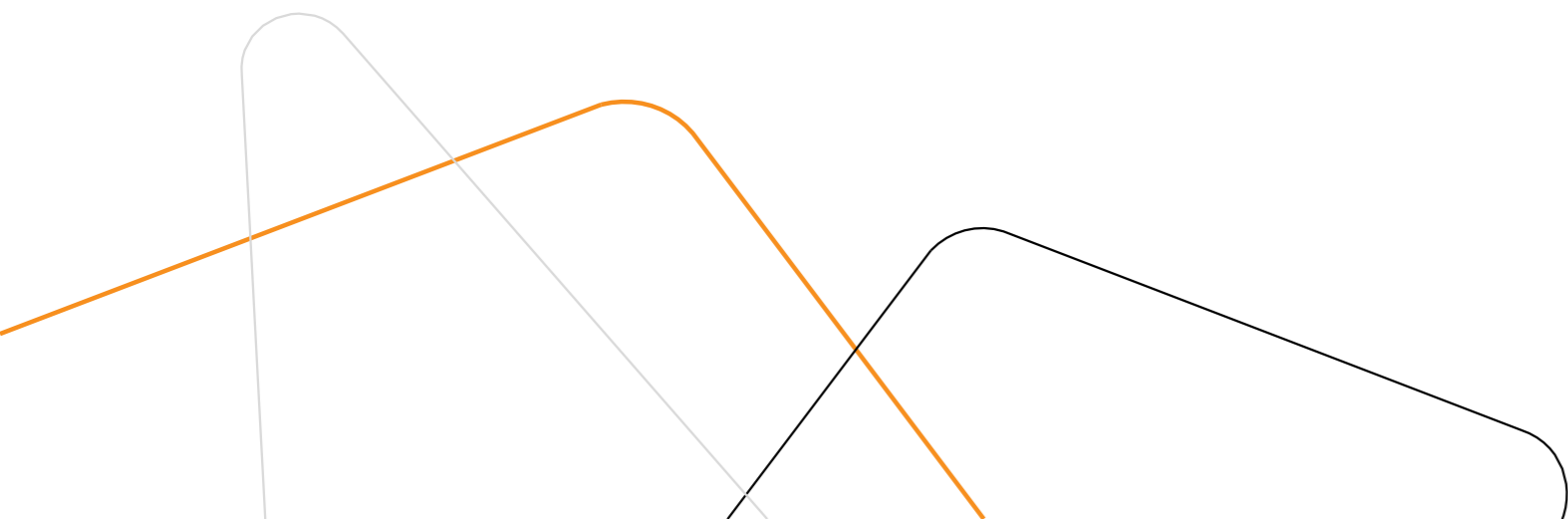


# Киберполигон Amprire

Возможности применения и развития

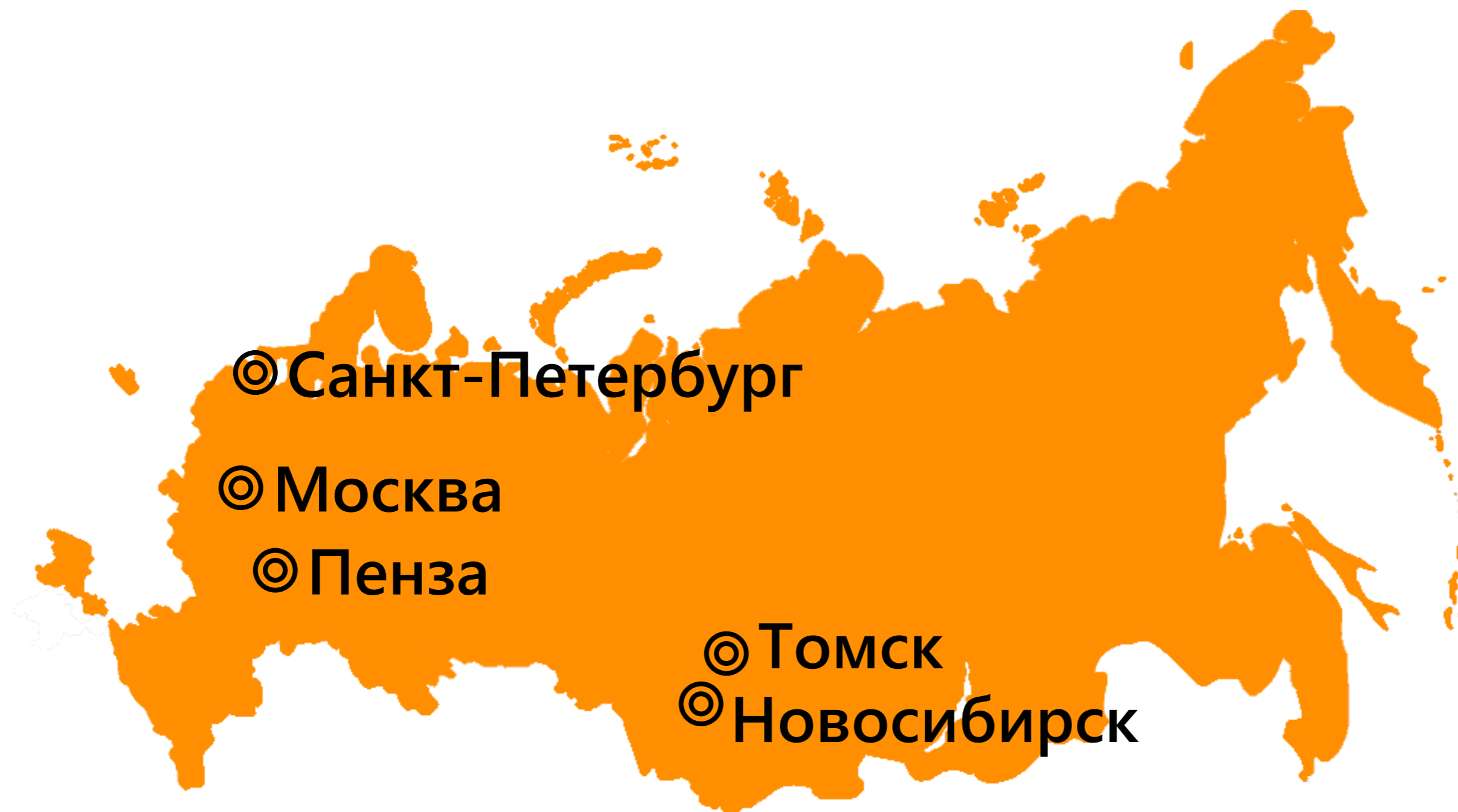




# Сегодня поговорим

- ✓ Про киберполигон Ampire
- ✓ Про сотрудничество с ВУЗами
- ✓ Про разработку шаблонов и сценариев

