360° Ampire

КОНФЕРЕНЦИЯ КИБЕРПОЛИГОНОВ

Вместе против цифровой уязвимости

24 апреля

г.Москва, Кибердом

Введение в киберучения: как тренировать опытных специалистов

Фефилов Александр,
руководитель направления УМП,
«Перспективный мониторинг»

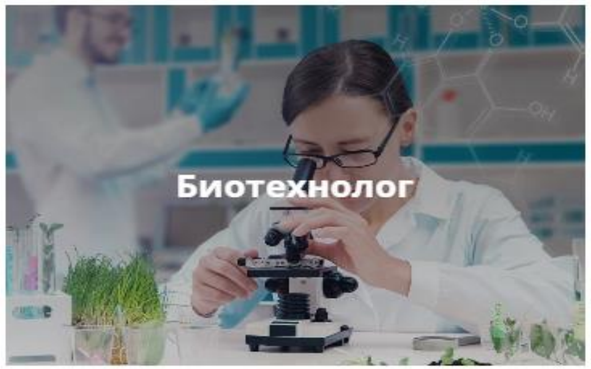
Ampire 360°

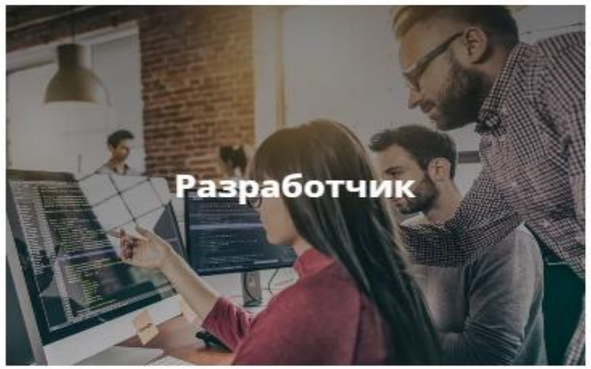
Киберучения

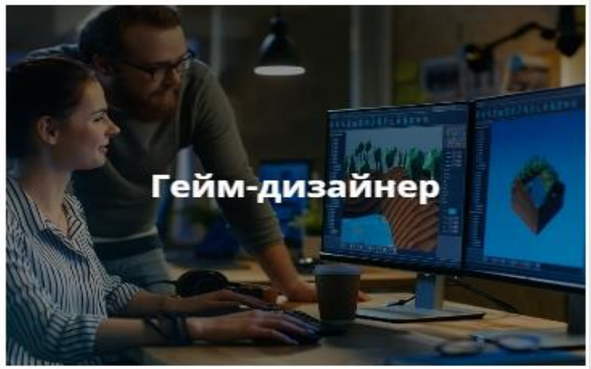
Для кого?

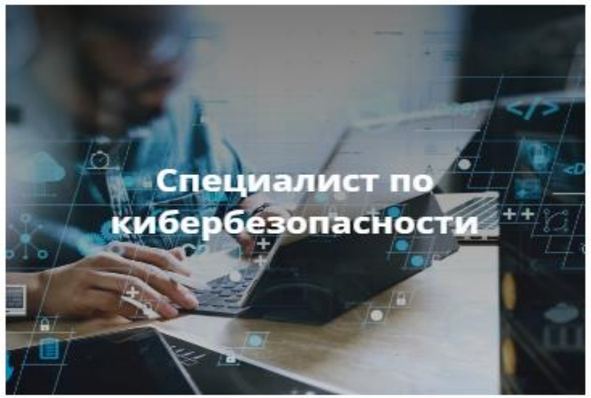
Ampire 360°

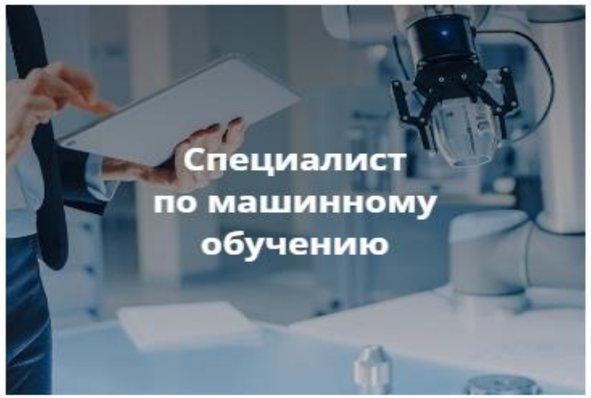
Профессии будущего

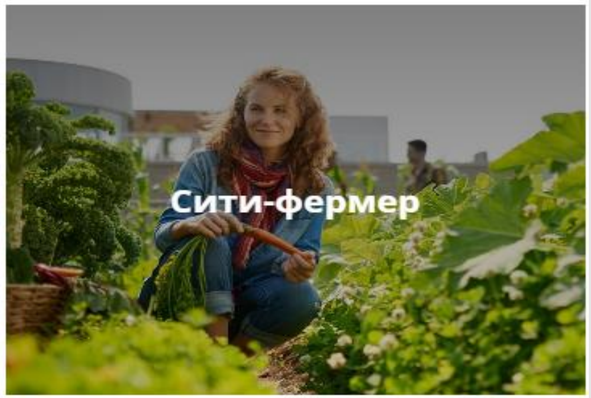












Я знаю
ПРОЕКТ KP.RU

КОМСОМОЛЬСКАЯ ПРАВДА

Специалист по кибербезопасности

Ampire 360°

- Операционная безопасность
- Сетевая безопасность
- Безопасность приложений
- Информационная безопасность

