# Введение

Киберполигон – платформа для проведения тренировок по информационной безопасности разного формата. Он предоставляет эмуляцию бизнес-процессов и информационной инфраструктуры типовых организаций различных отраслей (кредитно-финансового сектора, промышленности, энергетики, транспорта, связи). Участникам киберучений предоставляются технологии и инструменты для получения и отработки практических навыков по защите от кибератак.

Чем крупнее и сложнее виртуальная инфраструктура, тем больше вариантов проведения тренировок (обучений, учений режима «авария», образовательных мероприятий) и тем ближе к реальности и полезнее опыт участия.

**Киберполигон решает задачи по обучению специалистов различного уровня:**

* Непрерывное развитие компетенций, оперативная переподготовка и повышение квалификации для уже работающих специалистов в ходе интенсивных учений в среде, максимально приближенной к реальной; выявление и направление в сферу информационной безопасности талантливых и заинтересованных школьников; техническая, организационная и методологическая помощь вузам для практического обучения студентов.
* Контроль готовности ключевых предприятий и организаций к отражению кибератак, отладка взаимодействия крупных участников рынка, проверка сложных гипотез через проведение киберучений, в том числе, национального уровня. При этом очевидна опасность отработки практических навыков на реальных объектах: проведение атак (даже не целенаправленно разрушающих) может затронуть жизненно важные процессы предприятия.
* Изучение импульсного влияния корректности работы одной отрасли на другую, распределение последствий атаки по цепочке вертикально и горизонтально интегрированных производственных систем. Как нарушение в работе одного из предприятий цепочки повлияет на стабильность остальных отраслей? Существует ли вероятность возникновения каскадов аварий при атаке на отдельные структурные элементы?
* Изучение и тестирование того, как совокупность систем будет работать в нештатной ситуации – критически важно для проверки и повышения уровня защищенности государства или компании.

**Актуальность:**

1. *Рост количества атак и изобретательности злоумышленников*

В условиях массовой цифровизации, обострения геополитической обстановки, санкций наблюдается рост количества кибератак. При этом злоумышленники становятся изобретательнее, ставят перед собой более амбициозные цели, совершенствуют тактики и техники своих действий.  
  
В целом количество регистрируемых событий безопасности растет. Согласно отчету «Кибератаки на российские компании в 2023 г.», подготовленному компанией «Солар», количество выявленных событий безопасности в четвертом квартале 2023 г. увеличилось на 68% по сравнению с аналогичным периодом предыдущего года.



В ИБ-компаниях Positive Technologies и «Лаборатория Касперского» подтвердили растущую активность хакеров в отношении ИТ-бизнеса в РФ. Так, согласно оценкам Positive Technologies, доля ИТ-компаний в общем числе атакованных почти утроилась, до 17%. В «Газинформсервисе» отмечают рост атак на ИТ-компании на 20–25%. Как отметили в центре мониторинга кибербезопасности «Лаборатория Касперского», в России и СНГ ИТ-рынок остается в тройке наиболее атакуемых хакерами отраслей.

Aтаки на ИТ-компании нацелены в первую очередь на парализацию сетевой инфраструктуры, что может привести к серьезным нарушениям в работе компаний, потере клиентской базы и полной остановке работы. Кибератаки также могут использоваться «для достижения геополитических целей и манипулирования общественным мнением».

Уязвимость российских компаний перед хакерами связана с нехваткой ИТ-специалистов на рынке для обеспечения полноценной защиты, импортозамещением значимых систем и переходом на продукты типа OpenSource.

Компания МТС RED 21 июля 2023 года сообщила о том, что количество кибератак в первом полугодии 2023 года выросло примерно в два раза по сравнению с аналогичным периодом 2022 года. В среднем по России число атак продолжает расти, а их уровень снижается. Однако в ряде отраслей аналитики МТС RED фиксируют обратную ситуацию.

Как и в 2022 году, наиболее атакуемыми отраслями в первом полугодии стали информационные технологии (35%), промышленность (21%) и ритейл (15%). По статистике центра мониторинга и реагирования на кибератаки МТС SOC, они ежемесячно испытывали на себе от 500 до 1000 вредоносных кибервоздействий различного уровня сложности.

Кроме того, ритейл и промышленные предприятия подвергались наибольшему числу высококритичных атак. Аналитики связывают это с высоким уровнем цифровизации в данной сфере и зависимостью ключевых бизнес-процессов от нормального функционирования ИТ-систем.

### 

*ИБ-центр ФСБ фиксирует более 170 кибератак на Россию каждый день.*

Чтобы эффективно справляться с растущим потоком хакерских атак, нужно постоянно тренировать навыки и делать это в разнообразных условиях и сценариях.

1. *Нехватка кадров*

В ИБ-отрасли наблюдается серьезный дефицит квалифицированных специалистов по информационной безопасности. По данным совместного опроса «СерчИнформ» и hh.ru за 2022 г., 54% российских компаний испытывают нехватку ИБ-кадров, а среди субъектов КИИ таковых 48%.   
  
В таких условиях возникает потребность относительно быстро доучить и переучить большое количество людей. И для этого недостаточно обычных занятий в университете. Нужны практические инструменты, которыми и являются киберполигоны. Например, в рамках проекта «Национальный киберполигон» создаются опорные центры на базе профильных вузов страны. Определенные учебные заведения получают полный доступ к инфраструктуре киберполигона и функционируют в качестве полноценных учебных площадок по отработке навыков защиты от киберугроз.

1. *Растущий спрос на информационную безопасность детей*

Государство проявляет повышенный интерес к вопросу детской безопасности, которая напрямую связана с информационным пространством. И сейчас этот интерес наиболее ярко выражается в Концепции информационной безопасности детей, утвержденной Председателем Правительства РФ Михаилом Мишустиным в 2023 г. Создается большое количество разнообразных инструментов, программ и курсов, повышающих осведомленность детей в базовых аспектах информационной безопасности.  
  
В «Перспективном мониторинге» создана отдельная версия киберполигона, предназначенного в первую очередь для школьников. На базе этого инструмента предлагаются практико-ориентированные лабораторные работы по актуальным проблемам информационной безопасности, с которыми дети сталкиваются в Интернете. В рамках занятий обучаемый может на собственном опыте и в безопасной среде прочувствовать, что такое фишинговые письма и что будет с компьютером, если эти письма открыть, как выявлять фейковые новости, как защититься от мошенничества и кибербуллинга и т. д. Это не только помогает в повседневной жизни, повышает интерес ребенка к предметной области, но и способствует усилению безопасности детей в информационном пространстве.

1. *Динамика рынка*

В связи с постоянным ростом и развитием IT на рынке ИБ формируется устойчивое понимание, что для качественного усиления безопасности недостаточно установить несколько «железок» в организации и настроить софт. Становится популярной мысль, что укрепление информационной безопасности сродни тренажерному залу. Если хочешь накачать мышцы, недостаточно провести пару интенсивных занятий по пять часов. Важно заниматься регулярно, методично, пусть даже занятие будет продолжаться 30 минут. Киберполигоны позволяют заложить регулярность, способствуют формированию культуры информационной безопасности.

# Состояние технологии

Киберполигон – это своего рода «виртуальная страна». Создаются типовые инфраструктуры отраслевых предприятий, которые связываются друг с другом. При этом используется отраслевое программное обеспечение и оборудование. С их помощью эмулируются процессы реальной информационной инфраструктуры типовых предприятий и групп предприятий, объединенных единой специфической информационной и технологической средой.

Виртуальная система, по сути, – большая сеть из множества сегментов, включающих каналы связи, сетевые устройства, сервера, рабочие компьютеры, технологическое оборудование и любые иные специфические устройства, подключенные к этой сети. Она постоянно активна на уровне ПО и элементов инфраструктуры. Эмуляторы рабочих компьютеров действуют так, будто за ними сидят реальные пользователи, при этом существует опция включить операторов, совершающих ошибки.

В зависимости от потребностей и задач тренировки мы можем использовать разный набор СЗИ, находящихся в разной степени завершенности, работоспособности и даже поврежденности. Также повреждена или неправильно сконфигурирована может быть любая часть информационной системы эмулируемого предприятия: программное обеспечение, оборудование, сеть.

Последняя (но не по значению) составляющая часть киберполигона – цепочки сценариев нештатных ситуаций. Киберполигон предлагает как типовые комбинированные цепочки атак, так и кастомизированные или модифицированные под нужды конкретного мероприятия. Для упрощения конфигурации мероприятия блоки атак унифицированы: можно создать свою собственную цепочку атак или модифицировать текущую (заменой одного из блоков).