# Регионы присутствия



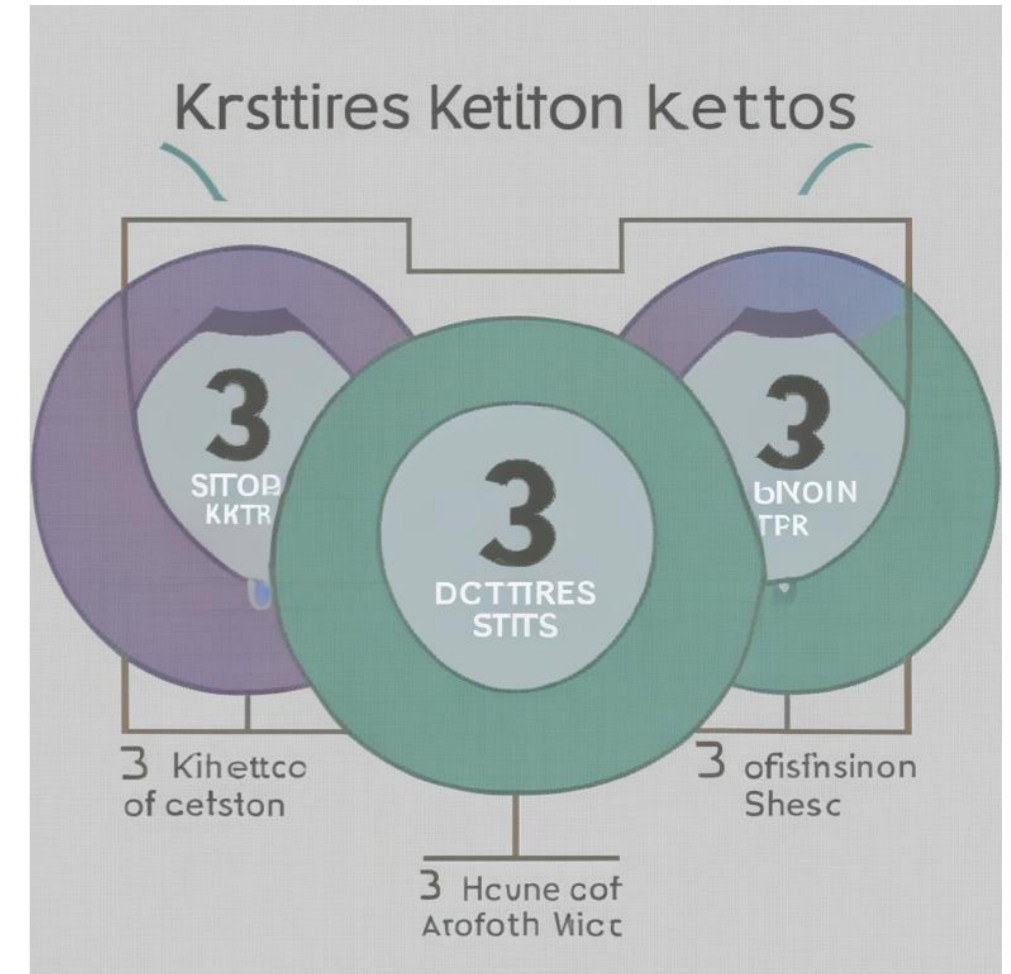
# Три кита ИБ ©ruDALL-E Kandinsky 2.1



Техника



Люди



Процессы

# Проактивная позиция



## Не можем повлиять

- 1) Сам факт атаки
- 2) Квалификация атакующего
- 3) Инструментарий
- 4) Объём ресурсов

## Можем повлиять

- 1) Стоимость атаки
- 2) Скорость реакции
- 3) Содержание реакции
- 4) Собственный опыт
- 5) Планы и изменения

