О ПРОБЛЕМАХ КИБЕРПОЛИГОНОВ



Михаил АКСЕНОВ
генеральный директор Defbox



Валерий ГОРБАЧЕВ
руководитель группы внедрения систем мониторинга АО «ДиалогНаука»

Киберполигоны остаются редким инструментом практической подготовки в области информационной безопасности. Создание и поддержка таких сред требует ресурсов, экспертизы и времени, поэтому далеко не каждая команда имеет возможность регулярно использовать инфраструктуру для отработки практических сценариев.

Наличие киберполигона не гарантирует, что команда получает от него устойчивую практическую пользу. Даже хорошо подготовленная техническая среда может использоваться эпизодически, а проведённые на ней учения не всегда становятся частью системной работы с компетенциями специалистов.

Поэтому вопрос о киберполигонах целесообразно рассматривать шире, чем вопрос о создании или приобретении тренировочной инфраструктуры. Для команды важна системность и выстраивание непрерывно работающего процесса, а не эпизодическая тренировка на полигоне. Руководителям же важно понимать, как практические упражнения связаны с развитием конкретных специалистов, как фиксируются результаты тренировок и каким образом этот опыт используется при планировании следующего этапа подготовки.

В этой статье мы рассмотрим основные проблемы киберполигонов и предложим способы их решения.

НЕПРЕРЫВНОСТЬ

Мы привыкли рассматривать киберполигоны как цифрового двойника некой инфраструктуры. В таком двойнике можно безопасно воспроизводить события и сценарии, связанные с информационной безопасностью. На нём можно моделировать инфраструктуру, действия нарушителей, работу средств защиты и процесс реагирования на инциденты. Такая среда позволяет специалистам получать практический опыт без риска для производственных систем.

Но задачи подготовки редко ограничиваются необходимостью провести определённое количество учений. Организации необходимо понимать, насколько сотрудники готовы выполнять конкретные функции, как развивается команда и какие направления требуют дополнительного внимания.

Для этого работа с тренировочной средой должна быть связана с последовательным и непрерывным процессом развития навыков. Эта часть обычно относится к обучающим платформам и покрыта традиционными полигонами поверхностно. Однако без выстроенного процесса обучения киберполигон будет оставаться тренировочным стендом, которым пользуются раз в год без ощутимой пользы.

Процесс обучения и обучающий контент даже важнее, чем масштаб или техничность тренировочного стенда. Такой процесс может начинаться с определения текущего уровня подготовки. У разных специалистов и подразделений могут быть различные задачи. Аналитикам центра мониторинга требуется уверенно работать с событиями и выявлять признаки атак. Специалистам по реагированию необходимо устанавливать причины и масштаб инцидентов. Системные администраторы могут участвовать в локализации угроз и восстановлении инфраструктуры. Руководителям важно понимать общую картину происходящего и принимать решения в условиях ограниченного времени.

Все эти направления требуют практики, и одинаковый сценарий не всегда одинаково полезен для каждого участника. Кроме того, необходимо собирать индивидуальные и сводные метрики, которые могли бы объективно показать успешность обучения.

В такой модели киберполигон становится частью непрерывного цикла и начинает приносить измеримую пользу. Тренировка даёт практический материал для оценки, а оценка влияет на содержание следующих тренировок (рис. 1).

МЕТРИКИ

Другая проблема полигонов — это прозрачность результатов. После проведённых учений вы знаете, удалось ли вам справиться с атакой, но вы не знаете ничего о вкладе разных членов команды в решение инцидента. Количество проведённых часов на полигоне или число успешно завершённых сценариев дают лишь общее представление об активности. Для развития команды важно понимать, какие действия специалист способен выполнять самостоятельно и насколько устойчиво он применяет полученный опыт.

Поэтому нельзя забывать об индивидуальной практике. Специалисты могут выполнять атомарные упражнения, актуальные для их должности. При таком подходе результат тренировки становится более конкретным.