Ampire 360°

Специалист по ИБ

Государственный сектор

- Органы государственной и муниципальной власти
- Министерства
- Ведомственные учреждения
- Правоохранительная сфера

Объекты КИИ

- Крупная промышленность
- Транспортная сфера
- Финансовая сфера
- Здравоохранение
- Электроэнергетика
- ТЭК

Центр кибербезопасности AMPIRE

Бизнес и образование

- Учреждения среднего и высшего образования
- Школы
- Дополнительное образование для детей
- Средний бизнес

Повышение готовности ключевых предприятий региона к киберинцидентам и обмен экспертизой

Специалист по ИБ

Ampire 360°

Требования к квалификации по профессиям

Единый квалификационный справочник должностей руководителей, специалистов и служащих

Профессиональный стандарт

Порядок разработки и утверждения профессиональных стандартов определён Постановлением Правительства РФ от 22.01.2013 № 23

Киберучения

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОСТАНОВЛЕНИЕ

от 6 мая 2016 г. № 399

МОСКВА

Об организации повышения квалификации специалистов по защите информации и должностных лиц, ответственных за организацию защиты информации в органах государственной власти, органах местного самоуправления, организациях с государственным участием и организациях оборонно-промышленного комплекса

Правительство Российской Федерации **п о с т а н о в л я е т :**

1. Утвердить прилагаемые Правила организации повышения квалификации специалистов по защите информации и должностных лиц, ответственных за организацию защиты информации в органах государственной власти, органах местного самоуправления, организациях с государственным участием и организациях оборонно-промышленного комплекса.

2. Рекомендовать федеральным государственным органам, органам государственной власти субъектов Российской Федерации, органам местного самоуправления, организациям с государственным участием и организациям оборонно-промышленного комплекса определить лиц, ответственных за обеспечение защиты информации, в пределах установленной штатной численности и обеспечить регулярное повышение квалификации этих лиц.

Председатель Правительства
Российской Федерации Д.Медведев

МИНИСТЕРСТВО ТРУДА И СОЦИАЛЬНОЙ ЗАЩИТЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ
от 1 ноября 2016 г. N 601н

ОБ УТВЕРЖДЕНИИ ПОЛОЖЕНИЯ О РАЗРАБОТКЕ ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ НЕЗАВИСИМОЙ ОЦЕНКИ КВАЛИФИКАЦИИ

Приложение
к приказу Министерства труда
и социальной защиты
Российской Федерации
от 1 ноября 2016 г. N 601н

ПОЛОЖЕНИЕ
О РАЗРАБОТКЕ ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ НЕЗАВИСИМОЙ ОЦЕНКИ КВАЛИФИКАЦИИ

6. Оценочное средство содержит:

а) наименование оцениваемой квалификации, утвержденное автономной некоммерческой организацией "Национальное агентство развития квалификаций" (далее - Национальное агентство) и содержащееся в реестре;

б) уровень квалификации, определенный в соответствии с требованиями к квалификации;

в) наименование и код профессионального стандарта или наименование и реквизиты федеральных законов и иных нормативных правовых актов Российской Федерации, на соответствие положениям которых проводится профессиональный экзамен;

☆ г) знания, умения, трудовые действия, трудовые функции в соответствии с требованиями к квалификации;

д) описание материально-технического обеспечения для проведения профессионального экзамена;

е) требования к кадровому обеспечению для проведения профессионального экзамена;

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

от 11 ноября 2019 года N 705

О конкурсной комиссии Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации по проведению конкурсного отбора на предоставление Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации субсидий из федерального бюджета на создание киберполигона для обучения и тренировки специалистов и экспертов разного профиля, руководителей в области информационной безопасности и информационных технологий современным практикам обеспечения безопасности

В целях реализации подпунктов "б" и "в" пункта 5 Правил предоставления субсидий из федерального бюджета на создание киберполигона для обучения и тренировки специалистов и экспертов разного профиля, руководителей в области информационной безопасности и информационных технологий современным практикам обеспечения безопасности, утвержденных постановлением Правительства Российской Федерации от 12 октября 2019 г. N 1320 (Собрание законодательства Российской Федерации, 2019, N 42, ст.5913) (далее - Правила),

приказываю:

1. Создать конкурсную комиссию Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации по проведению конкурсного отбора на предоставление Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации субсидий из федерального бюджета на создание киберполигона для обучения и тренировки специалистов и экспертов разного профиля, руководителей в области информационной безопасности и информационных технологий современным практикам обеспечения безопасности (далее - Конкурсная комиссия).