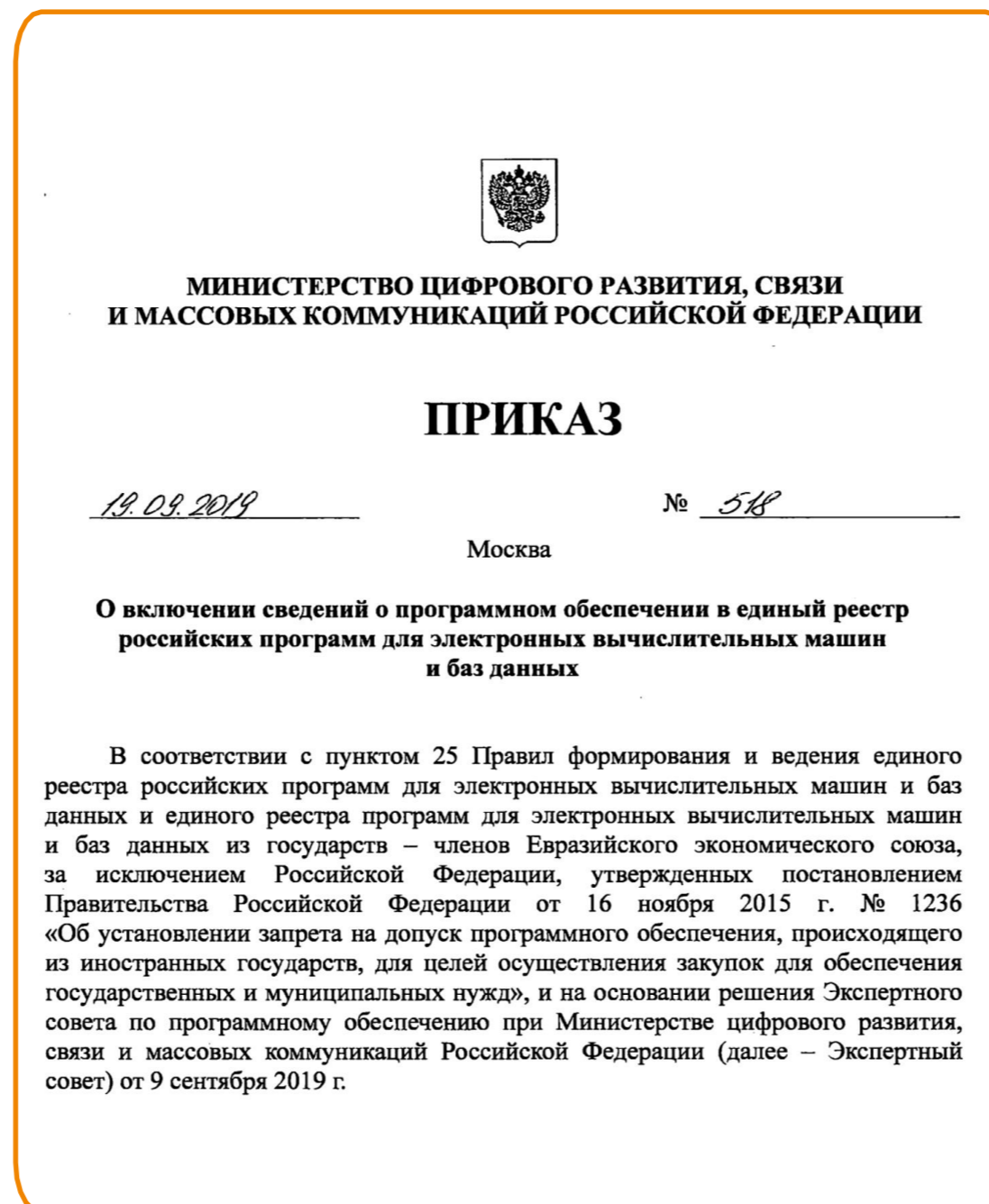
Способность действовать в **экстренной ситуации** зависит не от уровня **знаний**, а от уровня **подготовки**.



# Единый реестр российских программ для ЭВМ и БД



- **Класс ПО:** Информационные системы для решения специфических отраслевых задач
- **Сайт производителя:**
- **Дата регистрации:** 20 Сентября 2019
- **Решение уполномоченного органа:** Приказ Минкомсвязи России от 19.09.2019 №518





# Целевая аудитория

- Школьники и студенты с базовым знанием TCP/IP сетей, которые планируют работать в сфере защиты информации.
- ИБ-специалисты, которые хотели бы выделиться среди других кандидатов глубокими знаниями в определённых областях.
- ИТ-специалисты: новички и те, кто хотел бы увеличить перечень навыков в резюме.



Наша учебно-тренировочная платформа содержит сценарии различной сложности для проведения киберучений, сертификационных тестов и отработки необходимых навыков.



