.
- Вид КА.
- Успешность КА (успешна или неуспешна и почему).
- В случае успешности КА определить ее влияние на систему.
- В случае успешности КА определить дальнейшие действия злоумышленника.

Опыт проведения всероссийских киберучений и летних научных студенческих школ

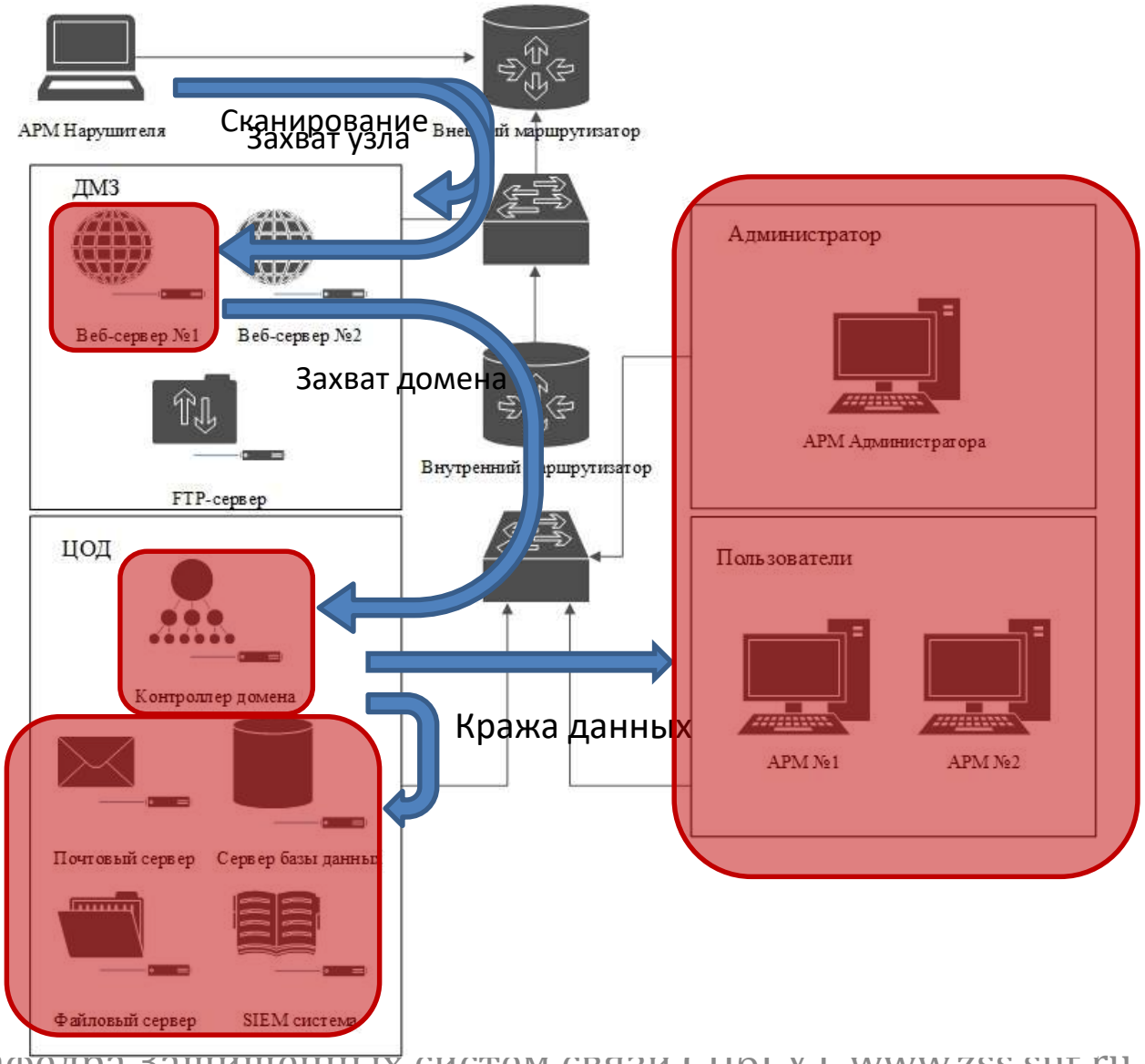
Региональный этап (схема инфраструктуры)



На типовую инфраструктуру будет проведена серия компьютерных атак:

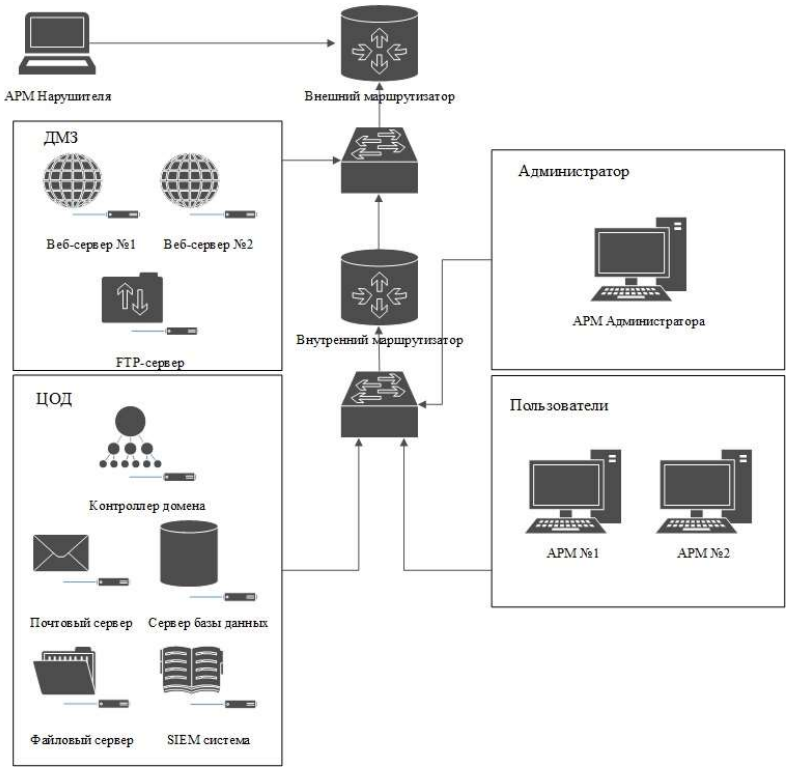
- ✓ Разведка.
- ✓ Вооружение.
- ✓ Доставка.
- ✓ Эксплуатация.
- ✓ Установка.
- ✓ Управление и взаимодействие.
- ✓ Воздействие на ресурс.

Опыт проведения всероссийских киберучений и летних научных студенческих школ



Опыт проведения всероссийских киберучений и летних научных студенческих школ

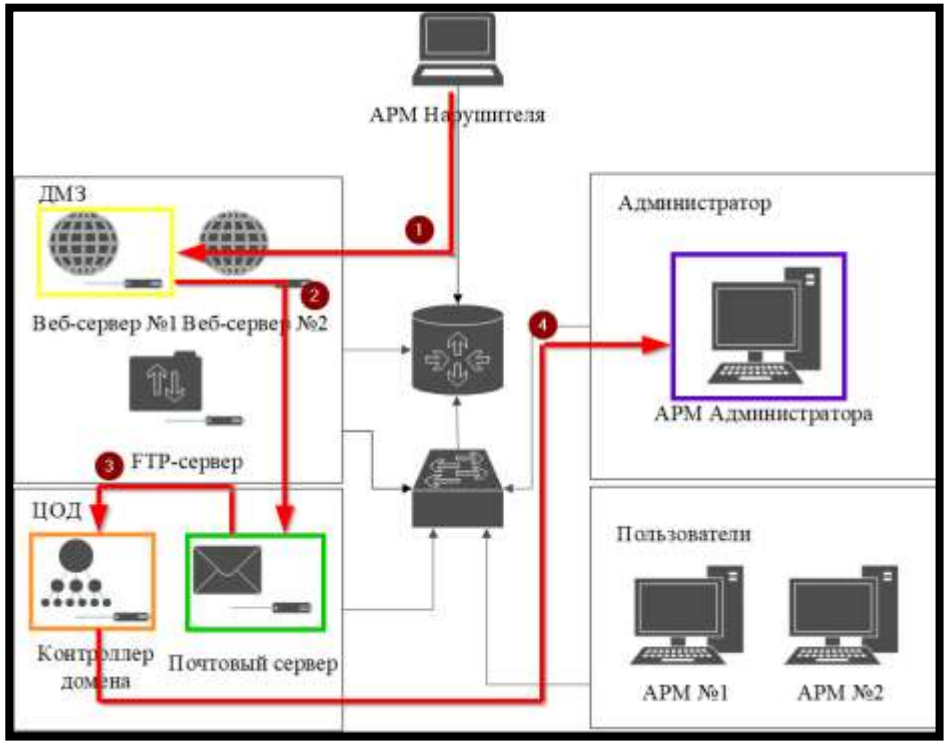
Всероссийский этап (схема инфраструктуры)