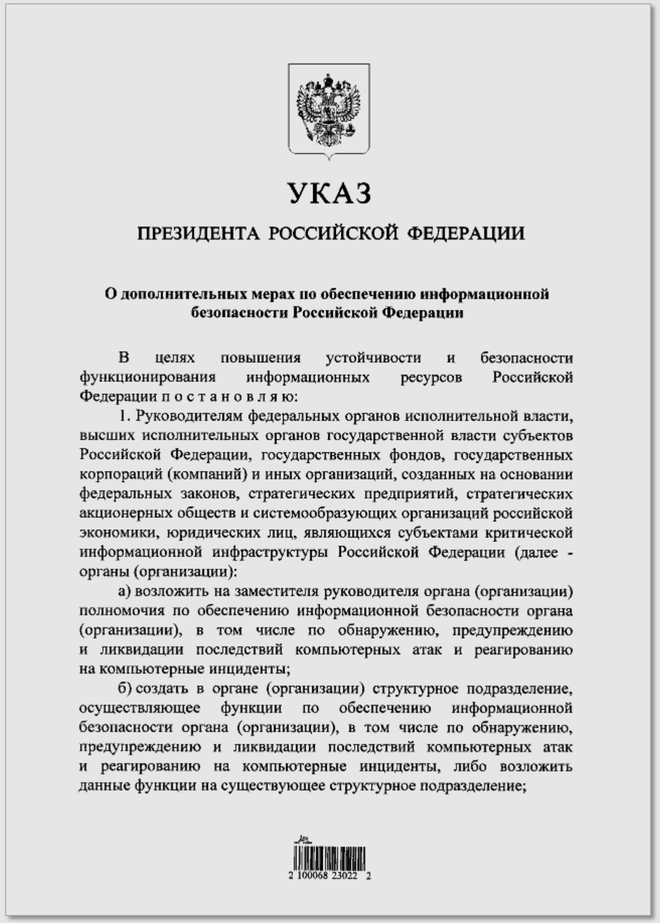
2. Утвердить:

положение о конкурсной комиссии Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации по проведению конкурсного отбора на предоставление Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации субсидий из федерального бюджета на создание киберполигона для обучения и тренировки специалистов и экспертов разного профиля, руководителей в области информационной безопасности и информационных технологий современным практикам обеспечения безопасности согласно приложению N 1 к настоящему приказу;

порядок рассмотрения конкурсной комиссией Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации по проведению конкурсного отбора на предоставление Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации субсидий из федерального бюджета на создание киберполигона для обучения и тренировки специалистов и экспертов разного профиля, руководителей в области информационной безопасности и информационных технологий современным практикам обеспечения безопасности поданных на конкурсный отбор заявок согласно приложению N 2 к настоящему приказу.

3. Контроль за исполнением настоящего приказа возложить на заместителя Министра цифрового развития, связи и массовых коммуникаций Российской Федерации А.В.Соколова, в том числе обеспечив в

Киберучения



УКАЗ

ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ

О дополнительных мерах по обеспечению информационной безопасности Российской Федерации

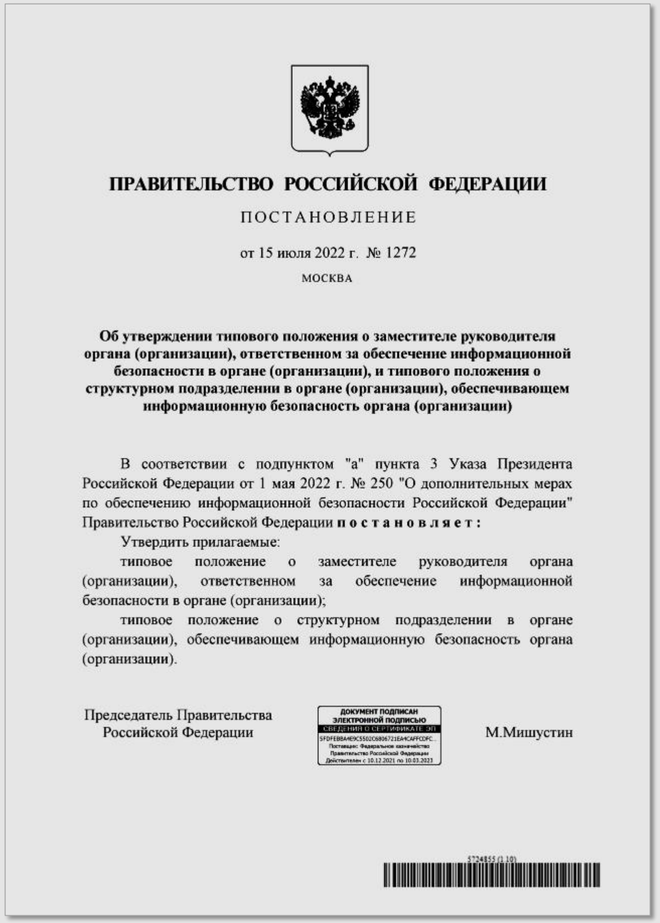
В целях повышения устойчивости и безопасности функционирования информационных ресурсов Российской Федерации п о с т а н о в л я ю:

1. Руководителям федеральных органов исполнительной власти, высших исполнительных органов государственной власти субъектов Российской Федерации, государственных фондов, государственных корпораций (компаний) и иных организаций, созданных на основании федеральных законов, стратегических предприятий, стратегических акционерных обществ и системообразующих организаций российской экономики, юридических лиц, являющихся субъектами критической информационной инфраструктуры Российской Федерации (далее - органы (организации):

а) возложить на заместителя руководителя органа (организации) полномочия по обеспечению информационной безопасности органа (организации), в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты;

б) создать в органе (организации) структурное подразделение, осуществляющее функции по обеспечению информационной безопасности органа (организации), в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты, либо возложить данные функции на существующее структурное подразделение;

2 100068 23022 2



ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОСТАНОВЛЕНИЕ

от 15 июля 2022 г. № 1272

МОСКВА

Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)

В соответствии с подпунктом "а" пункта 3 Указа Президента Российской Федерации от 1 мая 2022 г. № 250 "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации" Правительство Российской Федерации **п о с т а н о в л я е т :**

Утвердить прилагаемые:

типовое положение о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации);

типовое положение о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации).