# Цели киберучений



Создать собственный SOC



Научиться выявлять компьютерные атаки



Наладить взаимодействие между подразделениями



Устранить существующие уязвимости

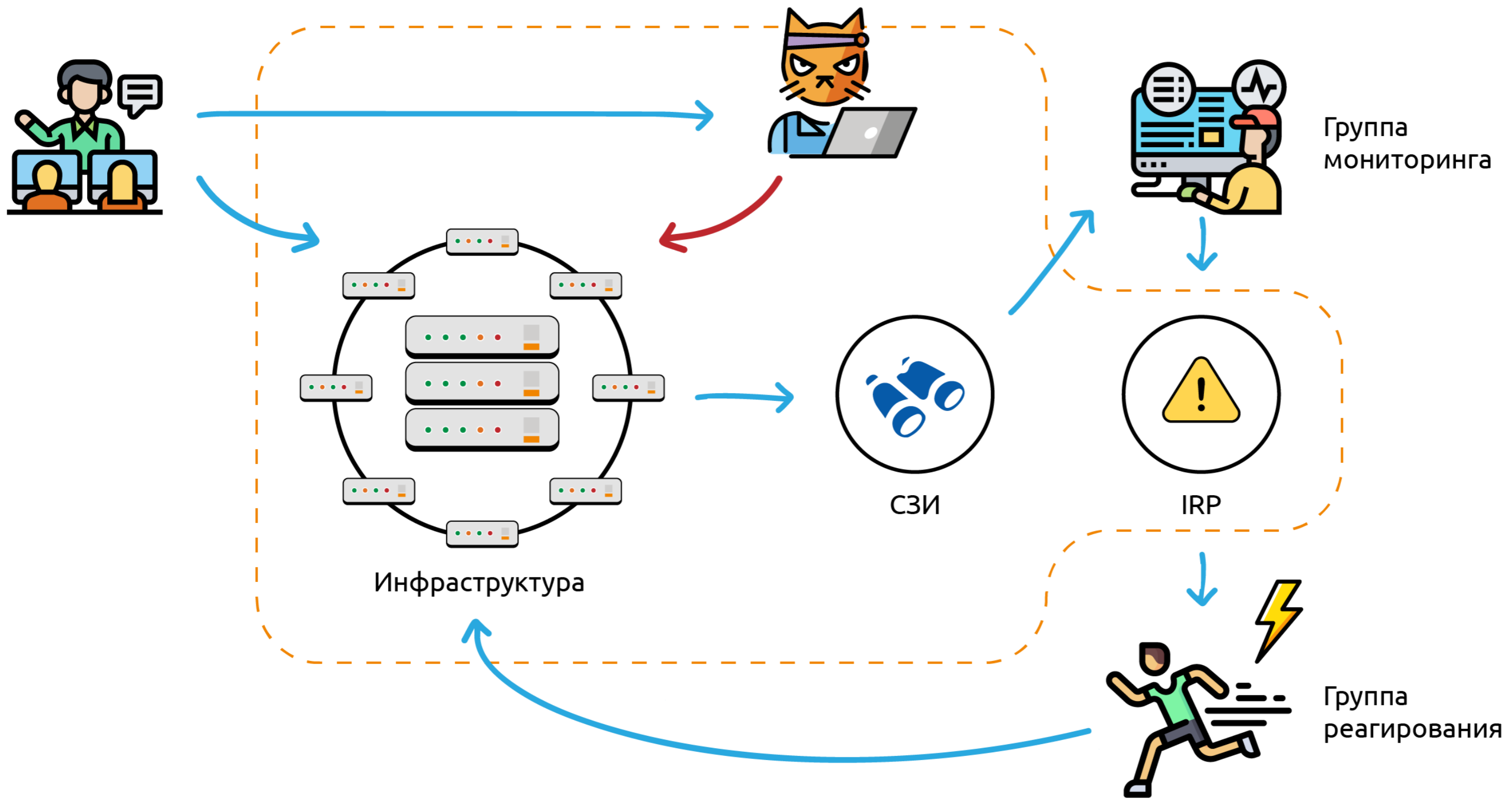
# Проведение киберучений на базе ПК



**Киберучения** – это процесс моделирования целевых компьютерных атак на некую ИТ-инфраструктуру с акцентом в сторону отработки навыков защиты:

- ✓ анализ событий ИБ;
- ✓ регистрация и расследование инцидентов ИБ;
- ✓ устранение причин успешного выполнения КА;
- ✓ командное взаимодействие.





# СЗИ



- ✓ VipNet IDS NS
- ✓ VipNet IDS HS
- ✓ VipNet TIAS
- ✓ IDS/IPS Suricata

- ✓ ELK
- ✓ Security Onion
- ✓ IDS/IPS Snort

**И почти любые другие**



# Типы проводимых занятий



1

Киберучения

2

Анализ защищённости и аудит ИТ-инфраструктуры виртуальной организации

3

Противодействие группе реальных нарушителей (концепция Red Team и Blue team)

4

Лабораторные работы по настройке средств безопасности и прикладных сервисов

5

Киберквесты



# Организационные **преимущества**

1

Круглосуточная готовность проводить занятия. Старт тренировки через 2 минуты после начала занятия.

2

Возможность зарабатывать на ДПО и повышении квалификации.

3

Бессрочная лицензия. Продолжит работать даже по истечению срока оплаченной технической поддержки.

4

Возможность заказной разработки тренировочной ИТ-инфраструктуры и сценариев.



# Оснащение лабораторий



Лаборатория на основе Учебно-тренировочной платформы Ampire выполняет требования федеральных государственных стандартов к материально-техническому и учебно-методическому обеспечению программ по **специальностям в информационной безопасности** и позволяет региону в короткие сроки подготовить специалистов, обладающих практическими навыками выявления компьютерных атак, расследования инцидентов информационной безопасности, реализации защитных мер для нейтрализации существующих недостатков безопасности в информационных сетях общего и специального назначения (связь, энергетика, финансовая сфера, ТЭК, промышленные предприятия различных отраслей).



# В поставку **входят**

✓ Программное обеспечение  
Ampire

✓ Подготовка преподавателей для  
работы с комплексом

✓ Рабочая программа,  
методические материалы

✓ Техническая поддержка

✓ Обновление контента

**Комплекс продолжит работать и  
без техподдержки**



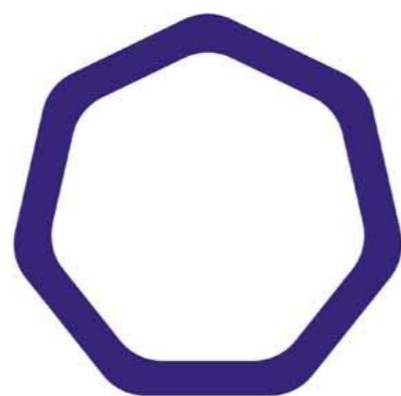




14

B 23

# Сотрудничаем с ВУЗами



**МТУСИ**  
Московский технический  
университет связи и информатики






# Пример **ГОТОВОГО** класса



# Поддерживаем Олимпиаду



Перспективный мониторинг



Всероссийская Студенческая Олимпиада по Информационной Безопасности

🏆 Завершился финал Всероссийской студенческой олимпиады по информационной безопасности. Лучшими в 2023 году стали:

- 1 место – Даниил Трошкин, студент Академии ФСО России;
- 2 место – Дмитрий Буренок, студент НИУ МИЭТ;
- 3 место – Александр Андреев, студент МТУСИ.

С заданиями на киберполигоне Amprе лучше всех справились:

- Андреев Александр, МТУСИ;
- Романько Максим, РТУ МИРЭА;
- Трошкин Даниил Алексеевич, Академия ФСО России.

Наши искренние поздравления победителям!

🔥 5 👍 1 🍌 1

👁 167 edited 15:11

Перспективный мониторинг



📌 Сегодня на базе Губкинец проходит финал Всероссийской студенческой олимпиады по информационной безопасности. Прямо сейчас ребята выполняют практическое задание на киберполигоне Amprе. За всех искренне боеем и желаем удачи в поисках уязвимостей! 🙌