*В отношении внутреннего устройства киберполигона специалисты обычно выделяют следующие типовые подсистемы/модули:*

* пользовательский интерфейс киберполигона – оболочку взаимодействия участников команд
* инфраструктура, на которой выполняется оркестровка сервисов, и которая, в зависимости от потребностей, имеет 3 основных типа представления:
* физическая эмуляция
* виртуализация/контейнеризация
* облачные технологии

*Прикладной уровень обеспечения работы киберполигона (модули):*

* симуляция интернет-сервисов
* управление компетенциями
* симуляция атак
* сбор данных и их анализ
* симуляция пользовательской активности
* оценка и отчетность
* разработка сценариев и контента
* инструментарий тренеров

В зависимости от задач и специфики, в состав инфраструктуры киберполигона обычно входит некое прикладное ПО/сервисы, обеспечивающие основные бизнес-процессы. Это также может быть не только ПО, но и специализированные аппаратные решения. Максимальная приближенность к реальной инфраструктуре обеспечивает качество киберполигона, но увеличивает его стоимость. Компании должны сохранять баланс в данном вопросе.

Отметим, что сценарии атак будут нужны не всегда – часть учений может проводиться с участием не только защитников, но и нападающих, и тогда не нужны никакие сценарии. Противостояние будет настоящим и непредсказуемым.

**Отметим ряд основных возможностей Киберполигона:**

* Моделирование современных, актуальных кибератак. Отработка регламентов расследования, реагирования и практических способов защиты;
* Обучение поиску как базовых, так и нетривиальных признаков атак;
* Развитие навыков самостоятельной подготовки к кибератаке: выстраивание процессов анализа и защиты, самостоятельное написание регламентов;
* Возможность проводить киберучения на отраслевых площадках;
* Снижение рисков за счет отработки регламентов по реагированию на внештатную ситуацию на внешней площадке;

Коммерческие компании сталкиваются с необходимостью постоянного улучшения практических навыков по выявлению и противодействию кибератакам – отработке штатных и нештатных ситуаций в обстановке, максимально приближенной к «боевой». Очевидно, что теория, чтение учебников, просмотр презентаций, общение с коллегами не дают специалисту, особенно начинающему, владения этими навыками. Приобретение необходимого опыта в ходе профессиональной деятельности – слишком долго и всегда ограничено условиями каждого отдельного места работы.

В крупных корпоративных департаментах по информационной безопасности присутствует потребность не только в обучении, но и в контроле динамики повышения квалификации сотрудников:

1. Стартовое обучение начинающих сотрудников информационной безопасности

2. Периодических поддерживающиеся тренировки

3. Масштабных учения всей команды ИБ.

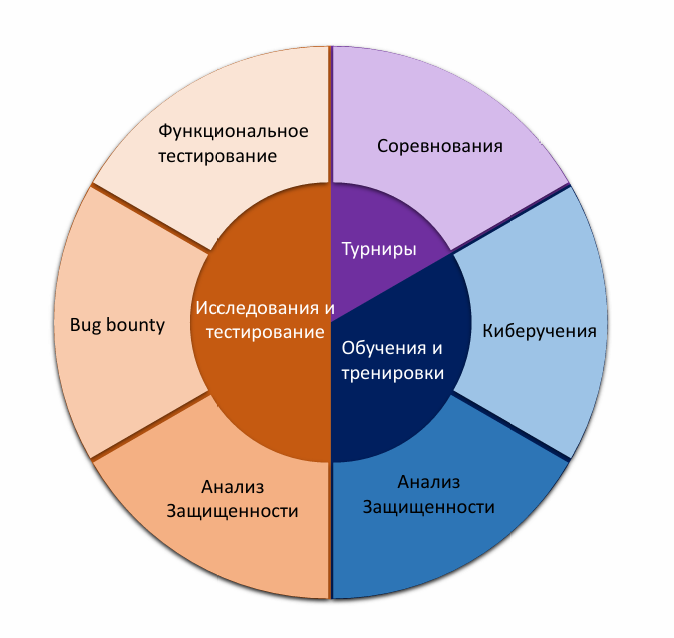
Создать технологическую среду и поддерживать её длительное время в актуальном состоянии – наукоёмкая и ресурсозатратная задача. При этом необходимо учитывать специфику угроз информационной безопасности в конкретной отрасли.

Важной задачей любой деятельности является поддержание необходимого уровня квалификации, которая достигается путем проведения обучения персонала и его тренировки. В части обеспечения информационной безопасности также остро встает вопрос тренировки – как её проводить, не нарушая базовые бизнес-процессы и не ослабляя текущий контроль информационной безопасности? Ответ – киберполигоны.

Например, на базе Standoff два раза в год проводится кибербитва с разными командами и моделями промышленной инфраструктуры. Платформа «Солар Кибермир» предлагает автоматическую систему скоринга для участников киберучений. А киберполигон Ampire оснащен инструментом «Конфигуратор сценариев», который позволяет на базе заложенных в продукт уязвимых узлов построить интересующий вектор атаки и отработать реагирование. В уязвимых узлах используются как широко известные, так и недавно появившиеся уязвимости.

**Таким образом, киберполигон позволяет:**

* проводить отработку атак (тестирование на проникновение) на «копию» ИТ-инфраструктуры предприятия, не создавая угроз основным бизнес-процессам;
* получать срезы навыков и знаний; определять, какие необходимо предпринять действия (в части сотрудников) для выстраивания наиболее эффективной защиты; составлять карты развития компетенций;
* осуществлять непосредственное обучение как сотрудников, отвечающих за ИТ и ИБ, так и представителей бизнес-подразделений;
* апробировать новые подходы и инструментарий ИБ;
* проводить оценку рисков, влияние реализации тех или иных угроз на бизнес-процессы компании.



# Перспективы

Чтобы определить вектор развития киберполигонов и понять, чем этот рынок «дышит», рассмотрим ключевые события, повлиявшие на его формирование и развитие. Некоторые тенденции носят долгосрочный характер и будут продолжать оказывать серьезное влияние.

*Стратегия национальной безопасности*

Указы о стратегии национальной безопасности принимались не один раз, в последнем из документов – Указе Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» – содержится раздел, посвященный достижению цели обеспечения информационной безопасности. В частности, п. 57 Указа предусмотрена задача развития системы прогнозирования, выявления и предупреждения угроз информационной безопасности, определения их источников, оперативной ликвидации последствий реализации таких угроз.

Киберполигоны – один из действенных способов решения такой задачи. Они являются тренировочным пространством, в рамках которого обучаемые учатся детектировать угрозы разного типа и устранять уязвимые места в информационной инфраструктуре.

Федеральным законом «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ введено понятие критической информационной инфраструктуры. За этим документом последовало еще несколько указов. С точки зрения устойчивого функционирования объектов КИИ интерес представляют Приказ от 21.12.2017 № 235 «Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования» и Приказ Федеральной службы безопасности Российской Федерации от 19.06.2019 № 282 «Об утверждении 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». Данными документами предусмотрены регулярные тренировки и обучение сотрудников в целях готовности к реагированию на инциденты безопасности и повышения квалификации в области ИБ.

Требования нормативных актов послужили дополнительным стимулом для предприятий, в частности, заставили задуматься о качественных инструментах, которые позволят системно проводить тренировочные мероприятия, сохранять прогресс, анализировать ошибки и совершенствовать навыки. Сегодня таким инструментом служат киберполигоны.

Классические киберучения проводятся в формате Blue Team, когда участники разделяются на группы мониторинга и реагирования. Первые выполняют функции обнаружения инцидентов информационной безопасности и предоставления сведений группе реагирования, участники которой закрывают уязвимости информационных систем и устраняют последствия кибератаки. Иногда команды мониторинга и реагирования объединяют в одну, тем самым обучаемым предоставляется вся полнота влияния на инфраструктуру.

Дополнительные функции и типы тренировок – системы автоматического скоринга, индивидуальные тренировки, соревновательные механики, тренировки в роли нарушителя – призваны разнообразить процесс, улучшить наблюдаемость, упростить работу по оценке достижений.

Создание национального киберполигона

В рамках Национальной программы «Цифровая экономика Российской Федерации» в 2019 г. были сформированы требования к созданию киберполигона. Формализация потребности в масштабах федеральных проектов отражает повышенный спрос не только на инструменты предотвращения и отражения угроз, но и на учебно-тренировочные платформы по подготовке ИБ-специалистов. Безусловно, спрос на практическую подготовку и, в частности, на повышение квалификации наблюдался и ранее: организовывались ДПО, курсы производителей и учебных центров, командно-штабные учения и занятия по повышению осведомленности. Все это послужило предпосылкой к созданию киберполигонов на уровне частных бизнесов и государства.

Объем мирового рынка Киберполигонов оценивался примерно в 1,2 млрд долларов США в 2023 году и, по прогнозам, достигнет около 3,5 млрд долларов США к 2032 году, увеличиваясь с совокупным годовым темпом роста (CAGR) 12,5% в течение прогнозируемого периода. Важным фактором роста, стимулирующим этот рынок, является растущая частота и сложность кибератак, что требует передовых решений для обучения специалистов по кибербезопасности.