Председатель Правительства Российской Федерации

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП
5F0FE88A4E9C5502C6B0672184AC4FCC0FC...
Поставщик: Федеральное казначейство
Правительство Российской Федерации
Действителен с 10.12.2021 по 10.03.2023

М.Мишустин

Ampire 360°

Киберучения

Почему они необходимы?

Дородный вырос, солидный,
Нелепый в чём-то… Не спорьте…
По-моему, очевидно:
Меня учить – только портить…

Анатолий Жуков

Киберучения

- субъект, имеющий значимые объекты КИИ, не реже одного раза в год организует и проводит тренировки по отработке мероприятий Плана реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак;

- организация и проведение тренировок **возлагаются** на подразделения и должностных лиц субъекта КИИ, ответственных за проведение мероприятий по реагированию на компьютерные инциденты и принятие мер по ликвидации последствий компьютерных атак.

п. 10 Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации (утв. приказом ФСБ России от 19.06.2019 № 282)

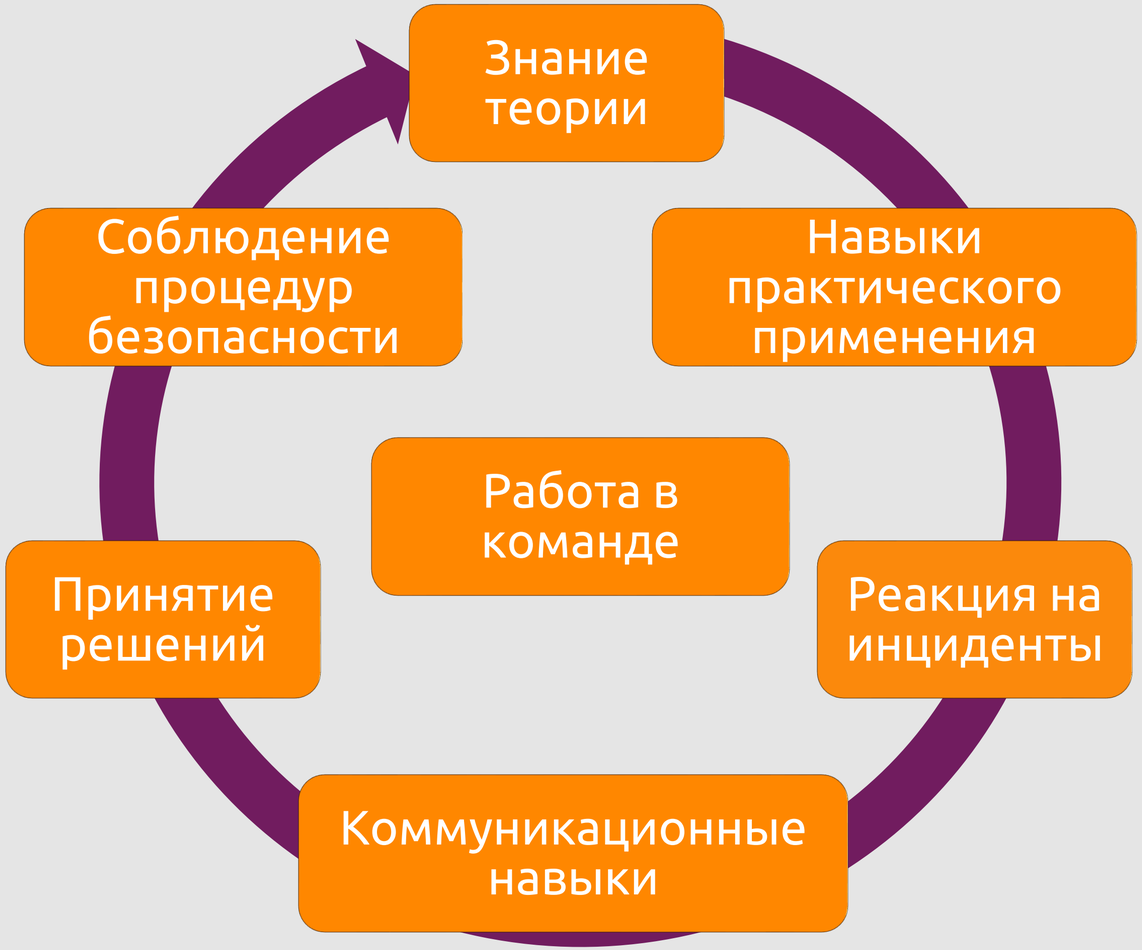
Киберучения

планирование и реализация обеспечивает выполнение требований:

- п. 25 Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования (утв. приказом ФСТЭК России от 21.12.2017 № 235);

- п. 13 Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации (утв. приказом ФСТЭК России от 25.12.2017 № 239), а также следующих видов мер по обеспечению безопасности значимого объекта: ДНС.2, ИПО.2, ИПО.3.