👍 11

👁 189 16:46

# И мы, и #Мы\_на\_связи



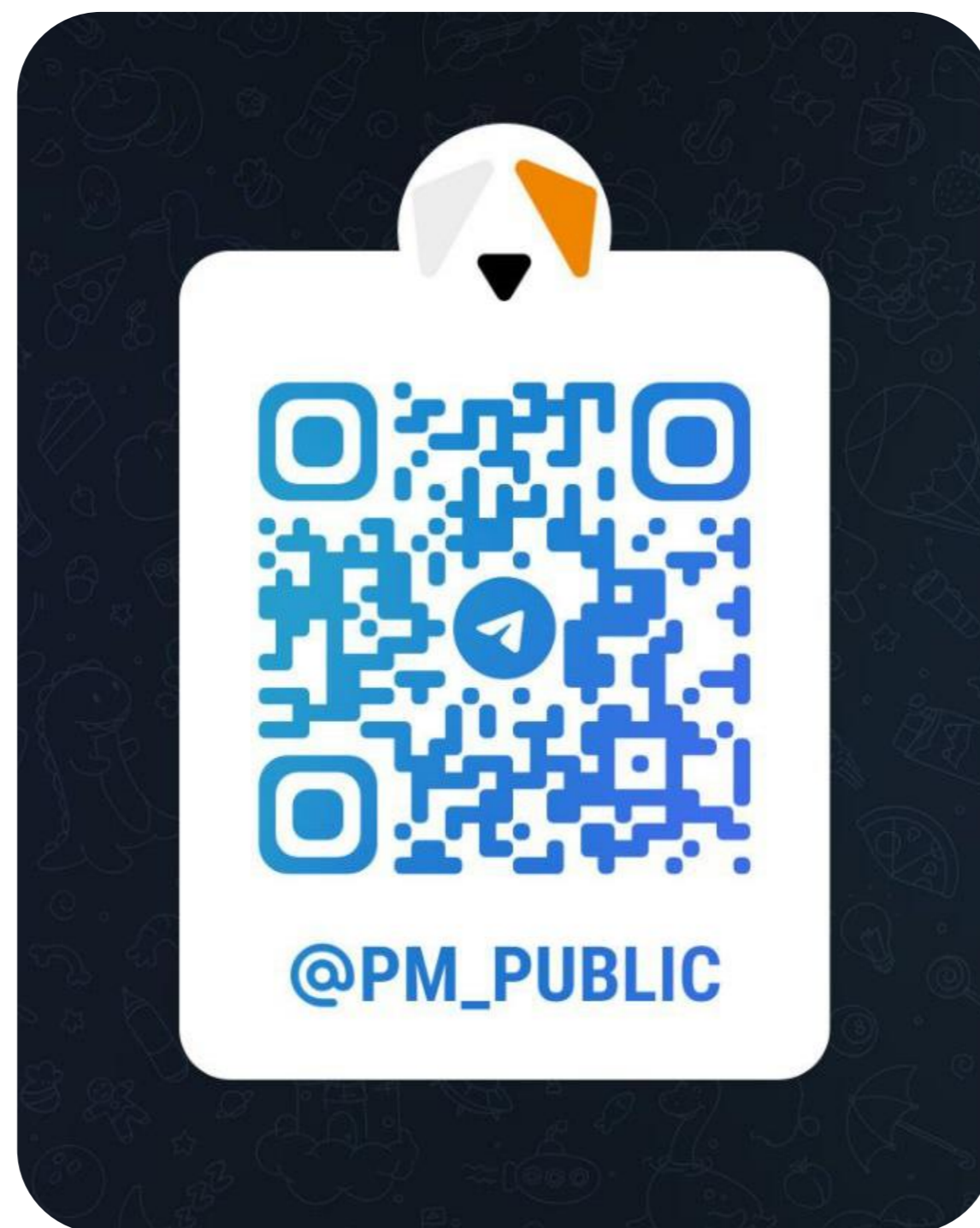
Перспективный мониторинг

Сегодня на форуме #Мы\_на\_связи в Сколково насыщенная программа от Перспективного мониторинга. Только что закончился первый поток киберсоревнований и у нас есть первая команда-победитель! Поздравляем участников и приглашаем следующие команды на второй поток.

👍 6 🔥 4

👁 106 12:33

# Join us **в** **Telegre**



# Как мы можем помочь друг другу

Нужно больше инфраструктур и сценариев!



# Уязвимостей **МНОГО!**





# И понятно, **что**

- ✓ Хочется тренироваться на своих ИТ
- ✓ Хочется тренироваться на своих угрозах
- ✓ Хочется отрабатывать актуальные уязвимости

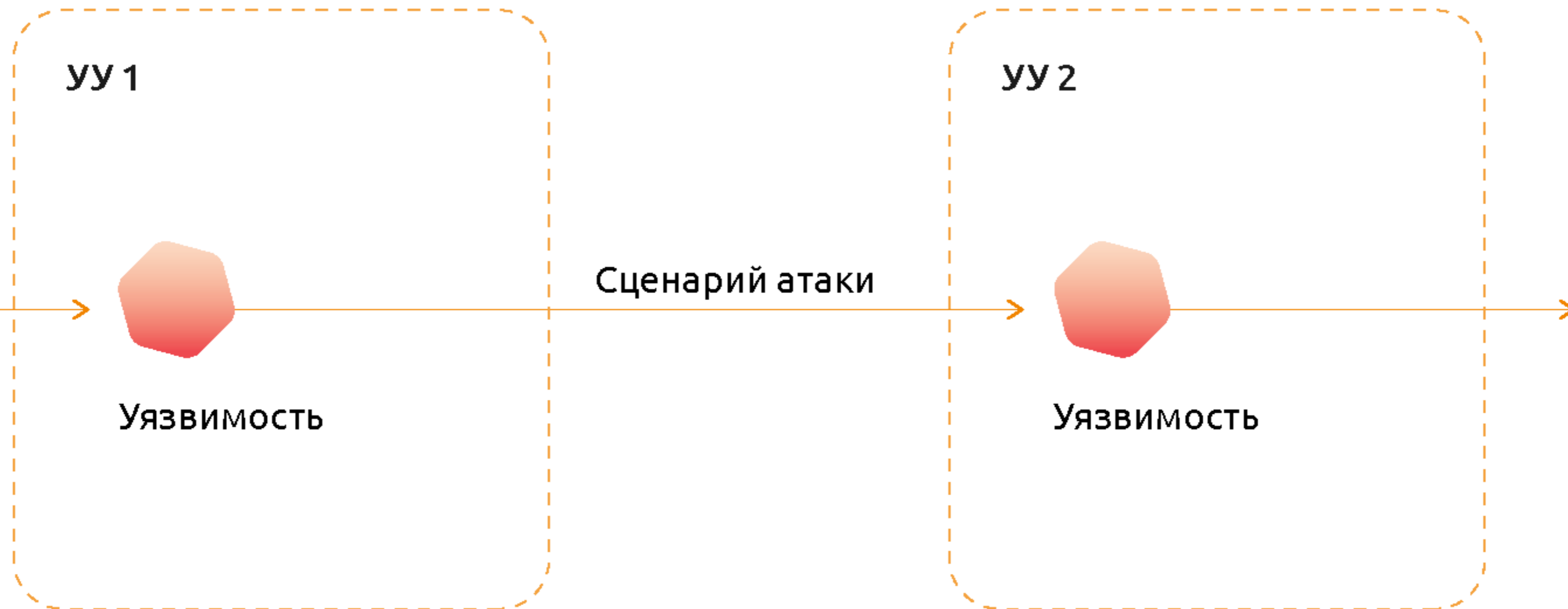
- ✓ Курсач сам себя не напишет.  
(Алиса, как зарегистрироваться в KursatchGPT)
- ✓ «Вы не видите?! Вас много, а я один!»