Одним из основных факторов роста рынка Киберполигонов является ускоренная цифровая трансформация в различных секторах. По мере того, как организации продолжают оцифровывать свои операции и активы, потребность в надежных мерах кибербезопасности приобретает первостепенное значение. Киберполигоны обеспечивают смоделированную среду для обучения и повышения квалификации персонала по кибербезопасности, что имеет важное значение для борьбы с передовыми постоянными угрозами (APT) и другими сложными кибератаками. Возможность практиковаться и оттачивать навыки в контролируемой виртуальной среде снижает риск реальных уязвимостей.

Кроме того, растущие инвестиции в кибербезопасность со стороны правительств и частных предприятий способствуют росту рынка. Правительства по всему миру признают важность кибербезопасности для национальной обороны и защиты критически важной инфраструктуры. В результате они финансируют инициативы по разработке и развертыванию платформ киберполигонов для обучения военнослужащих и государственных служащих. Аналогичным образом, компании частного сектора, особенно в BFSI и ИТ-секторах, вкладывают значительные средства в обучение кибербезопасности для защиты конфиденциальной информации и поддержания доверия клиентов.

Появление передовых технологий, таких как искусственный интеллект (ИИ) и машинное обучение (ML), также способствует росту рынка Киберполигонов. Эти технологии расширяют возможности платформ киберполигонов, обеспечивая анализ в режиме реального времени и адаптивные сценарии обучения. Искусственный интеллект и машинное обучение могут моделировать широкий спектр киберугроз, что позволяет специалистам по кибербезопасности испытывать и реагировать на различные векторы атак. Такая технологическая интеграция имеет важное значение для того, чтобы идти в ногу с меняющимся ландшафтом угроз и обеспечивать комплексные решения по обучению.

С региональной точки зрения, ожидается, что Северная Америка будет доминировать на рынке Киберполигонов в течение прогнозируемого периода. Развитая технологическая инфраструктура региона в сочетании со значительными инвестициями в кибербезопасность делает его благодатной почвой для внедрения платформ киберполигонов. Присутствие крупных технологических компаний и фирм, занимающихся кибербезопасностью, еще больше ускоряет рост рынка. В Европе и Азиатско-Тихоокеанском регионе также ожидается значительный рост, обусловленный повышением осведомленности о кибербезопасности и увеличением инвестиций в инициативы по цифровой трансформации.

Прямых аналогов киберполигонов на данный момент не существует. Такие известные мировые площадки, как TryHackMe, Hack The Box, помогают получить новые знания и навыки, но они не позволяют в единицу времени взглянуть на ситуацию под всеми углами и ориентированы прежде всего на «атакующую» аудиторию. Самостоятельно развернуть похожий комплекс очень сложно и дорого. Поэтому наметившаяся тенденция рынка киберполигонов к росту сохранится в ближайшие годы и, скорее всего, значительно повлияет на процесс образования в сфере информационной безопасности.

Рынок платформ Киберполигонов предоставляет значительные возможности для роста и инноваций. Одна из ключевых возможностей заключается в растущей интеграции передовых технологий, таких как искусственный интеллект (ИИ) и машинное обучение (ML), в платформы киберполигонов. Эти технологии расширяют возможности платформ, обеспечивая анализ в режиме реального времени и адаптивные сценарии обучения. Искусственный интеллект и машинное обучение могут моделировать широкий спектр киберугроз, что позволяет специалистам по кибербезопасности испытывать и реагировать на различные векторы атак. Постоянное развитие этих технологий предоставляет поставщикам возможности для разработки более сложных и эффективных решений для обучения. Возможность предлагать индивидуальные и высокореалистичные учебные модули является значительной возможностью для роста на этом рынке.

Еще одной важной возможностью на рынке платформ Киберполигон является растущий спрос на обучение кибербезопасности в различных секторах. По мере того, как киберугрозы продолжают развиваться и становиться все более изощренными, организации в разных отраслях осознают важность инвестирования в обучение своих сотрудников кибербезопасности. Растущие нормативные требования и необходимость защиты конфиденциальных данных стимулируют спрос на надежные решения для обучения. Возможность предлагать отраслевые учебные модули и решать уникальные задачи, с которыми сталкиваются различные отрасли, является ключевой возможностью для вендоров на этом рынке. Растущее внимание к передовым практикам кибербезопасности и растущая доступность платформ кибердиапазона поддерживают рост рынка.

Несмотря на значительные возможности, рынок платформ Киберполигон также сталкивается с определенными угрозами и вызовами. Одной из основных проблем является высокая стоимость развертывания и обслуживания платформ киберполигонов. Локальное развертывание, в частности, требует значительных инвестиций в оборудование и ИТ-ресурсы, что может стать препятствием для небольших организаций с ограниченным бюджетом. Хотя облачные решения предлагают более экономичную альтернативу, опасения по поводу безопасности данных и соответствия требованиям могут помешать их внедрению. Потребность в постоянных обновлениях и обслуживании, чтобы идти в ногу с меняющимся ландшафтом угроз, является еще одной проблемой, с которой сталкиваются поставщики на этом рынке. Способность решать эти проблемы и предлагать экономически эффективные и безопасные решения для обучения имеет важное значение для роста рынка.

# Рыночная ниша

Киберполигоны многопрофильны – в них затрагиваются разные аспекты информационной безопасности (пентест, OSINT, мониторинг, реагирование и т. д.), разные форматы занятий (Blue Team, Red Team, CSIRT, Red Team vs Blue Team и т. д.), различные тактики и техники атак, уязвимости.

В настоящее время наблюдается повышенный спрос на киберполигоны среди высших учебных заведений, которые стараются изменить подход, перейти от «бумажной информационной безопасности» к практике. Так, например, в нескольких технических университетах, где поставлен киберполигон, студенты проходят регулярные практические занятия на его базе, используют данный инструмент в курсовых и дипломных проектах, сдают зачеты по пройденным сценариям. Все это позволяет студенту получить представление об информационной безопасности, максимально близкое к реальности, ознакомиться с типовыми инструментами, утилитами, средствами защиты информации и т. д. В то же время проходивший киберучения студент лучше готов к собеседованию в ИБ-компании, быстрее вливается в рабочий процесс. А с появлением киберполигона для детей к процессу подключаются еще и общеобразовательные школы. Эта тенденция сохранится и в дальнейшем.

Проявляют интерес к киберполигонам предприятия топливно-энергетического комплекса и финансовых организаций. Заказчики желают проводить киберучения на цифровых двойниках, чтобы сотрудники тренировались в привычном им контексте. Сама по себе разработка цифровых двойников – сложная задача из-за наличия специфического ПО и даже физического оборудования. По этой причине некоторые крупные компании предпочитают сосредоточиться на создании собственного киберполигона. Это несколько замедляет распространение киберполигонов в отраслях, в отличие от вузов. Однако спрос на киберполигоны сохранится и дальше, потому что существующие платформы активно развиваются, а создание собственного киберполигона – очень ресурсоемкая задача. (целевая аудитория и рыночная ниша)

Один из путей, по которому идут разработчики киберполигонов, – сотрудничество с отраслевыми научными институтами по созданию специализированных профильных шаблонов. Так, в 2023 г. совместными усилиями НТЦ МЭИ и «Перспективного мониторинга» был разработан и интегрирован в киберполигон цифровой двойник энергосистемы. В нем моделируются атаки, которые перехватывают управляющие сигналы к РЗА, в результате на подстанции возникает короткое замыкание. Особенность такой атаки в том, что в SCADA-системе, связанной с РЗА, оператор не видит негативных изменений в функционировании системы. Они станут для него очевидными, только когда случится само короткое замыкание. Есть и другие примеры интеграций с различными отраслями. Например, недавно на фестивале PHDays организаторы мероприятия предлагали участникам кибербитвы сценарий, в котором существовали два государства с предприятиями различных отраслей – нефтегазовой, металлургической, транспортной и не только. Атаки на эту инфраструктуру приводили к различным последствиям, таким как остановка перекачки нефти, транспортный коллапс и др. Все это визуализировалось на физических макетах государств.

Рынок киберполигонов находится в стадии роста. Сейчас охвачена лишь небольшая часть организаций, у которых есть прямой интерес к внедрению таких решений, и киберполигоны продолжат увеличивать свою долю на рынке.

Сегмент приложений включает оборонный сектор, финансовый сектор, ИТ и телекоммуникации, образование и др. Каждый сектор применения имеет уникальные требования и проблемы, которые стимулируют спрос на специализированные решения для киберполигонов.

В оборонном секторе платформы киберполигонов в первую очередь используются для обучения военнослужащих и обеспечения безопасности критически важной инфраструктуры. Растущая частота кибератак, нацеленных на системы обороны, требует передовых учебных решений для подготовки военного персонала к реальным сценариям. Возможность моделировать крупномасштабные кибервойны и проверять устойчивость оборонных сетей является ключевым фактором роста для этого сегмента.