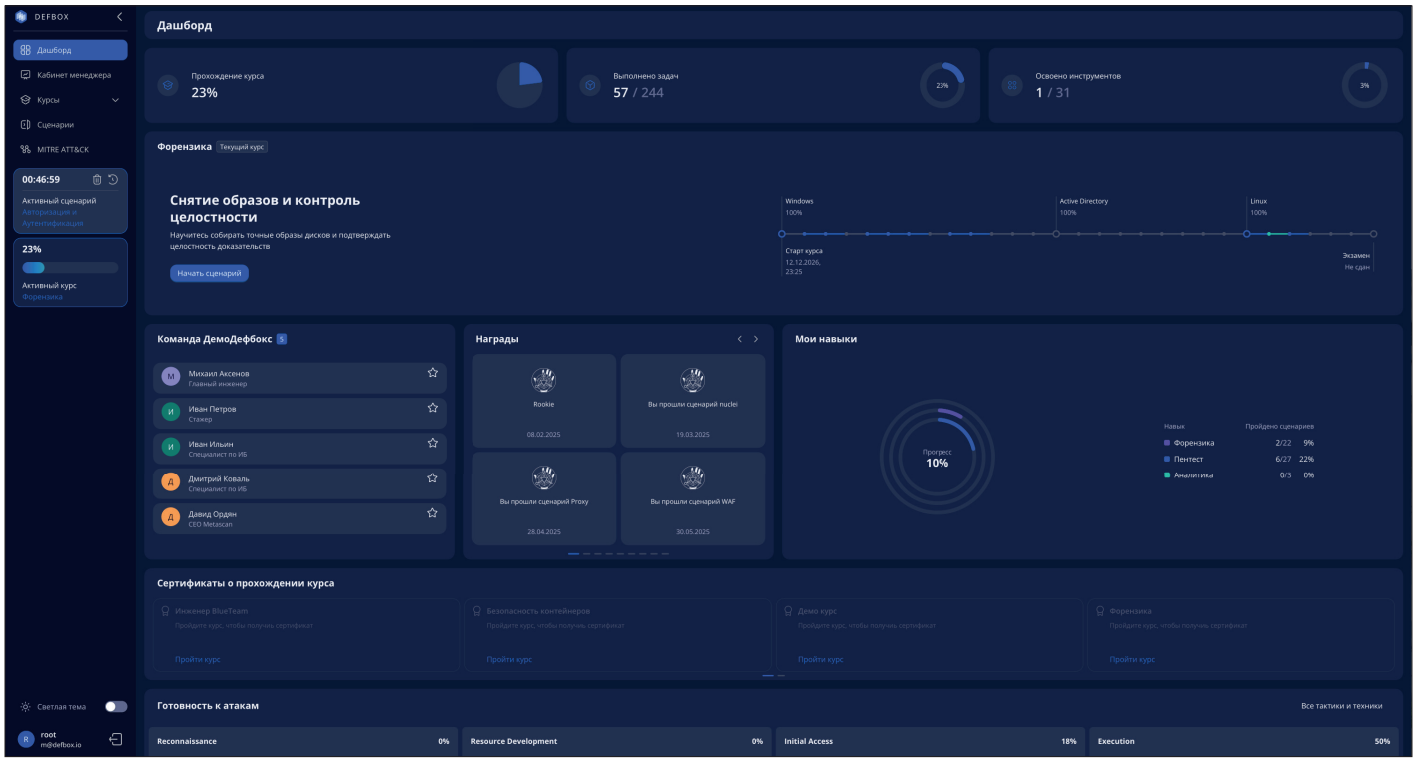


Рисунок 1. Дашборд прогресса обучения пользователя

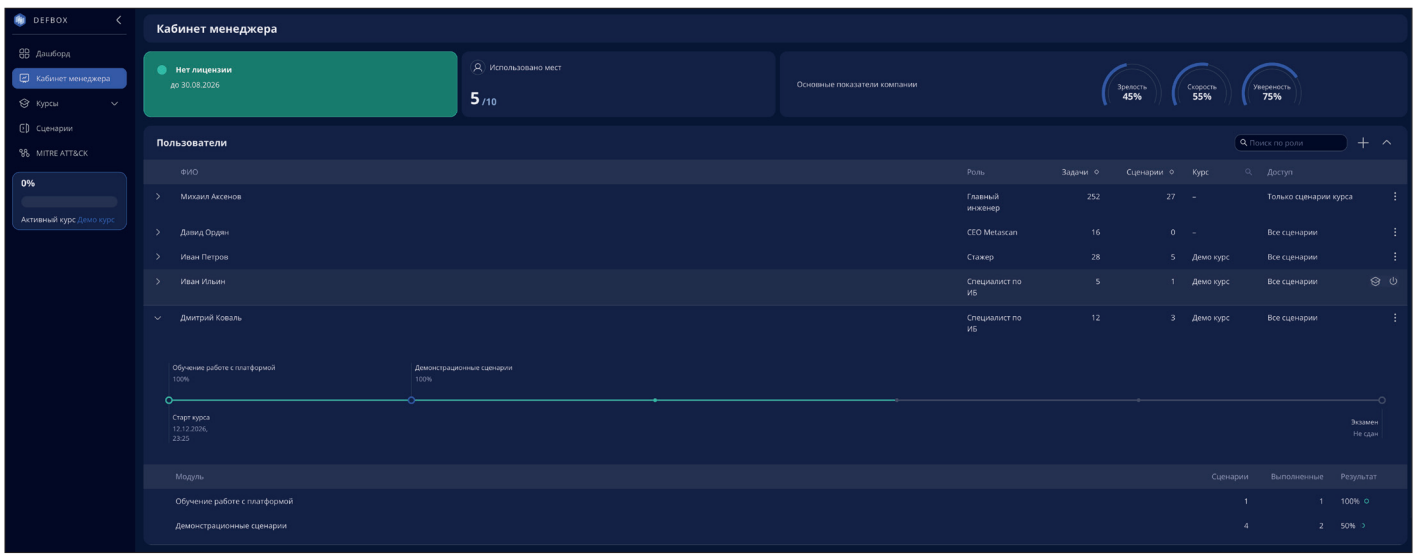


Рисунок 2. Пример экрана метрик с общей и индивидуальной статистикой

Можно увидеть, что специалист уверенно работает с определённым типом данных, но испытывает сложности при интерпретации результатов. Другой участник может быстро обнаруживать аномалии, однако нуждаться в дополнительной практике при расследовании причин их появления. Третий хорошо выполняет технические задачи, но пока недостаточно уверенно взаимодействует с другими участниками процесса.

Такая информация значительно полезнее общей оценки успешности учения.

Со временем она позволяет формировать профиль компетенций специалиста и отслеживать его развитие. При этом речь идёт не о едином рейтинге, который сводит подготовку человека к одному показателю. Гораздо важнее видеть структуру навыков: что уже освоено, что используется уверенно, а какие задачи требуют дальнейшей практики.

Для руководителя команды такая система создаёт возможность принимать решения на основе фактических результатов подготовки. Становится понятнее, какие направления стоит развивать у отдельных специалистов и какие навыки необходимо усиливать на уровне всей команды (рис. 2).

УПРАЖНЕНИЯ, А НЕ ПОЛИГОНЫ

При слове «киберполигон» часто возникает образ масштабной инфраструктуры с большим количеством виртуальных машин, сложной сетевой архитектурой и множеством взаимосвязанных сервисов. Такие среды действительно необходимы для определённых задач, прежде всего для комплексных учений, в которых участвуют различные подразделения и воспроизводятся сложные сценарии.

Однако значительная часть навыков может отрабатываться в гораздо более компактной среде.