**Нам есть, чем ответить!**

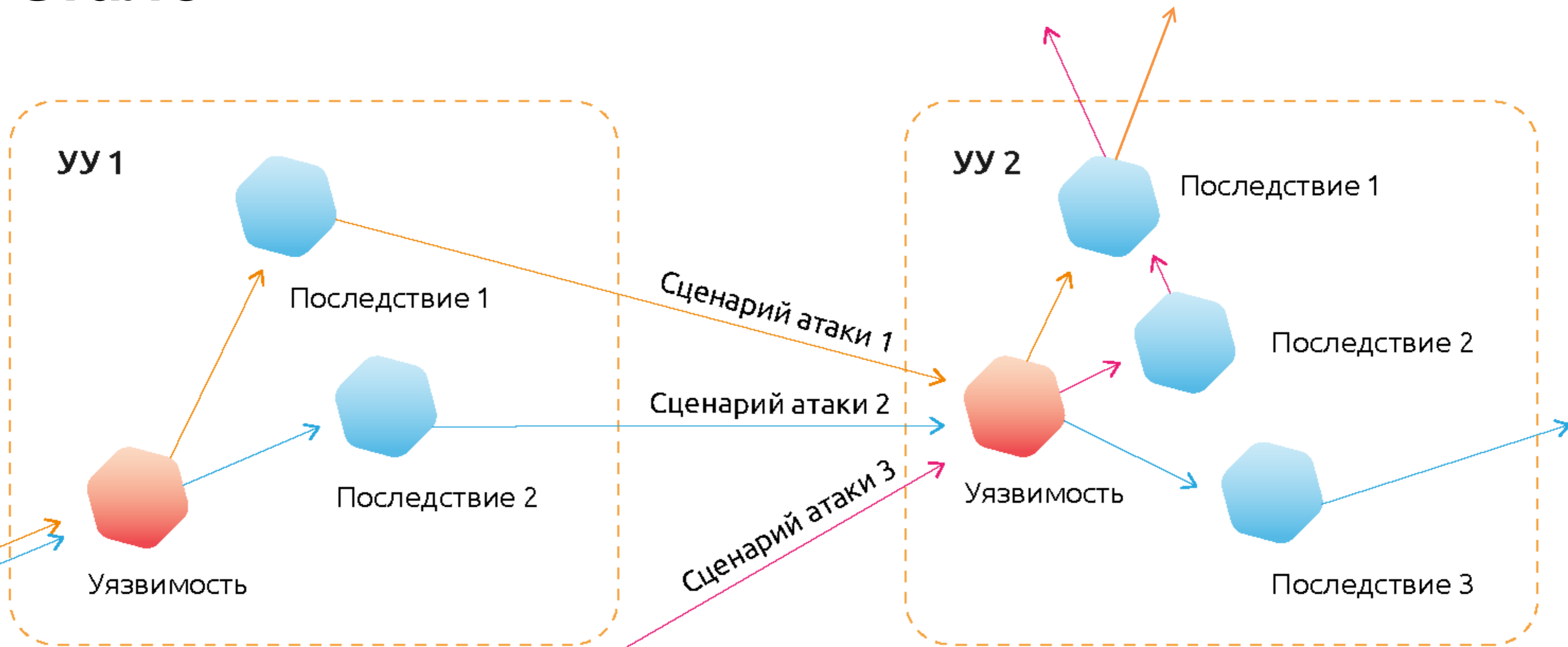


**Идея Конфигуратора** —  
дать возможность преподавателю  
самостоятельно подготавливать шаблон  
организации и формировать вектор атаки