Сектор финансов является еще одним крупным последователем платформ киберполигонов. Финансовые учреждения являются основными целями для кибератак из-за конфиденциального характера данных, с которыми они работают. Киберполигоны обеспечивают контролируемую среду для обучения специалистов по кибербезопасности в секторе, позволяя им обнаруживать и реагировать на различные типы киберугроз. Растущие нормативные требования и необходимость защиты данных клиентов являются важными факторами, способствующими внедрению платформ киберполигонов в этом секторе. Возможность проводить регулярное обучение и оценку помогает финансовым учреждениям соответствовать отраслевым стандартам и нормам.

В секторе ИТ и телекоммуникаций быстрые темпы технологического прогресса и растущая сложность киберугроз стимулируют спрос на платформы кибердиапазона. Эти платформы позволяют ИТ-специалистам опережать возникающие угрозы и разрабатывать эффективные стратегии их устранения. Возможность моделировать атаки на телекоммуникационную инфраструктуру и проверять отказоустойчивость сетей имеет решающее значение для поддержания непрерывности обслуживания и защиты данных клиентов. Растущее внедрение облачных вычислений и устройств IoT еще больше усиливает потребность в надежных решениях для обучения кибербезопасности в этом секторе. Возможность предлагать комплексные решения по обучению специалистов в области ИТ и телекоммуникаций является ключевым фактором роста для этого сегмента.

Сектор образования все больше осознает важность обучения кибербезопасности для студентов и преподавателей. Платформы киберполигонов интегрируются в учебные программы для обеспечения практического обучения в области кибербезопасности. Способность моделировать реальные сценарии и предоставлять практический опыт имеет важное значение для подготовки следующего поколения специалистов по кибербезопасности. Растущий акцент на образовании в области STEM и растущее число программ кибербезопасности в учебных заведениях стимулируют внедрение платформ киберполигонов в этом секторе. Возможность предлагать комплексные решения по обучению студентов и преподавателей является ключевым фактором роста для этого сегмента.

Рынок Киберполигонов сегментирован по размеру предприятия на малые и средние предприятия и крупные предприятия. Каждый сегмент имеет уникальные характеристики и требования, которые влияют на внедрение платформ киберполигонов.

Крупные предприятия с их значительными ресурсами и сложной ИТ-инфраструктурой являются основными пользователями платформ кибердиапазона. Этим организациям требуются передовые решения по обучению для борьбы со сложными киберугрозами, с которыми они сталкиваются. Возможность моделировать крупномасштабные атаки и обучать несколько команд одновременно имеет важное значение для крупных предприятий. Высокие ставки, связанные с защитой конфиденциальных данных и поддержанием непрерывности бизнеса, стимулируют спрос на надежные решения для обучения кибербезопасности в этом сегменте.

Крупные предприятия часто имеют специальные команды по кибербезопасности и значительные бюджеты на обучение и развитие. Платформы Киберполигонов предоставляют этим организациям инструменты для постоянного улучшения их состояния кибербезопасности. Возможность проводить регулярные тренинги и моделировать различные сценарии атак помогает крупным предприятиям опережать возникающие угрозы. Интеграция искусственного интеллекта и машинного обучения в платформы киберполигонов еще больше расширяет их возможности, обеспечивая анализ в режиме реального времени и адаптивные сценарии обучения. Растущая сложность киберугроз и растущие нормативные требования являются значительными факторами роста для внедрения платформ кибердиапазона на крупных предприятиях.

С другой стороны, малые и средние предприятия сталкиваются с различными проблемами и возможностями при внедрении платформ киберполигонов. Хотя малые и средние предприятия могут не обладать таким же уровнем ресурсов, как крупные предприятия, они в такой же степени уязвимы для кибератак. Растущее число киберугроз, нацеленных на малые и средние предприятия, делает обучение кибербезопасности необходимым. Однако высокая стоимость локального развертывания может стать препятствием для многих малых и средних предприятий. Облачные платформы киберполигонов представляют собой экономически эффективное решение, позволяющее малым и средним предприятиям получить доступ к передовым инструментам обучения без значительных первоначальных инвестиций. Возможность масштабирования платформы по мере необходимости и снижение нагрузки на внутренние ИТ-ресурсы делают облачные решения особенно привлекательными для малого и среднего бизнеса.

Растущее осознание важности кибербезопасности среди малых и средних предприятий стимулирует спрос на платформы для киберполигонов. Многие малые и средние предприятия признают, что инвестиции в обучение кибербезопасности имеют важное значение для защиты их бизнеса и поддержания доверия клиентов. Растущая доступность облачных решений и растущее внимание к передовым практикам кибербезопасности поддерживают внедрение платформ кибердиапазона в этом сегменте. Способность предлагать гибкие и масштабируемые решения по обучению, адаптированные к потребностям малого и среднего бизнеса, является ключевым фактором роста для этого сегмента.

В целом, анализ размера предприятия подчеркивает различные потребности и проблемы, с которыми сталкиваются крупные предприятия и малые и средние предприятия при внедрении платформ киберполигонов. В то время как крупным предприятиям требуются передовые и масштабируемые решения для борьбы со сложными киберугрозами, малым и средним предприятиям необходимы экономичные и гибкие инструменты обучения для защиты своего бизнеса. Растущий спрос на обучение кибербезопасности в обоих сегментах стимулирует рост рынка, при этом облачные решения играют решающую роль в удовлетворении потребностей малых и средних предприятий.

Конкурентная среда на рынке платформ Киберполигон характеризуется присутствием нескольких ключевых игроков, каждый из которых стремится укрепить свои рыночные позиции за счет инноваций, стратегического партнерства, а также слияний и поглощений. Рынок отличается высокой конкуренцией, при этом поставщики сосредоточены на разработке передовых решений для удовлетворения растущих потребностей организаций в различных секторах. Интеграция технологий искусственного интеллекта и машинного обучения в платформы киберполигонов является ключевым направлением для многих вендоров, поскольку это расширяет возможности их решений.

На российском рынке киберполигонов, предназначенных для проведения технических киберучений и повышения квалификации специалистов по информационной безопасности, выделяются несколько ключевых игроков:

* **BI.ZONE Cyber Polygon**: платформа, разработанная компанией BI.ZONE, предназначена для моделирования и отработки сценариев кибератак в различных отраслях.
* **Jet CyberCamp**: решение от компании «Инфосистемы Джет», предоставляющее возможности для проведения киберучений и тренингов по информационной безопасности.
* **The Standoff**: платформа, созданная компанией Positive Technologies, используется для проведения киберучений и соревнований между командами специалистов по кибербезопасности.
* **Национальный киберполигон**: инициатива, реализуемая «Ростелекомом» в рамках национальной программы «Цифровая экономика Российской Федерации». На базе этого полигона создаются опорные центры в ведущих вузах страны для подготовки специалистов и проведения киберучений.
* **Ampire**: платформа, разработанная компанией «Перспективный мониторинг», предназначена для обучения и тренировки специалистов в области кибербезопасности.

Эти платформы активно используются для проведения киберучений, тестирования систем защиты и подготовки специалистов в области информационной безопасности в России.

# Производители

Для анализа производителей выбраны:

* Национальный киберполигон
* Киберполигон Standoff 365 от Positive Technologies
* Киберполигон Ampire от АО «Перспективный мониторинг»

Для повышения кибербезопасности в России работает **Национальный киберполигон**. Это один из крупнейших проектов по информационной безопасности, реализуемых по национальному проекту «Цифровая экономика» (с 2023 года проект развивается самостоятельно, с апреля 2024 года проект создания «Национального киберполигона» исключён из национальной программы). Он выполняется силами «Ростелекома» с привлечением экспертизы сотрудников его дочерней компании «РТК-Солар», национального провайдера технологий и сервисов кибербезопасности.

Ключевая цель проекта — усиление киберустойчивости нашей страны за счет повышения готовности предприятий важнейших отраслей к выявлению и отражению кибератак, а также восстановлению их последствий в максимально короткие сроки

*Что такое Национальный киберполигон и его опорные центры*

Национальный киберполигон представляет собой цифровые копии инфраструктур предприятий со специфическим оборудованием, характерным для конкретной отрасли. По данным департамента обеспечения кибербезопасности Минцифры России, на сегодняшний день в рамках проекта доступны корпоративный, электроэнергетический, нефтегазовый и банковский, телекоммуникационный сегменты. Обучение и тренировки реализуются через сеть опорных центров, создаваемых на базе профильных вузов страны. Определенные учебные заведения имеют полный доступ к инфраструктуре киберполигона и функционируют как полноценные учебные площадки по отработке навыков защиты от киберугроз.

Основная задача Национального киберполигона — подготовка высококвалифицированных кадров в сфере безопасности. Появление таких площадок на базе университетов дает регионам возможность обеспечивать практико-ориентированную подготовку студентов и формировать кадровый резерв отрасли. Последнее очень важно для решения проблемы дефицита специалистов по кибербезопасности, который сегодня оценивается в 20–50 тыс. человек ежегодно и постоянно увеличивается.