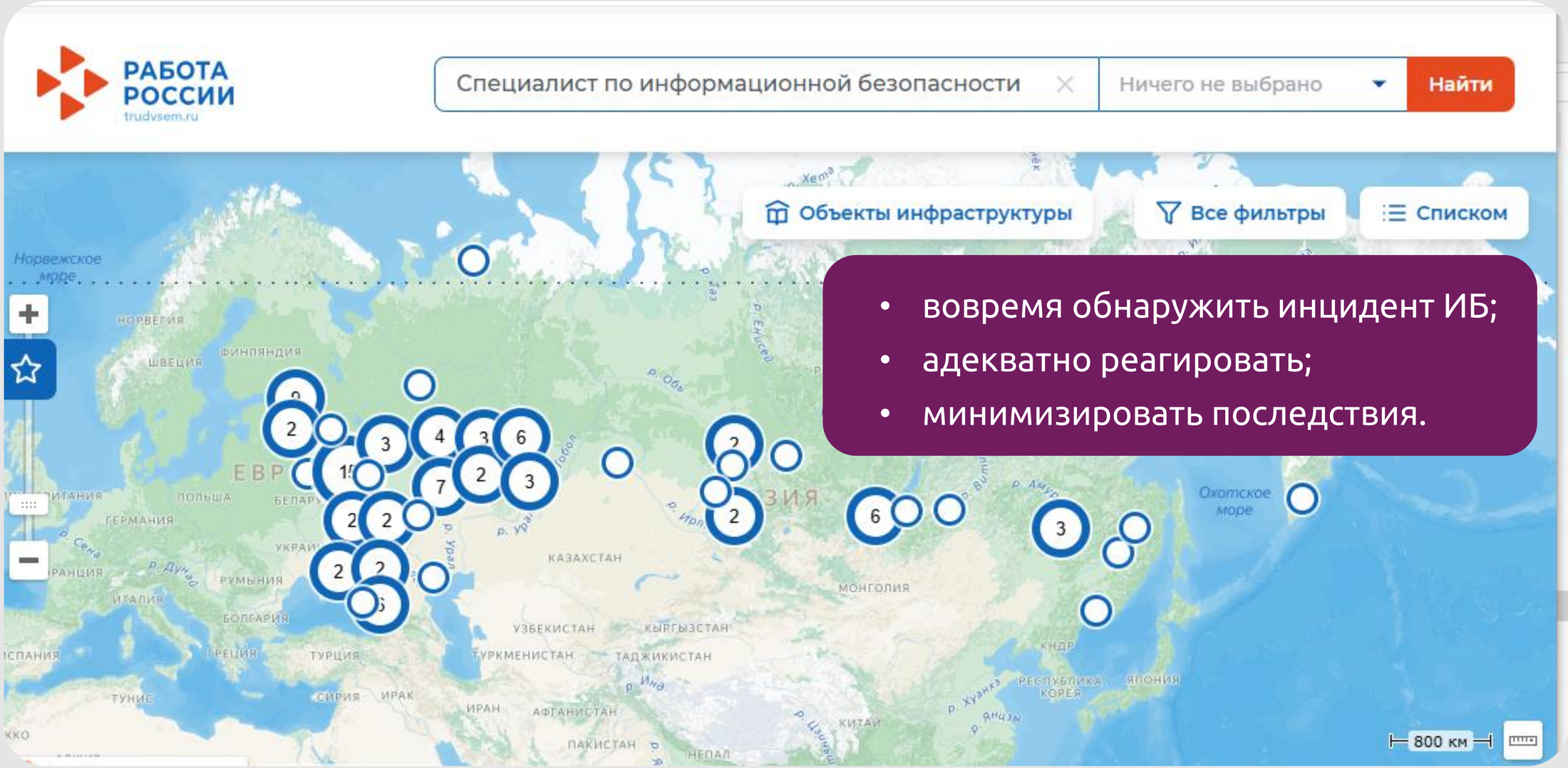
Оценка компетенций



Основные методики

Тестирование знаний	Симуляции атак	Ролевые игры	Анализ кейсов
проведение тестов или экзаменов	оценка реакции персонала на реальные или моделированные угрозы	отработка алгоритмов коллективного взаимодействия	проверка знаний на практических задачах

Ampire 360°



- вовремя обнаружить инцидент ИБ;
- адекватно реагировать;
- минимизировать последствия.

Ampire 360°

Киберучения

Какие они бывают?

Классификация

Ampire 360°

Виды учений

- Аналитические
- Экспериментальные

Публичность

- Закрытые
- Открытые

Целевая аудитория

- Руководители
- Администраторы
- Пользователи

Виды сценариев

- Ролевые
- Мультизадачные
- CTF

Характер проведения

- Организационные
  - Штабные учения
  - Штабные игры
  - Мастер-классы
- Технические
  - Управление и контроль
  - Отработка навыков
  - Полномосштабные
- Смешанные

Масштаб

- Внутренние
- Отрасливые
- Межотрасливые

Методические основы киберучений и CTF-соревнований
Александр Владимирович Дорофеев, НПО «Эшелон»
Алексей Сергеевич Марков, МГТУ им. Н. Э. Баумана