Небольшой полигон, состоящий из двух или трёх машин, позволяет сосредоточиться на отдельном упражнении. В одной системе может воспроизводиться действие пользователя или нарушителя, во второй — работа целевого сервиса, в третьей — сбор и анализ событий. Даже такой минимальный набор даёт возможность моделировать многие типовые ситуации, связанные с обнаружением и расследованием инцидентов.

Главное преимущество небольших сред заключается в управляемости и предсказуемости.

Разработчику проще контролировать исходные условия сценария и ограничивать количество факторов, влияющих на результат. Если задача посвящена определённому навыку, участнику не требуется одновременно разбираться с десятками систем и большим количеством второстепенных событий.

Это делает упражнение более понятным как с точки зрения создания, так и с точки зрения проверки результатов.

Небольшой сценарий проще собрать, протестировать и изменить. Если в ходе пилотного запуска становится понятно, что упражнение содержит неоднозначные условия или даёт недостаточно данных для анализа, его можно оперативно скорректировать. Такой подход особенно важен для организаций, которые регулярно обновляют программу подготовки и хотят создавать упражнения под конкретные задачи.

Проверка результатов также становится более прозрачной.

Для каждого упражнения можно заранее определить ожидаемые действия участника. Например, необходимо обнаружить определённое событие, установить его источник, определить затронутую систему или сформировать корректное заключение. В дальнейшем можно фиксировать не только итоговый ответ, но и ход выполнения задачи: какие данные использовал специалист, сколько времени потребовалось для анализа и на каком этапе возникли сложности.