На сегодняшний день действуют восемь точек присутствия Национального киберполигона в российских вузах:

• Дальневосточный федеральный университет (ДВФУ);

• Научно-технологический университет «Сириус»;

• Сибирский государственный университет телекоммуникаций и информатики (СибГУТИ);

• Национальный исследовательский университет ИТМО;

• Поволжский государственный университет телекоммуникаций и информатики (ПГУТИ);

• Московский технический университет связи и информатики (МТУСИ);

• Оренбургский государственный университет (ОГУ);

• Образовательный центр в Санкт-Петербургском университете телекоммуникаций им. проф. М.А. Бонч-Бруевича (СПбГУТ).

Учащиеся тренируются на эмулированной инфраструктуре предприятий с оборудованием, актуальным для конкретной отрасли, учатся выявлять и отражать цепочки атак, сценарии которых повторяют действия настоящих злоумышленников, Киберучения проходят в условиях, максимально близких к реальным, что позволяет будущим выпускникам получить практический опыт защиты от киберугроз уже во время учебы.

Помимо подготовки новых кадров в сфере информационной безопасности у Национального киберполигона есть и вторая функция. В опорных центрах проходят мастер-классы с целью повышения квалификации действующих специалистов по кибербезопасности, а также межотраслевые киберучения. Подобные мероприятия помогают сотрудникам служб кибербезопасности отрабатывать на практике сценарии выявления киберугроз без риска реального ущерба для предприятий. В разное время в киберучениях принимали участие Минэнерго, Центробанк, ТМК, Группа «Синара». Всего на Национальном киберполигоне было проведено более 200 киберучений.

****

*Как проходят киберучения*

На платформе Национального киберполигона могут проводиться мероприятия как в формате тренировочных киберучений, так и различных этапов всероссийских соревнований. В частности, на базе Национального киберполигона регулярно проходят студенческие олимпиады по кибербезопасности. Помимо этого, есть образовательные интенсивы, организуемые совместно с «Финтех Хабом» Банка России, финалы Национальной технологической олимпиады по профилю «Информационная безопасность», «Летняя школа по кибербезопасности» в партнерстве с Университетом «Сириус».

В киберучениях есть две стороны: атакующая и защищающаяся. В роли защитников выступают студенты. Атакующая сторона — это автоматизированные скрипты, которые по заранее разработанному сценарию реализуют вектор атаки. Например, для образовательного интенсива «Летней школы по кибербезопасности» эксперты «РТК-Солар» на платформе Национального киберполигона развернули лабораторную структуру с цифровыми копиями предприятий различных отраслей. Во время киберучений студенты защищали выделенный им объект от кибератак.

Поучаствовать в соревнованиях по кибербезопасности могут и школьники.

*Международные киберучения на Национальном киберполигоне*

В июне в рамках Петербургского международного экономического форума (ПМЭФ-2022), на базе Национального киберполигона в России прошли первые международные киберучения. В них приняли участие представители шести стран: России, Белоруссии, Казахстана, Азербайджана, Пакистана и Вьетнама. Специалисты Национального киберполигона развернули цифровой двойник инфраструктуры энергетического объекта и разработали автоматизированные сценарии атак, которые повторяли действия реальных злоумышленников, направленные на различные российские организации. Целью учений была координация усилий по борьбе с хакерами на мировом уровне и практическая отработка информационного обмена между странами-участницами об осуществляемых атаках.

*Планы на будущее*

Каждый из нас или является, или может стать объектом кибератаки — это вопрос времени, поэтому кибербезопасность — предмет для постоянной рефлексии, тренировок, стресс-тестов и так далее. В планах правительства развивать сеть опорных пунктов Национального киберполигона и довести число таких площадок до 15. Власти рассчитывают, что создание специальных площадок в российских вузах позволит подготовить специалистов по кибербезопасности и повысить квалификацию уже действующих сотрудников для ликвидации различных цифровых атак.

Планирует расширяться и функционал Национального киберполигона. В долгосрочной перспективе также планируется расширить инфраструктуру киберполигона сегментами, которые покроют в том числе транспортную, металлургическую и горнодобывающую отрасли. В департаменте обеспечения кибербезопасности Минцифры России добавили, что также обсуждается возможность моделирования на инфраструктуре киберполигона типовых объектов информационных ресурсов госорганов и критической информационной инфраструктуры объектов жизнеобеспечения.

**Standoff 365** — это платформа Positive Technologies, предназначенная для организации киберучений, моделирования атак и защиты, а также проведения программ bug bounty. Она представляет собой уникальный киберполигон, который объединяет в себе современные технологии, реальную инфраструктуру и сценарии атак, что позволяет компаниям и специалистам отрабатывать защиту от киберугроз.

На Standoff 365 есть два формата: офлайн и онлайн. Первый — это та самая кибербитва, красивое мероприятие с интенсивной работой по 12 часов в сутки, столкновение с десятками атак и сотнями инцидентов. Офлайн-формат — это отличная возможность для обучения и быстрой прокачки навыков, но на него нужно выделить время, собрать и подготовить команду. Часто после такого интенсива клиенты просят оставить им доступ к полигону для продолжения расследований инцидентов, вызванных атакующими, и отладки процессов в реальном, более спокойном режиме. В связи с этим сделали онлайн-полигон Standoff 365 доступным как для атакующих, так и для защитников, а также воспроизвели инфраструктуры разных отраслей, которые можно исследовать.

Онлайн-киберполигон Standoff 365 позволяет решать большое число задач безопасности с помощью почти 16 000 уже зарегистрированных на нем белых хакеров, а также за счет возможности быстрого подключения инфраструктуры, подписки и кастомизации. Исследователи безопасности работают на платформе с воспроизведенными системами компаний, за каждой из которых стоит команда защиты. Важно, что эти инфраструктуры могут быть типовыми, а могут включать в себя реальные бизнес-процессы, сервисы, софт, оборудование, которые использует сам заказчик. Кроме того, есть возможность воспроизводить те риски, которые опасны именно для вашей компании. Соответственно, атаки белых хакеров не только помогут обучить специалистов по ИБ, но и устроят проверку боем для реальных фрагментов вашей инфраструктуры. По запросу на киберполигоне может быть создан новый отраслевой сегмент — это, кстати говоря, способствует повышению интереса хакеров, а значит, работа «синих» на полигоне станет еще интереснее и полезнее.

Онлайн-киберполигон специально проектировали так, чтобы можно было легко подключить фрагмент инфраструктуры любой компании, ее сервисы и информационные системы. Такие фрагменты могут быть анонимизированы, чтобы не давать подсказки нападающим. Белым хакерам всегда интересно исследовать новую инфраструктуру, а компании смогут оценить уровень своей уязвимости. Например, крупный ретейлер предложил проверить на кибербитве свою программу лояльности, чтобы убедиться в ее надежности перед внедрением. В первый раз хакеры нашли уязвимости и записали себе на счет 1 млн баллов. Через год, когда клиент доработал свое ПО, взломать программу уже не смогли.

На онлайн-киберполигоне исследователям не нужно находиться по 12 часов в день, как это происходит на интенсивной офлайн-битве. Здесь защитники могут отслеживать и расследовать даже те атаки, которые развиваются в течение многих месяцев. Фактически это своего рода threat intelligence, или киберразведка: можно проследить действия нападающих практически в прямом эфире. Кроме того, можно расследовать самые опасные атаки, которые в реальной жизни могут развиваться месяцами, — так называемые advanced persistent threats.

Онлайн-полигон позволяет проверить собственные средства защиты информации, максимизировать и отточить их работу. Можно поэкспериментировать с разными параметрами СЗИ, испытать их отработку на практике. Для реальной инфраструктуры такие эксперименты чреваты опасными последствиями, а на киберполигоне они вполне возможны.

По умолчанию на полигоне, конечно, используются средства защиты информации, созданные Positive Technologies, но клиенты справедливо хотят иметь возможность разместить на Standoff продукты других производителей, чтобы сравнить решения, провести пилотное внедрение или отработать свою работу с теми СЗИ, с которыми реально работает их команда.

**Основные возможности Standoff 365**

*Киберполигон:*

* Моделирование инфраструктуры:
* Платформа имитирует реальные корпоративные инфраструктуры, включая бизнес-процессы, ИТ-системы и средства защиты.
* Это позволяет анализировать взаимодействие компонентов и проверять их устойчивость к кибератакам.

*Проведение киберучений:*

* Участники могут выполнять роли атакующих (Red Team), защитников (Blue Team) и наблюдателей (White Team).
* Реализуются сценарии реальных атак, таких как компрометация данных, отключение критической инфраструктуры и кража конфиденциальной информации.

*Тестирование инструментов безопасности:*

* Платформа позволяет проверять работу средств защиты информации в условиях реальных атак.

*Bug Bounty программы:*

* Компании могут запускать программы по поиску уязвимостей в своих продуктах или системах.
* Привлечение внешних исследователей (этических хакеров) для поиска и исправления уязвимостей.
* Предлагаются значительные денежные вознаграждения за найденные проблемы.