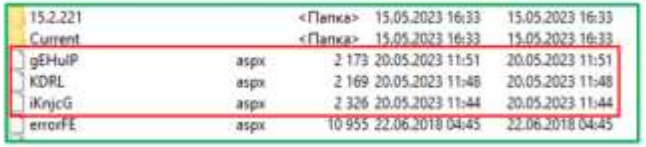


После выявления компьютерной атаки (КА) командам необходимо произвести максимально подробное описание КА с обязательным указанием следующих пунктов:

- ✓ дата и время проведения КА;
- ✓ IP-адрес атакующего;
- ✓ IP-адрес жертвы;
- ✓ вид КА (Например: подбор пароля к сервису FTP, эксплуатация уязвимости MS17-010, XSS, сканирование и тд.)
- ✓ успешность КА (успешна или неуспешна и почему, скриншот);
- ✓ в случае успешности КА определить ее влияние на систему;
- ✓ в случае успешности КА определить дальнейшие действия злоумышленника.

Опыт проведения всероссийских киберучений и летних научных студенческих школ



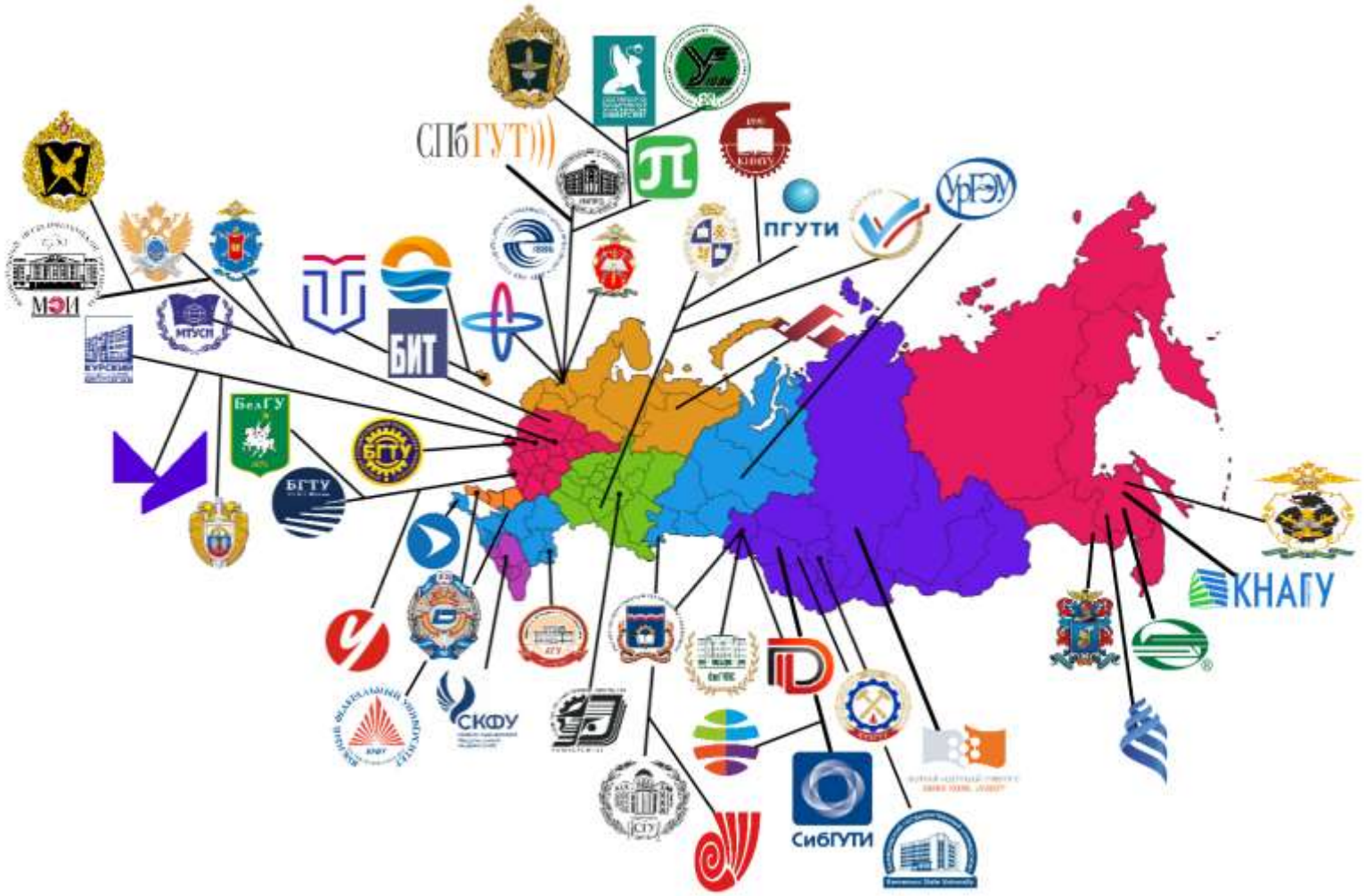


Шаги атаки:

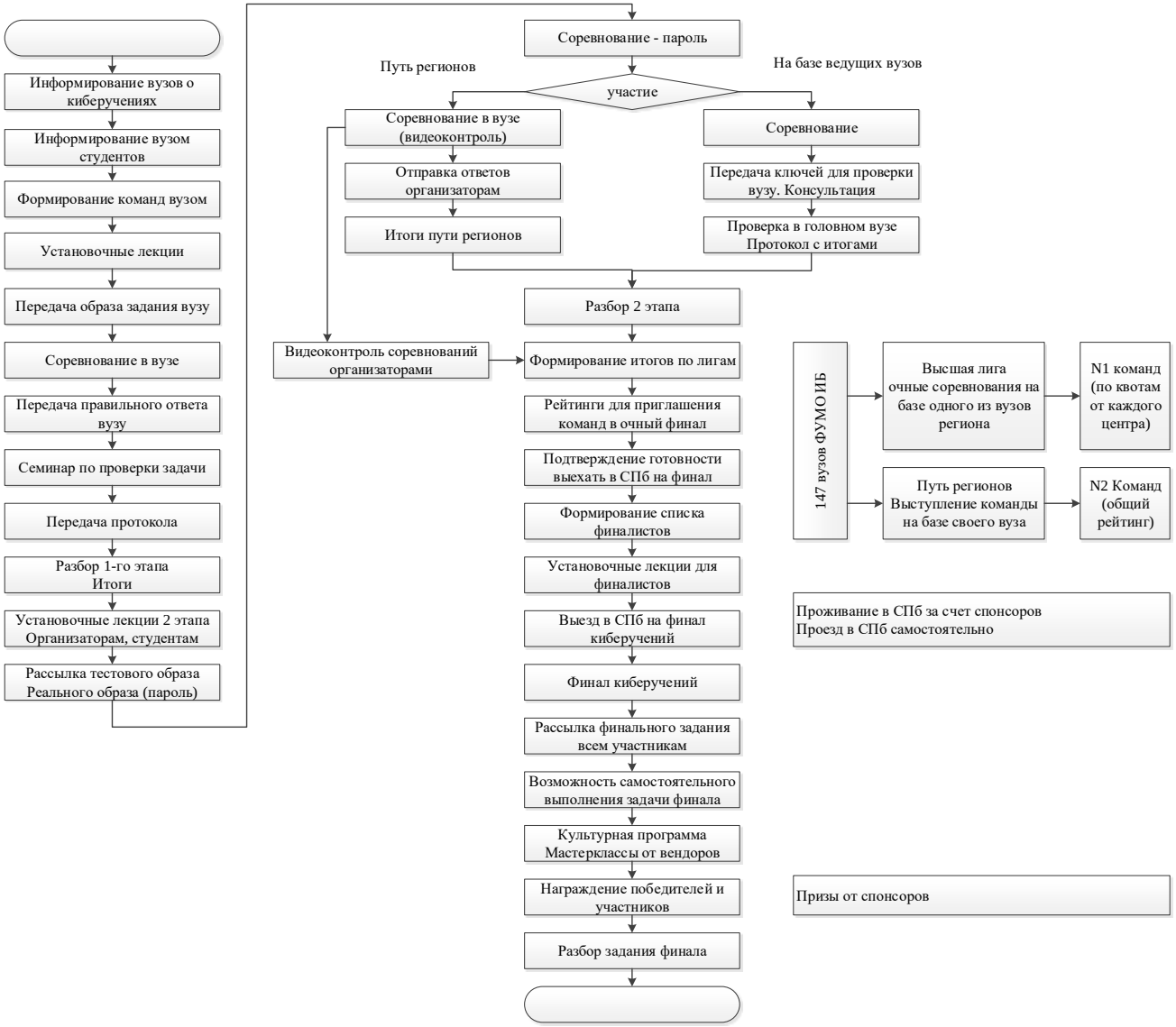
- ✓ Сканирование
- ✓ Подбор пароля WordPress (веб-сервер №1)
- ✓ Установка вредоносного плагина на WordPress (веб-сервер №1)
- ✓ Повышение привилегий на WordPress (веб-сервер №1)
- ✓ Закрепление на веб-сервере
- ✓ Эксплуатация уязвимости ProxyLogon почтового сервера
- ✓ Создание пользователя с правами администратора домена
- ✓ Закрепление на почтовом сервере
- ✓ Боковое перемещение на контроллер домена
- ✓ Воздействие на компьютер администратора