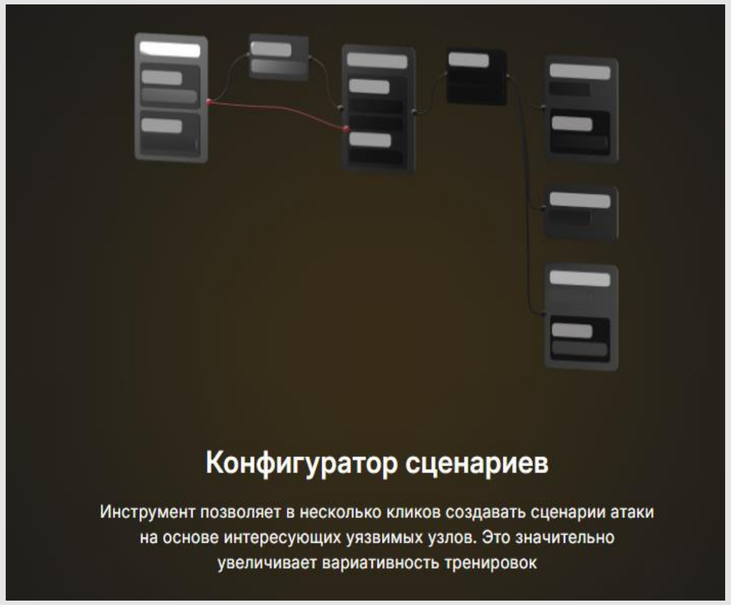
Формат

Формат для отработки атак - Red Team

Задача обучаемых - атаковать виртуальную инфраструктуру и найти флаг на одном из уязвимых узлов. Отлично подходит для начинающих пентестеров

Формат противодействия атакам - Blue Team

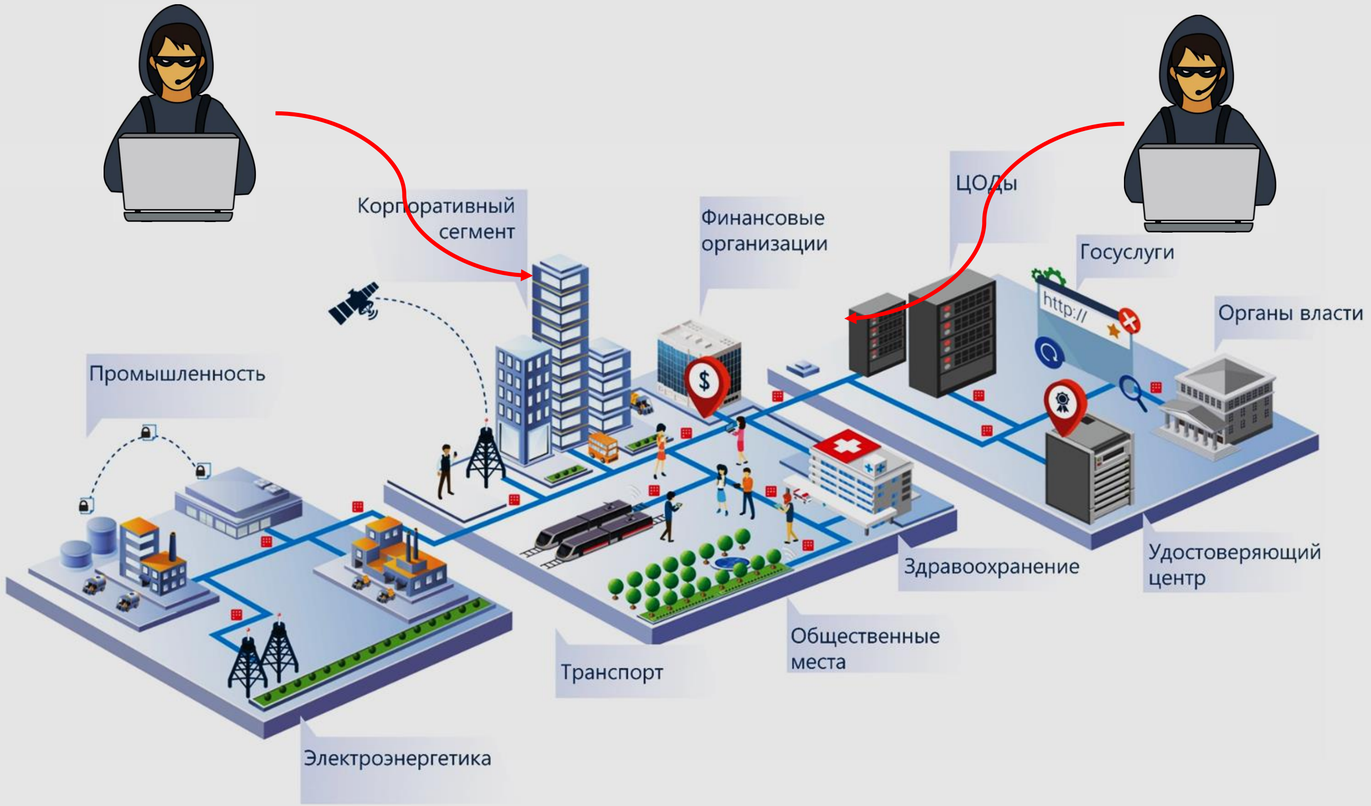
Задача обучаемых - закрыть уязвимости в инфраструктуре и устранить последствия атаки виртуального нарушителя. Формат моделирует работу центра мониторинга



Конфигуратор сценариев

Инструмент позволяет в несколько кликов создавать сценарии атаки на основе интересующих уязвимых узлов. Это значительно увеличивает вариативность тренировок