*Dream Hunting (уникальная опция):*

* Участникам предлагаются сложные сценарии атак, такие как:
  + Внедрение вредоносного кода в программное обеспечение компании.
  + Кража денежных средств или критически важных данных.
* Вознаграждения за выполнение задач могут превышать $650,000, что делает платформу привлекательной для высококвалифицированных специалистов.

*Встречи сообщества:*

* Регулярные мероприятия для специалистов, на которых обсуждаются новейшие методики защиты, тенденции кибератак и инструменты обеспечения безопасности.
* Платформа поддерживает развитие профессионального сообщества специалистов по кибербезопасности.

**Применение Standoff 365**

*Для компаний:*

* Выявление слабых мест в защите до реальных атак.
* Подготовка сотрудников к эффективному реагированию на инциденты.
* Улучшение стратегии защиты данных и ИТ-инфраструктуры.

*Для специалистов:*

* Участие в киберучениях позволяет приобрести практический опыт.
* Возможность получения вознаграждений за найденные уязвимости.
* Обмен опытом и знаниями в рамках профессионального сообщества.

**Преимущества Standoff 365**

*Масштабируемость:*

* Платформа поддерживает моделирование как небольших, так и крупных корпоративных сетей.

*Реализм:*

* Используются сценарии реальных атак, основанные на анализе текущих угроз.

*Совместимость:*

* Поддержка различных систем и технологий для проведения комплексных киберучений.

*Поддержка профессионального сообщества:*

* Привлечение специалистов со всего мира для поиска уязвимостей и отработки навыков защиты.

**Результаты использования Standoff 365**

*Популярность среди компаний:*

* С момента запуска платформа привлекла более 4000 специалистов и десятки организаций.
* Выплаты за найденные уязвимости составляют миллионы рублей, что подчеркивает её востребованность.

*Повышение квалификации специалистов:*

* Участники получают уникальные навыки, которые сложно развить в условиях реальной работы без угрозы для бизнеса.

Standoff 365 от Positive Technologies — это не просто платформа, а экосистема для повышения уровня кибербезопасности, где объединяются интересы бизнеса, исследователей и профессионального сообщества.

**Киберполигон Ampire (**АО «Перспективный мониторинг») предназначен для обучения, подготовки и тренировки специалистов по информационной безопасности для государственных организаций, кредитно-финансовой сферы, объектов критической информационной инфраструктуры, телекома и других отраслей.

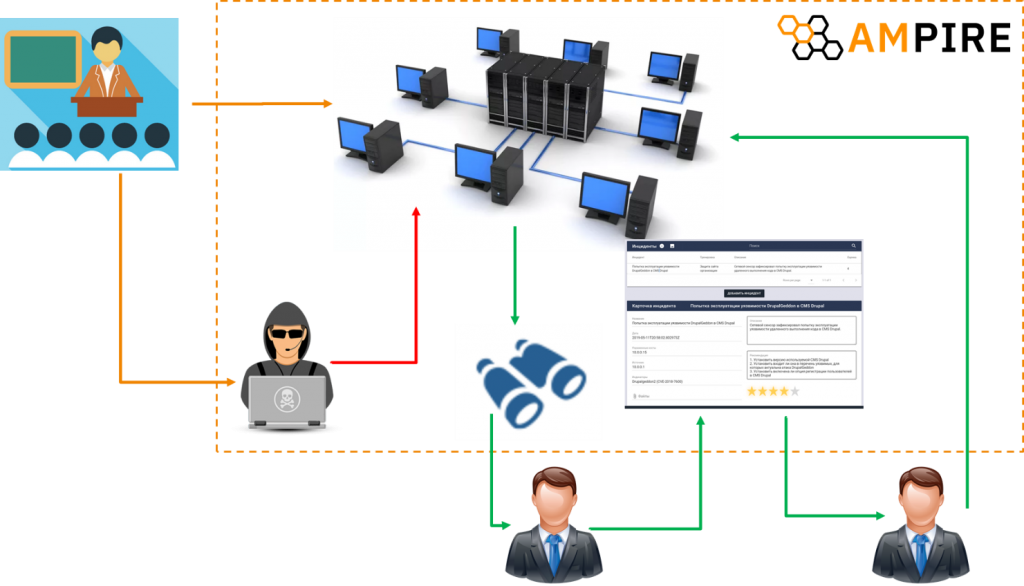
Ampire решает следующие задачи:

* помогает отработать навыки выявления компьютерных атак и расследования инцидентов информационной безопасности;
* учит оценивать защищённость элементов информационных сетей;
* налаживает взаимодействие между подразделениями;
* показывает способы нейтрализации и предупреждения компьютерных атак.

В ходе киберучений на Ampire сотрудники профильных подразделений получат следующие основные навыки:

* мониторинг и обнаружение компьютерных атак;
* работа со специальным программным обеспечением для обнаружения и анализа событий информационной безопасности;
* настройка и применение средств защиты информации;
* разработка предложений по исправлению выявленных недостатков безопасности;
* проведение расследований и нейтрализация последствий компьютерных инцидентов.

*Как устроен Ampire:*



В Ampire каждый пользователь принадлежит к одной из трёх категорий: администратор, преподаватель или обучаемый.

Администратор отвечает за развёртывание системы и организацию пользовательской инфраструктуры. Он может создавать/блокировать пользователей, назначать пользователей преподавателями, управлять шаблонами информационных систем (добавлять, редактировать, удалять). Администратор не имеет доступа к интерфейсу преподавателя и интерфейсу обучаемого.

Преподаватель отвечает за проведение киберучений. Он создаёт, редактирует и удаляет профили участников тренировки, включает их в группы мониторинга и реагирования, создаёт тренировки на базе имеющихся шаблонов.

Для отработки навыков обнаружения и устранения последствий компьютерных атак преподаватель управляет виртуальными нарушителями: запускает и останавливает сценарии атак, выполняет отдельные этапы.

Для оценки качества работы группы мониторинга преподаватель может просматривать и оценивать создаваемые обучаемыми карточки инцидентов. Для выдачи рекомендаций обучаемым преподавателю доступна система быстрых сообщений (мессенджер).

Во время тренировки преподаватель может отслеживать статусы заложенных в шаблон уязвимостей, корректность работы всех узлов шаблона, на котором проходит тренировка.

Группа мониторинга следит за событиями информационной безопасности, заводит карточки инцидентов, подтверждает инциденты, заведённые автоматическими средствами.

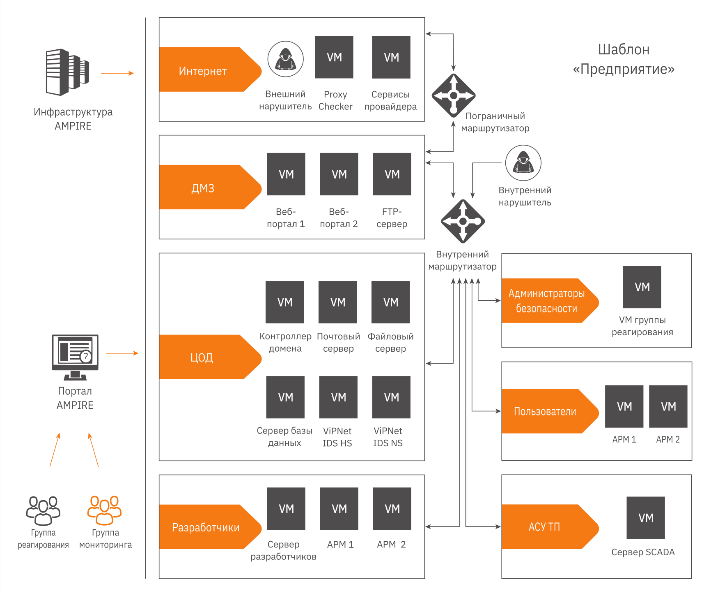
Участники групп мониторинга и реагирования имеют доступ к встроенным в шаблон средствам обнаружения компьютерных атак и дополнительным системам защиты информации, характерным для выбранной тренировки.

Одно из преимуществ Ampire — это невозможность что-то сломать. Виртуальная инфраструктура, на которой проходит каждая тренировка, разворачивается копированием из шаблона, поэтому команды могут действовать свободно, без опаски повредить какой-либо объект инфраструктуры или сервис. При необходимости, новая копия информационной сети восстанавливается за 3–5 минут (в зависимости от сложности шаблона).

Ampire позволяет моделировать типовые и специализированные информационные системы (Шаблоны), активировать векторы компьютерных атак, характерные для внешнего и внутреннего нарушителей (Сценарии). Комплекс предоставляет пользователю специализированное ПО для обнаружения следов компьютерных атак и инструменты для повышения уровня защищённости информационной системы, на которой проходит тренировка.

*Шаблоны:*

Шаблон информационной системы в Ampire — это набор виртуальных машин (сервера, рабочие станции, сетевое оборудование и т.д.), которые моделируют работу типовой сети организации (например, офис, банк, предприятие). Состав шаблонов в комплексе определяется на момент поставки, но может быть расширен по требованиям заказчика. Эта потребность возникает в основном из-за желания проводить обучение на макетах информационных систем, максимально близких к уже существующим у заказчика. Шаблон можно дополнить специфическими для конкретного заказчика сервисами, оборудованием и средствами защиты информации (учитывая возможность работы в виртуальной среде и лицензионные ограничения).