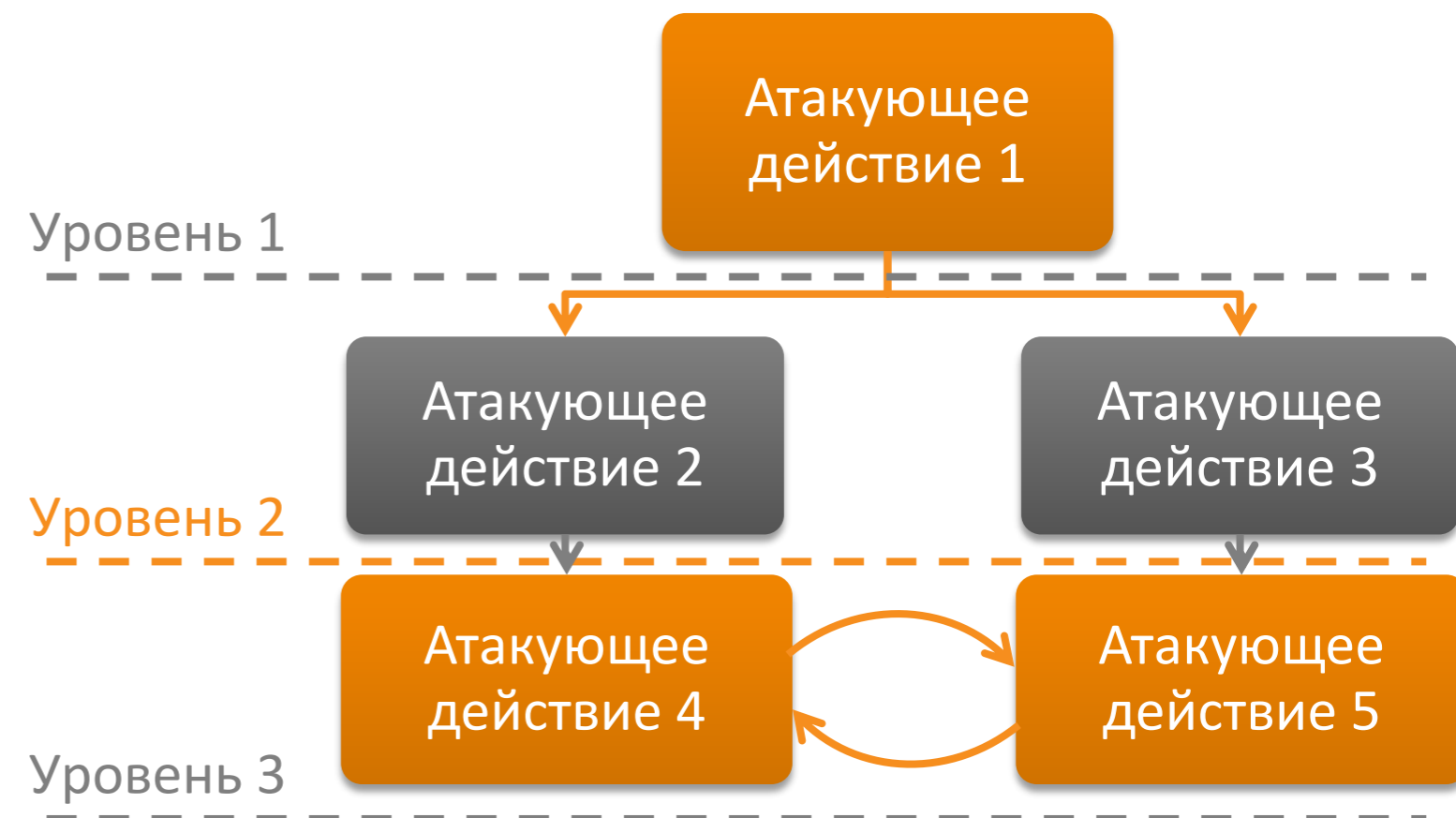
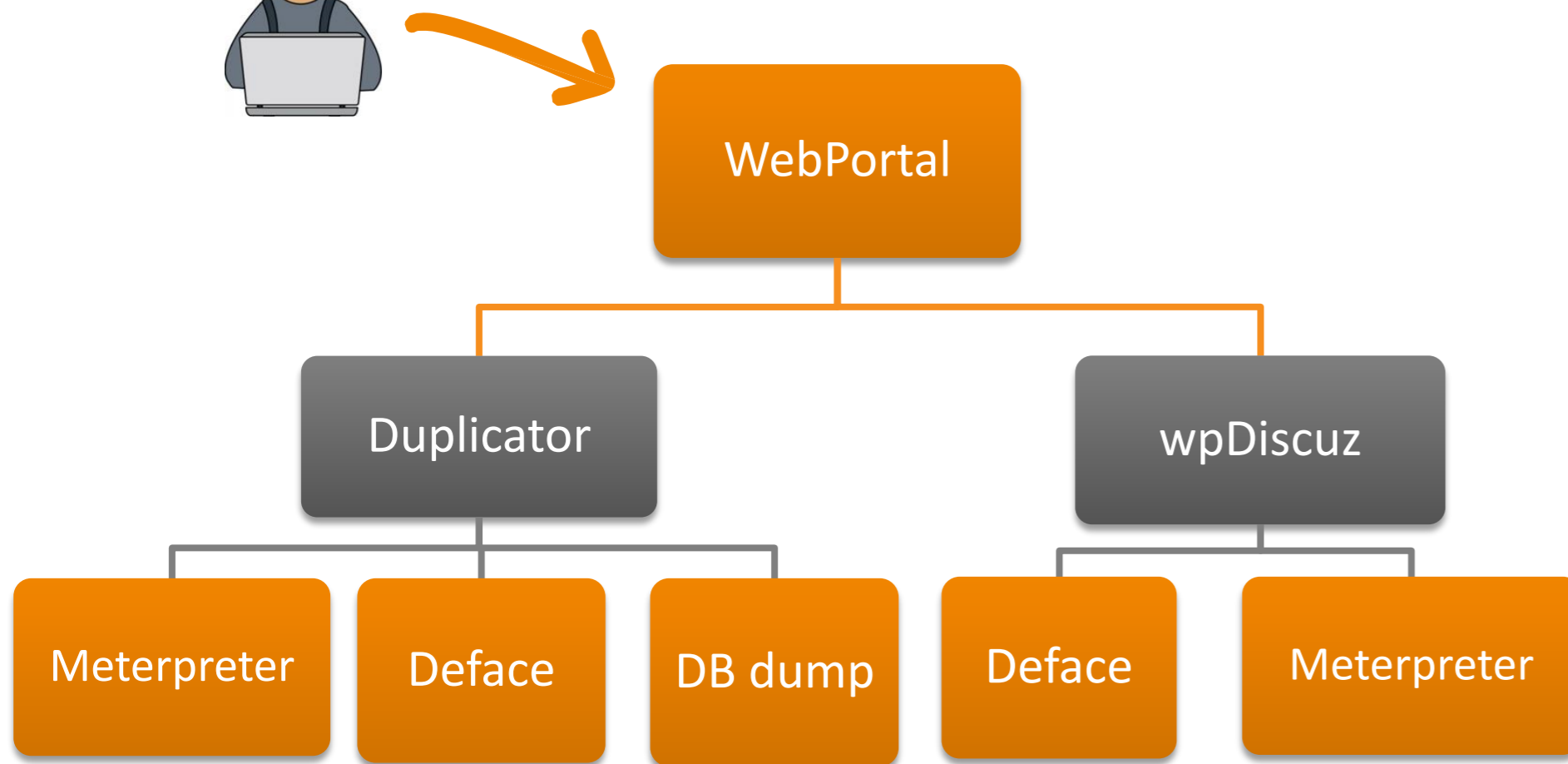
# Было