Шаблон


Корпоративный сегмент
Финансовые организации
ЦОДы
Госуслуги
Органы власти
Промышленность
Здравоохранение
Удостоверяющий центр
Общественные места
Транспорт
Электроэнергетика

Ampire 360°

Киберучения

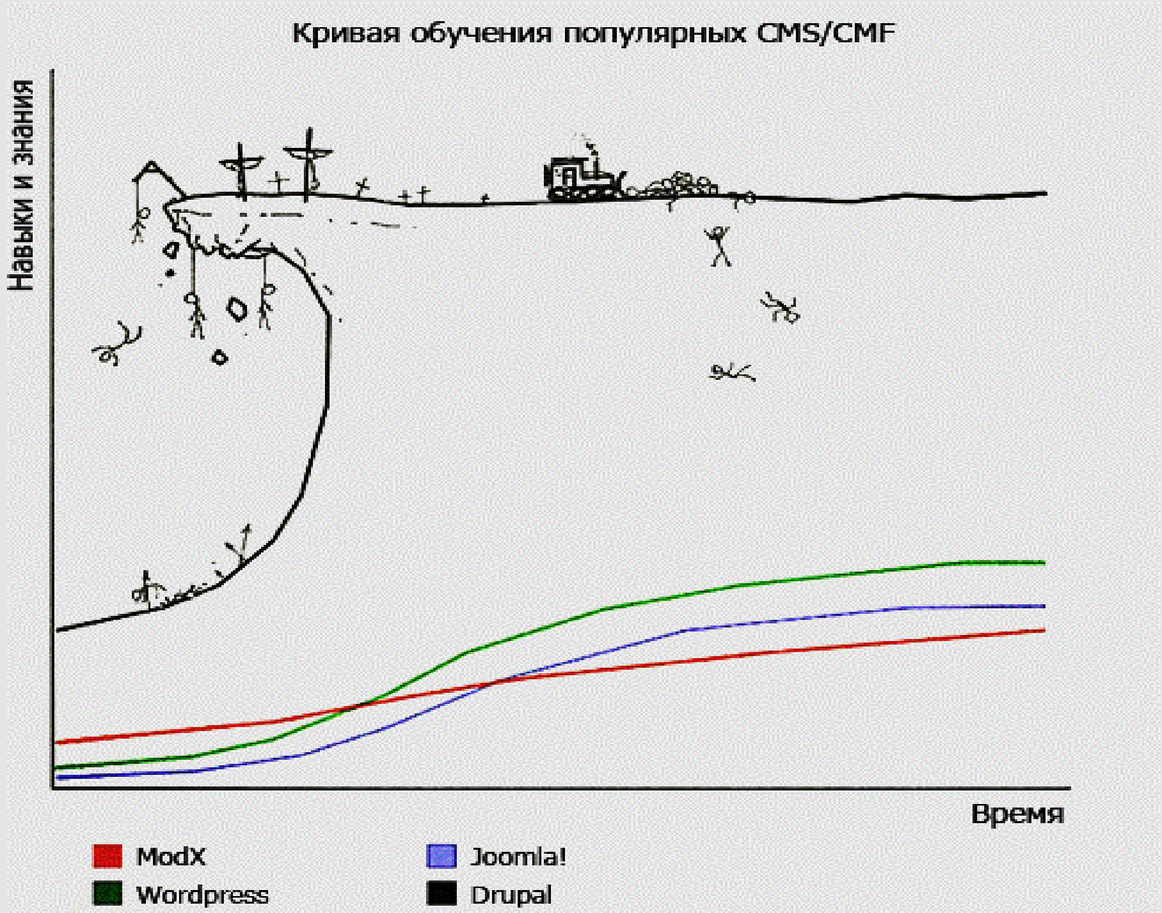
Как проводить?