*Пример логической схемы одного из существующих типовых шаблонов.*

При запуске тренировки преподаватель разворачивает экземпляр информационной инфраструктуры на базе одного из имеющихся в комплексе шаблонов.

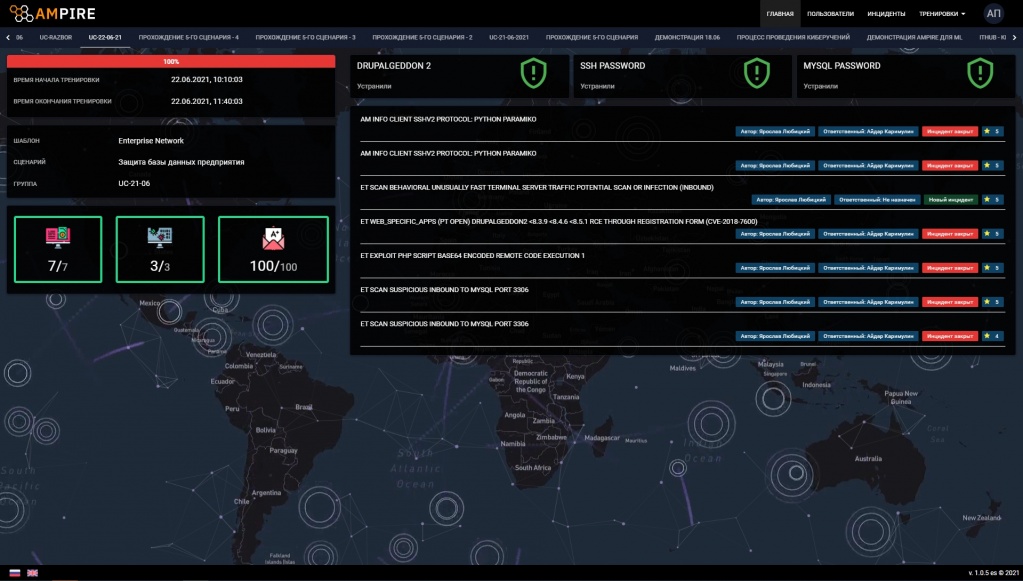
*Сценарии:*

Сценарий в Ampire — это имитация реальной компьютерной атаки на инфраструктуру. Сценарии атак разрабатывают сотрудники «Перспективного мониторинга», которые проводят десятки проектов по тестированию на проникновение в год («белые хакеры») или работают с инцидентами в Центре мониторинга.

Все действия атакующего автоматизированы в рамках сценария, поэтому для проведения полноценных киберучений нет необходимости привлекать «живую» атакующую команду.

При прохождении командами сценария преподаватель самостоятельно управляет виртуальными нарушителями: активирует, останавливает, даёт задание на выполнение отдельных шагов.

На главном информационном экране киберполигона отображается статус тренировки, статус устранения имеющихся уязвимостей в экземплярах информационных систем, заведённые в рамках прохождения сценария.



*Форматы проведения киберучений:*

При очном формате киберучений группы студентов работают непосредственно в классе одного из учебных заведений, оборудованных комплексом Ampire или имеющих подключение к облачной версии комплекса.

С командами на месте работают один-два преподавателя, помогая отрабатывать запланированные сценарии. Преподаватели оценивают карточки инцидентов, отвечают на вопросы, дают советы по процессам мониторинга, реагирования и взаимодействия команд.

В онлайн-киберучениях члены команд подключаются к комплексу удалённо по VPN-каналу со своих рабочих мест. Преподаватель работает со студентами в режиме видеоконференцсвязи и через сервисы мгновенных сообщений, в которых созданы чаты для команд.

Преимуществом такого подхода является независимость от географического расположения участников и возможность объединения в команды студентов из разных точек.

*С преподавателем и без преподавателя:*

При проведении киберучений крайне важно наличие преподавателя или координатора. Это может быть сотрудник организации, которая приобрела учебно-тренировочную платформу Ampire (обучение и методические материалы включены в поставку), сотрудник компании-разработчика комплекса АО «Перспективный мониторинг» или сотрудник одного из учебных центров.

Мы также можем предоставить доступ к киберполигону просто как к облачному решению. В данном случае «Перспективный мониторинг» берёт на себя только вопросы работоспособности комплекса; за проведение киберучений полностью отвечает заказчик.

*Мобильный комплекс:*

Команда Ampire Team разработала мобильную версию киберполигона, предназначенную для проведения выездных тренировок на площадке заказчика.



Мобильный Ampire состоит из:

* сервера формата tower, производительности которого достаточно для работы одной копии инфраструктуры предприятия;
* девяти ноутбуков для участников киберучений;
* ноутбука преподавателя;
* маршрутизатора;
* монитора;
* комплекта коммутации и периферии.

Всё оборудование перевозится в жёстком кофре на колёсах, который обеспечивает сохранность устройств и может быть рабочим местом преподавателя.

Предусмотрена возможность покупки или аренды мобильного Ampire и проведения тренировок с привлечением преподавателей «Перспективного мониторинга» или учебных центров.

Помимо описанных, возможны разнообразные комбинации вариантов проведения киберучений в зависимости от организационных (наличие места проведения, необходимость командирования сотрудников на обучение, сроков и т. д.) и технических (интернет-подключение, наличие необходимого числа выделенных рабочих мест и т. д.) возможностей заказчика. Всегда можно подобрать устраивающие все стороны решение и формат.

*Соответствие государственным образовательным стандартам:*

Учебные заведения могут создавать на базе киберполигона Ampire лаборатории для обучения практическим аспектам информационной безопасности как студентов, так и слушателей программ дополнительного образования, в том числе курсов повышения квалификации и профессиональной переподготовки.

Такая лаборатория практически полностью соответствует требованиям федеральных государственных стандартов к материально-техническому и учебно-методическому обеспечению программ по специальностям: Информационная безопасность (10.03.01 и 10.04.01), Информационная безопасность автоматизированных систем (10.05.03), Безопасность информационных технологий в правоохранительной сфере (10.05.05), а также в значительной степени дополняет возможности лабораторий по специальностям Информационные системы и технологии (09.03.02 и 09.04.02) и Информационно-аналитические системы безопасности (10.05.04).

Учебные заведения могут приобрести учебно-тренировочную платформу Ampire на особых условиях по академической лицензии.

**Сравнительный анализ киберполигонов**

|  |  |  |  |
| --- | --- | --- | --- |
|  | Национальный киберполигон РФ | Ampire | Standoff 365 |
| Разработчик | «Ростелеком» | «Перспективный мониторинг» | Positive Technologies |
| Основная цель | Подготовка специалистов, повышение киберустойчивости организаций и проведение национальных киберучений | Тренировка навыков специалистов, моделирование атак | Проведение киберучений, программ Bug Bounty и моделирование сложных атак |
| Масштаб применения | Федеральный уровень, в рамках национальной программы «Цифровая экономика» | Корпоративный и отраслевой уровень | Международный, с акцентом на широкий круг компаний и исследователей |
| Особенности инфраструктуры | Интеграция с реальными инфраструктурами компаний; используется в ВУЗах и госучреждениях | Моделирование инфраструктуры компаний, включая IoT и критическую инфраструктуру | Высокий уровень реализма; поддержка сложных сценариев атак |
| Участники | Государственные структуры, крупные корпорации, образовательные учреждения | Корпоративные клиенты, специалисты по ИБ | Этические хакеры, крупные компании, исследователи |
| Функционал | - Проведение национальных киберучений - Моделирование угроз - Анализ защищенности госструктур | - Моделирование атак - Тренировка защитных сценариев - Отработка защиты IoT и промышленной автоматизации | - Моделирование атак и защиты - Проведение киберучений - Программы Bug Bounty - Конкурсы Dream Hunting |
| Поддержка сообществ | Поддержка образовательных и государственных инициатив | Поддержка специалистов по ИБ | Программы обучения и объединение исследователей через встречи сообщества |
| Уровень сложности | Средний — ориентирован на подготовку широкого круга участников | Высокий — поддержка сложных сценариев атак | Очень высокий — включает сложные задания, такие как Dream Hunting |
| Масштабируемость | Ограничена федеральным и национальным уровнями | Легко адаптируется под потребности компаний | Гибкость и возможность настройки под любые сценарии |
| Программы Bug Bounty | Нет | Нет | Есть, с крупными вознаграждениями |
| Вознаграждения участникам | Нет | Нет | Есть, до $650,000 за выполнение сложных сценариев |
| Обучение и тренировки | Основной фокус: тренировка госструктур и студентов | Основной фокус: корпоративные команды и эксперты | Основной фокус: широкий круг участников, включая хакеров и корпоративные команды |
| Интеграция с реальными системами | Да | Частичная | Да |
| Преимущества | - Поддержка госструктур и национальных инициатив - Развитие образования | - Подходит для корпоративных тренировок - Включает промышленную инфраструктуру | - Высокая гибкость и реализм - Программы вознаграждений - Привлечение исследователей со всего мира |
| Недостатки | Ограниченность масштабов и участников | Отсутствие международного охвата, слабая поддержка сообществ | Требует высокого уровня подготовки участников |

# Заключение

*Анализ состояния и перспектив киберполигонов*

*Роль киберполигонов в информационной безопасности*

Киберполигоны представляют собой инновационные платформы для проведения учений по кибербезопасности в условиях, максимально приближенных к реальности. Они обеспечивают моделирование бизнес-процессов и инфраструктуры предприятий различных отраслей, таких как финансовый сектор, энергетика, транспорт и телекоммуникации. Это позволяет участникам не только отрабатывать навыки реагирования на инциденты, но и проверять готовность предприятий к отражению атак. Ключевые функции киберполигонов включают:

* Моделирование современных атак;
* Разработку стратегий защиты;
* Обучение специалистов различного уровня подготовки.