Опыт проведения всероссийских киберучений и летних научных студенческих школ

Участники Всероссийский соревнований за последние 3 года



Предложения о организации соревнований 2025 г.



Предложения о организации соревнований 2025 г.

- Информирование вузов о киберучениях
- Информирование вузом студентов
- Формирование команд вузом
- Установочные лекции
- Передача образа задания вузу
- Соревнование в вузе
- Передача правильного ответа вузу
- Семинар по проверки задачи
- Передача протокола
- Разбор 1-го этапа
  Итоги

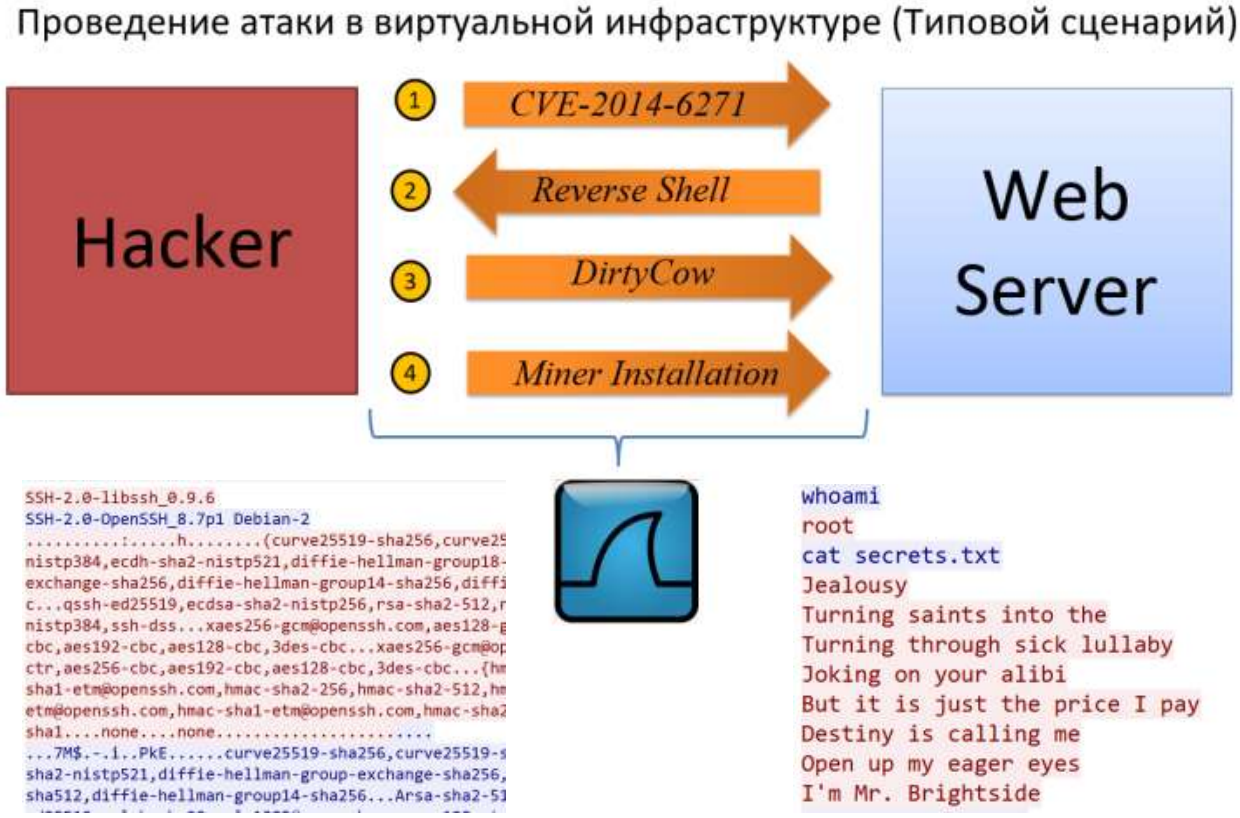
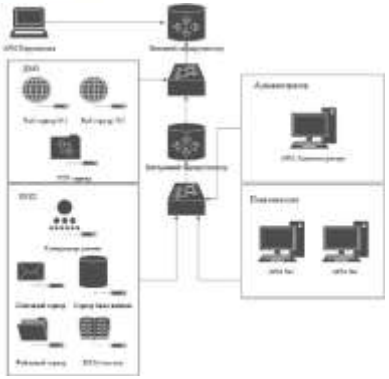