# Стало




# Конфигуратор



# Конфигуратор







































Шаблоны и сценарии 

**Мои шаблоны**

- Корпоративная сеть предприятия**  
Описание: Корпоративная сеть предприятия Stable version
- Предприятие (конфигуратор)**  
Описание: Каркас шаблона Предприятие для конфигуратора сценариев
- Сеть Телеком-оператора**  
Описание: Сеть Телеком-оператора
- АСУ Siemens**  
Описание: ASU template WinCC Unified
- Астра**  
Описание: Инфраструктура предприятия Астра

**Базовые сценарии** | **Сценарии конфигуратора**

Последствие:  | Уязвимость:



Название ↓	Сложность	Длительность(мин)	Действия
WP Webmin	Средний уровень	90	  
Webmin	Легкий уровень	90	  
Tyumen-SC2-2	Сложный уровень	90	  
Tyumen-SC2-1	Сложный уровень	90	  
TuAr_test	Средний уровень	90	  
test2	Сложный уровень	90	  
SOC-5	Сложный уровень	90	  
SOC-2022-4-v2	Сложный уровень	90	  
SOC-2022-3	Сложный уровень	90	  
SOC-2022-2	Сложный уровень	90	  
SOC-2022-1	Сложный уровень	90	  
linux lpe user2	Сложный уровень	90	  

**Уязвимости**

- WordPress wpDiscuz
- Linux LPE
- Apache

**Последствия**

- WordPress Deface
- Apache meterpreter
- Pkexec AddUser

Автор  Shirkunov Evgeny 6 месяцев назад Обновлено  Ilyin Anton около 2 часов назад

## Разработка сценариев ...

В этой статье ничего нет. Нажмите здесь, чтобы добавить содержимое.

### Подстатьи<sup>20</sup>

[Уязвимые узлы \(таблица\)](#)

[Правила ведения таблицы](#)

[Реестр уязвимостей V2](#)

[Уязвимости, потенциально возможные для разработки](#)

[Гайд для разработчика сценариев](#)

[Процесс разработки уязвимого узла V2](#)

[Процесс создания уязвимого узла](#)

[Артефакты для интеграции уязвимого узла](#)

[Чеклист интеграции уязвимого узла](#)

[Полезные куски кода](#)

[Правила именования](#)

[Полезные материалы](#)

[Конфигуратор. Функционал сканирования](#)

[Сценарии Конфигуратора](#)

[Сторонняя разработка](#)

[Процесс ведения документации УУ](#)

[Версии ВМ УУ](#)

[GitLab](#)

[Разработка скриптов автоматизации](#)

[Kali](#)



00:00:00  
ЧЧ ММ СС



Группа **test**  
Шаблон **Предприятие (конфигуратор)**  
Сценарий **Защита ЦОД**  
Время начала **16:39**  
Время окончания **18:09**

**Уязвимости**

- УЯЗВИМОСТЬ 1**  
НЕ УСТРАНЕНО
- УЯЗВИМОСТЬ 2**  
СЕРВЕР НЕДОСТУПЕН
- WORDPRESS DUPLICATOR**  
УСТРАНЕНО  
ЗАКРЫЛ: Иван Защитник

**Последствия**

- ПОСЛЕДСТВИЕ 1**  
НЕ УСТРАНЕНО
- ПОСЛЕДСТВИЕ 2**  
НЕ УСТРАНЕНО
- WORDPRESS METERPRETER**  
УСТРАНЕНО

**Загрузка вредоносного ПО на почтовый сервер**

Автор **Василий Наблюдатель**  
Ответственный **Иван Защитник**

рассматривается



**Нестандартные запросы по сети к почтовому серверу**

Автор **Василий Наблюдатель**  
Ответственный **Иван Защитник**

закрыт



**Загрузка вредоносного ПО на AD**

Автор **Василий Наблюдатель**  
Ответственный **Иван Защитник**

рассматривается



**Эксплуатации уязвимости CVE-2020-1472 на контролере домена**

Автор **Василий Наблюдатель**  
Ответственный **Иван Защитник**

закрыт



**Эксплуатации уязвимости загрузки произвольных файлов на веб-сервере**

Автор **Василий Наблюдатель**  
Ответственный **Иван Защитник**

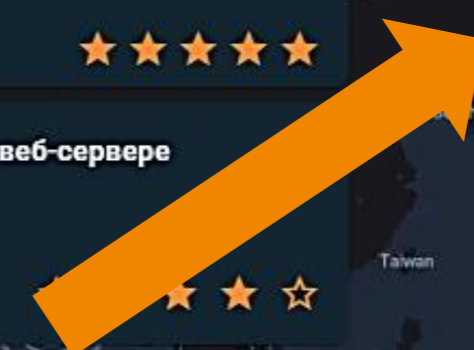
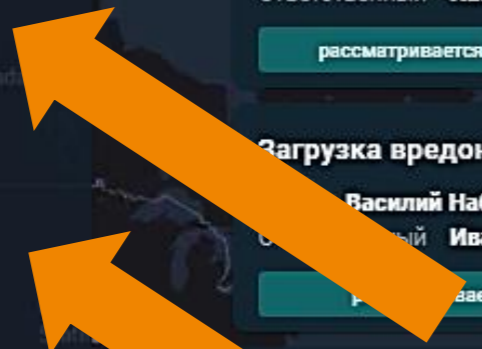
рассматривается



**Эксплуатации уязвимости Path Traversal на веб-сервере**

Автор **Василий Наблюдатель**  
Ответственный **Иван Защитник**

рассматривается





# Спасибо за внимание!

Бугай Иван

Руководитель направления по  
работе с ключевыми  
Заказчиками  
«Перспективный мониторинг»

[Ivan.Bugay@amonitoring.ru](mailto:Ivan.Bugay@amonitoring.ru)