Киберполигоны становятся критически важным инструментом в условиях роста числа и сложности кибератак, особенно в период массовой цифровизации и обострения геополитической ситуации. Они позволяют минимизировать риски реального ущерба, одновременно обучая сотрудников реагировать на потенциальные угрозы.

*Актуальность и текущая ситуация на рынке*

Рост числа атак:

* В 2023 году количество выявленных событий безопасности увеличилось на 68% по сравнению с 2022 годом. Основные цели атак – ИТ-компании, промышленность и ритейл, что связано с высокой степенью цифровизации этих отраслей.
* Более 170 кибератак фиксируется ежедневно в России, что подтверждает возрастающую угрозу для ключевых секторов экономики.

Дефицит кадров:

* По данным исследований, более 50% российских компаний сталкиваются с нехваткой специалистов по информационной безопасности. Этот дефицит препятствует внедрению комплексных решений и технологий защиты.
* Киберполигоны решают эту проблему за счет создания учебных площадок на базе вузов, позволяя оперативно переучивать специалистов и привлекать новые кадры в отрасль.

Растущая сложность угроз:

* Современные атаки часто затрагивают цепочки поставок и интегрированные системы, что может привести к каскадным сбоям. Киберполигоны помогают моделировать такие сценарии и оценивать их последствия.

*Динамика и тенденции развития рынка*

Мировой рост:

* Мировой рынок киберполигонов оценивается в 1,2 млрд долларов США (2023 год) и ожидается, что к 2032 году он достигнет 3,5 млрд долларов при среднегодовом темпе роста 12,5%. Ключевые драйверы – цифровизация и рост числа атак.

Интеграция с ИИ и ML:

* Использование искусственного интеллекта и машинного обучения расширяет возможности киберполигонов, позволяя создавать адаптивные сценарии, проводить анализ в режиме реального времени и моделировать сложные угрозы.

Развитие облачных решений:

* Облачные киберполигоны делают технологии доступными для малого и среднего бизнеса, устраняя барьеры, связанные с высокими затратами на локальное развертывание.

*Сегментация и ключевые пользователи*

Образование:

* Киберполигоны интегрируются в образовательные программы, предоставляя студентам и преподавателям возможность приобретать практические навыки. Такие инициативы формируют кадровый резерв и способствуют развитию STEM-образования.

Оборонный сектор:

* Обеспечивает подготовку военных специалистов, позволяет моделировать кибервойны и проверять устойчивость сетей критической инфраструктуры.

Финансовые учреждения:

* Активно используют киберполигоны для обучения персонала и тестирования защиты от атак на конфиденциальные данные.

ИТ и телекоммуникации:

* Сектор требует регулярных тренировок для опережения развивающихся угроз, что делает платформы киберполигонов важной частью защиты инфраструктуры.

Малый и средний бизнес:

* Несмотря на ограниченные бюджеты, этот сегмент активно внедряет облачные решения, осознавая необходимость обучения сотрудников и тестирования защиты.

*Технологические аспекты*

Киберполигоны включают типовые модули и подсистемы:

* Моделирование инфраструктуры: эмуляция реальных сетей и оборудования, что позволяет анализировать взаимодействие систем.
* Сценарии атак: как автоматизированные, так и настраиваемые, обеспечивают обучение в условиях, имитирующих реальные угрозы.
* Сбор и анализ данных: позволяет выявлять уязвимости и разрабатывать стратегии их устранения.
* Современные платформы, такие как Standoff 365 и Ampire, используют ИИ и ML для анализа угроз в режиме реального времени, а также предлагают инструменты для моделирования нестандартных атак.

*Перспективы развития*

Интеграция с государственными инициативами:

* В России Национальный киберполигон активно используется для подготовки специалистов и проведения киберучений. Планируется расширение сети опорных центров в вузах до 15 точек.

Международное сотрудничество:

* Киберполигоны используются для координации усилий против кибератак на глобальном уровне, включая обмен информацией между странами.

Расширение сегментов применения:

* Ожидается развитие инфраструктуры, охватывающей транспортную, металлургическую и горнодобывающую отрасли.

Индивидуализация решений:

* Платформы киберполигонов будут настраиваться под потребности конкретных отраслей и предприятий, обеспечивая высокую адаптивность и точность.

***Выводы***

Киберполигоны становятся ключевым элементом в обеспечении кибербезопасности, предоставляя уникальные возможности для обучения, тестирования и повышения квалификации. Рост рынка поддерживается развитием технологий, глобальными угрозами и необходимостью подготовки специалистов. В ближайшие годы основное внимание будет уделено созданию более доступных решений, интеграции с государственными инициативами и расширению функционала, что обеспечит их устойчивое развитие и востребованность на мировом уровне.

***Литература***

[Киберполигон Ampire](https://amonitoring.ru/product/ampire/)

[Обзор рынка киберполигонов (Cyber Polygons)](https://www.anti-malware.ru/analytics/Market_Analysis/Cyber-Polygons#part1)

[Киберполигон](https://cyberpoly.ru/?ysclid=m2uhejecuo889320311)

[Киберучения в национальном масштабе: как работают киберполигоны в России — РБК](https://www.rbc.ru/technology_and_media/01/11/2022/635bfe3f9a794799a7e0b42e?ysclid=m2uhf3f8jv356864195)

[Защита от цифровых атак: как в России работают киберполигоны | Национальные проекты РФ](https://xn--80aapampemcchfmo7a3c9ehj.xn--p1ai/news/zashchita-ot-tsifrovykh-atak-kak-v-rossii-rabotayut-kiberpoligony/)

[Роль киберполигона в обеспечении ИБ](https://www.securityvision.ru/blog/rol-kiberpoligona-v-obespechenii-ib/?ysclid=m2uhfsdffu767255282)

[Будь готов: возможности и польза киберполигона](https://blogs.forbes.ru/2023/12/14/bud-gotov-vozmozhnosti-i-polza-kiberpoligona/?ysclid=m2uhg5je2616838459)

[Хочешь мира – готовься к войне или зачем нужен киберполигон](https://www.securitylab.ru/analytics/512874.php?ysclid=m2uhgkkih3346449579)

[Расширяем возможности SOC поведенческой аналитикой](https://ib-bank.ru/kadry/files/files/presentations/13/vitkova.pdf?ysclid=m2uhj60avm663238378)

[Российские безопасники представили новый отечественный киберполигон](https://www.securitylab.ru/blog/company/awillix/352600.php)

[Киберполигоны в стадии роста: преимущества и перспективы - Connect, №5-6, 2024](https://amonitoring.ru/article/kiberpoligony-v-stadii-rosta-connect/?ysclid=m45klsvr1i986378919)

[Отчет об исследовании рынка платформ Cyber Range за 2032 год](https://dataintelo.com/report/cyber-range-platform-market)

[Число кибератак в России и в мире](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A7%D0%B8%D1%81%D0%BB%D0%BE_%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA_%D0%B2_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8_%D0%B8_%D0%B2_%D0%BC%D0%B8%D1%80%D0%B5?ysclid=m45mtrvawl563743242)

[Otchet\_KIBERATAKI-NA-ROSSIYSKIE-KOMPANII-V-1-KV-2024-updated.pdf](https://rt-solar.ru/upload/iblock/3df/gdh0ltkza37nqjgbkl1x25t8gwtwgofh/Otchet_KIBERATAKI-NA-ROSSIYSKIE-KOMPANII-V-1-KV-2024-updated.pdf?ysclid=m45my0u4ke572073671)

[КИБЕРМИР - Национальный киберполигон](https://cybermir.ru/?ysclid=m45npgyrxk776768203)

[Как выйти на новый уровень безопасности, используя киберполигон](https://www.anti-malware.ru/practice/methods/Standoff-365-Cyber-Polygon)

[Standoff 365](https://standoff365.com/?ysclid=m45wfz57du413372600)