Компактные полигоны позволяют быстро создавать и проверять такие атомарные упражнения, а затем включать их в более сложные сценарии (рис. 3).

ЗАКЛЮЧЕНИЕ

Развитие киберполигонов постепенно отходит от концепции наращивания вычислительных мощностей, увеличения количества виртуальных машин и усложнения моделируемой инфраструктуры. Масштабные среды сохраняют значение для отдельных типов учений, однако сами по себе размер и техническая сложность полигона не определяют эффективность подготовки.

Всё большее значение приобретает связь тренировочной среды с образовательным контентом и задачами развития конкретных навыков. Упражнения должны не только воспроизводить реалистичные сценарии, но и последовательно встраиваться в программу подготовки: от освоения отдельных навыков к комплексным задачам и командному взаимодействию.

Следующим направлением развития становится формирование непрерывного процесса обучения, в котором практические упражнения регулярно сменяют друг друга, а результаты каждой тренировки используются при планировании следующей.

Такой подход позволяет отслеживать развитие специалистов, своевременно выявлять дефицит компетенций и адаптировать содержание подготовки к потребностям команды. Именно эта интеграция создаёт основу для перехода от отдельных тренировок к управляемому и непрерывному развитию практических навыков специалистов по информационной безопасности.

Таким образом, дальнейшее развитие киберполигонов связано не столько с экстенсивным наращиванием инфраструктуры, сколько с переходом к управляемой практике, встроенной в образовательный процесс. Ключевыми критериями эффективности становятся измеримый рост квалификаций, способность команды действовать в условиях неопределённости и готовность специалистов к постоянному обучению. Поэтому перспективные киберполигоны следует рассматривать как адаптивные экосистемы, где сценарии, обучающий контент, метрики и обратная связь образуют синергию постоянного совершенствования. Именно такой подход позволяет превратить полигон из технологической площадки в устойчивый инструмент развития кадрового потенциала в сфере информационной безопасности.

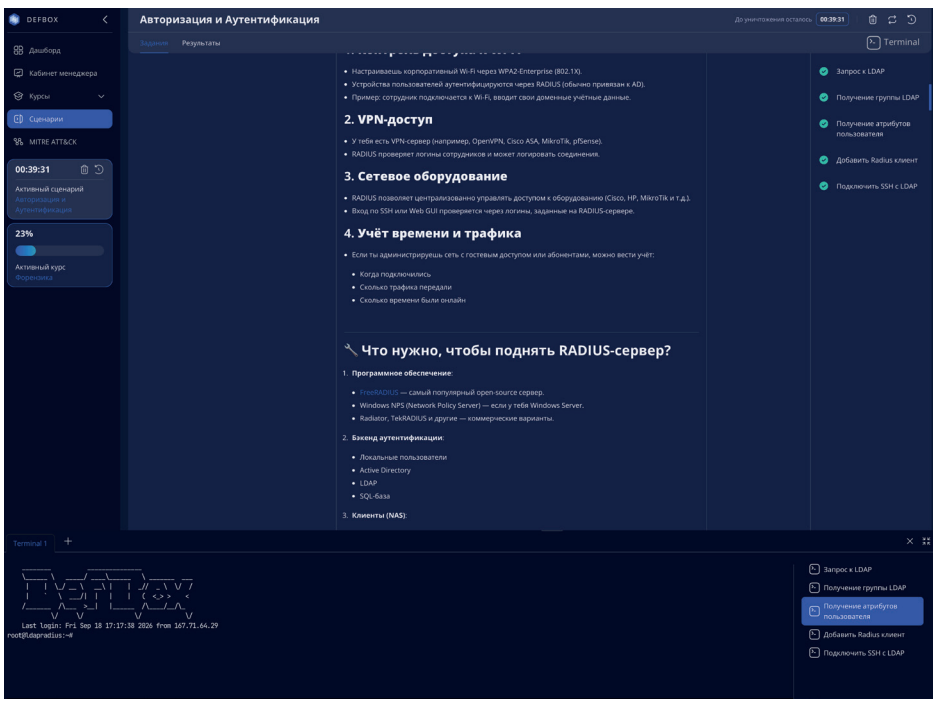


Рисунок 3. Обучение как набор атомарных блоков с понятной теорией