Рис.1 - Подбор пароля по протоколу SSH

Рис.2 - Управление Linux-системой при помощи шелла

Предложения о организации соревнований 2025 г.



Установочные лекции 2 этапа
Организаторам, студентам

Рассылка тестового образа
Реального образа (пароль)

Соревнование - пароль

Путь регионов

На базе ведущих вузов

участие

Соревнование в вузе
(видеоконтроль)

Отправка ответов
организаторам

Итоги пути регионов

Соревнование

Передача ключей для проверки
вузу. Консультация

Проверка в головном вузе
Протокол с итогами

Разбор 2 этапа

Видеоконтроль соревнований
организаторами

Формирование итогов по лигам

Предложения о организации соревнований 2025 г.

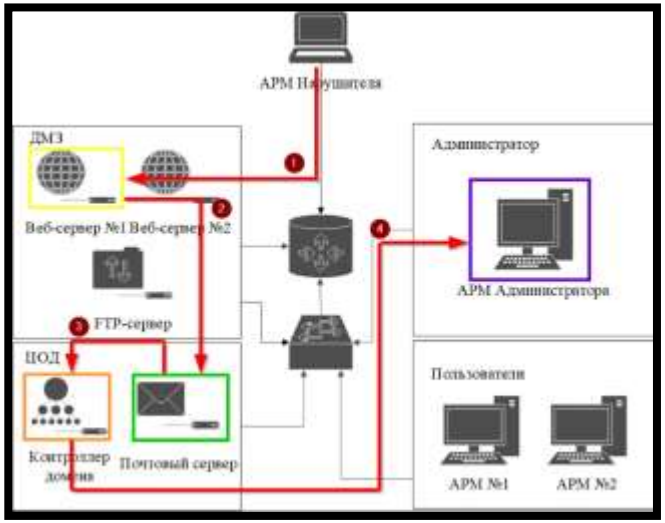
- Формирование итогов по лигам
- Рейтинги для приглашения команд в очный финал
- Подтверждение готовности выехать в СПб на финал
- Формирование списка финалистов
- Установочные лекции для финалистов
- Выезд в СПб на финал киберучений
- Финал киберучений
- Рассылка финального задания всем участникам
- Возможность самостоятельного выполнения задачи финала
- Культурная программа Мастерклассы от вендоров
- Награждение победителей и участников
- Разбор задания финала

147 вузов ФУМО ИБ

- Высшая лига очные соревнования на базе одного из вузов региона → N1 команд (по квотам от каждого центра)
- Путь регионов Выступление команды на базе своего вуза → N2 Команд (общий рейтинг)

Проживание в СПб за счет спонсоров
Проезд в СПб самостоятельно

Призы от спонсоров



Предложения о организации соревнований 2025 г.

Предложение по плану:

Мероприятия	Даты	Организатор
Рассылка приглашения, регистрация	Апрель	ФУМО ИБ
Отборочный тур	29 апреля	СПбГУТ, вузы
Второй тур	29-30 мая	СПбГУТ, головные вузы ФУМО ИБ
Финал	4-5 октября	СПбГУТ, ……., Управление ФСТЭК по СЗФО РФ; ФУМО ИБ

Контакты

Заведующий кафедрой ЗСС:

Красов Андрей Владимирович, к.т.н., доцент.

E-mail: krasov@inbox.ru

Тел.: (812) 326-31-58

Тел.: +7 921 999 03 14

Адрес: 193232, Санкт-Петербург, пр. Большевиков, д. 22 корп. 1 ауд. 200/1.

Преподавательские: ауд. 205/1, 202/1.

Лаборатории: 204/1, 206/1, 207/1, 338/1, 600/1, 603/1, 613/1.

Сайт кафедры: www.zss.sut.ru