Ampire 360°

Пеший по-машинному

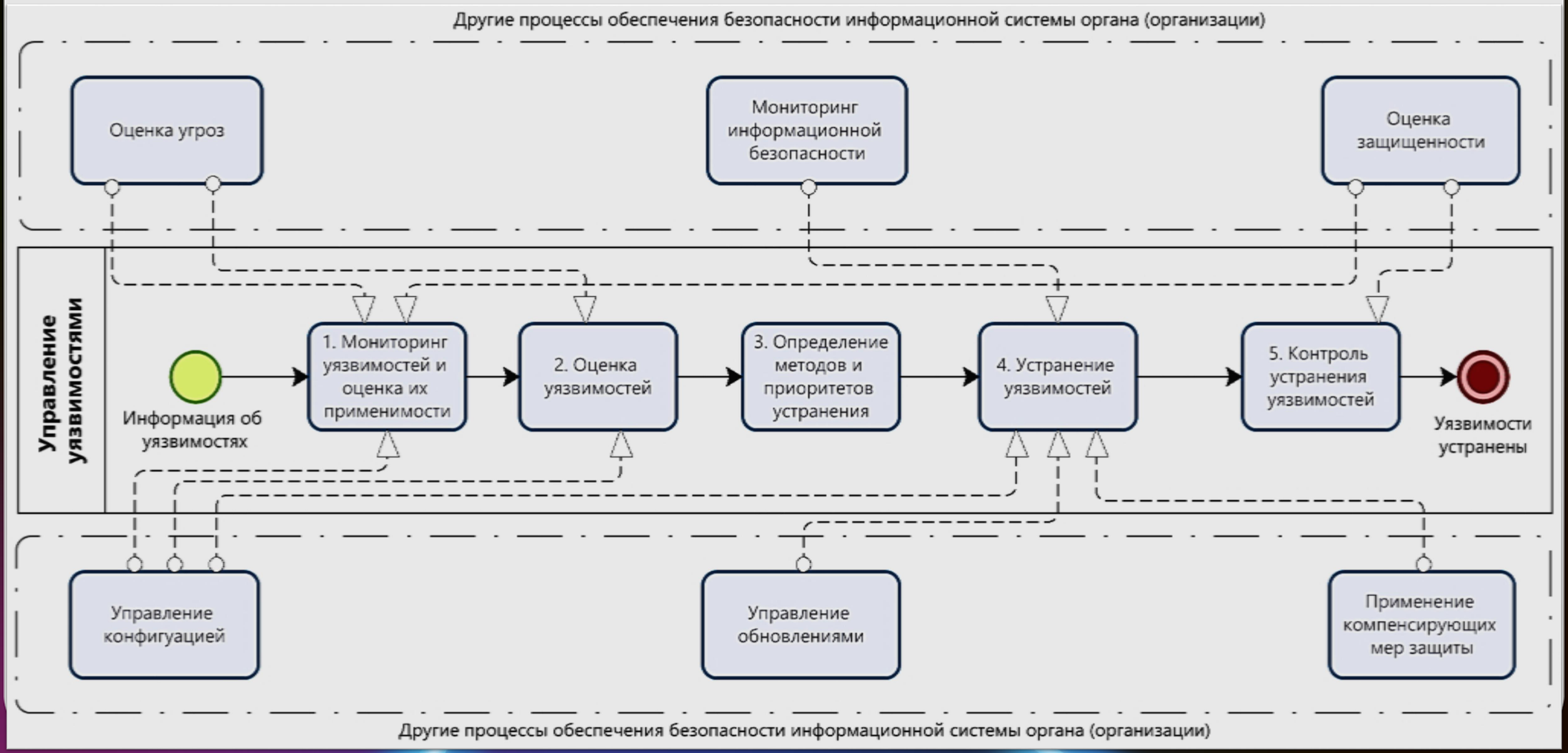
Ampire 360°

Порог входа



Кривая обучения

Из документа ФСТЭК России от 17 мая 2023 года «Руководство по организации процесса управления уязвимостями в органе (организации)»



Ampire 360°

Описание этапа	Формат занятия			Вид занятия				
	BlueTeam	CSIRT	Red Team	Киберквест	Киберучения	Соревнования		
						выявление КА	защита ИС	CTF
Рекомендуемое количество участников в 1-й тренировке	до 28 (19+9)	до 9	до 3	без ограничения	8-10 /3-5 /1-3	10-19	3-5	1-3
Создание учетных записей, ролевая модель	гр. монитор. гр. реагиров. + лидер	участники + лидер	участники + лидер	-	+	+	+	+
Создание тренировки в Ampire (формат)	+	+	+	BlueTeam CSIRT RedTeam	BlueTeam/ CSIRT/ RedTeam	BlueTeam	CSIRT	RedTeam
Вводный инструктаж	+	+	+	-	-	-	-	-
Контроль хода тренировки	+	+	+	-	+	+	+	+
Подведение итогов тренировки	+	+	+	-	+	+	+	+
Отчет о результатах	+	+	+	-	+	+	+	+
Показатели оценки	ср. оценка + успешность	успешность прохождения	выполнение заданий	-	успешность прохождения	% угроз, баллы	мин. время закрытия	мин. время поиска флага
Рекомендуемое время, мин	30 - 120	30 - 120	30 - 120	60 - 90	90	60	90	90

Занятия на киберполигоне

Ampire 360°

Начало: 18.11.2024 04:59

Завершение: 18.11.2024 07:31

Группа: ОИВ

Сценарий: 3.Защита данных файлового сервера

Успешность прохождения сценария

100%

Инцидентов создано	Средняя оценка инцидента	Цепочек кибератаки создано	Среднее время устранения уязвимости	Среднее время устранения последствия
7	4.00	0	1:51:31	2:06:41

Уязвимости и последствия

Web1 MySQL Password	Устранено на 104 мин.	**MS1710**	Устранено на 120 мин.
Уязвимость без последствий		FS backdoor	Устранено на 138 мин.
RDP Checker	Устранено на 110 мин.		
Manager meterpreter	Устранено на 114 мин.		

Начало: 19.11.2024 08:13

Завершение: 19.11.2024 09:11

Группа: ОИВ

Сценарий: 3.Защита данных файлового сервера

Успешность прохождения сценария

100%

Инцидентов создано	Средняя оценка инцидента	Цепочек кибератаки создано	Среднее время устранения уязвимости	Среднее время устранения последствия
11	3.55	0	48:14	49:31

Уязвимости и последствия

Web1 MySQL Password	Устранено на 44 мин.	**MS1710**	Устранено на 42 мин.
Уязвимость без последствий		FS backdoor	Устранено на 45 мин.
RDP Checker	Устранено на 57 мин.		
Manager meterpreter	Устранено на 53 мин.		

360° Ampire

Благодарю за внимание!