
STANDOFF
ПРАВИЛА

# Содержание

# 1. О платформе Standoff 365

Standoff 365 — это социальная платформа, позволяющая общаться и обмениваться опытом, киберполигон для проведения киберучений и исследовательская площадка для проверки защищенности систем и оборудования. В основе платформы лежит технология быстрого развертывания и доступа к информационной инфраструктуре и подключения к ней внешних систем и оборудования.

Платформа позволяет проводить киберучения Standoff для исследования атак на информационную инфраструктуру и приложения, а также для реагирования на инциденты. На платформе разворачиваются сегменты полигона. В них воссоздаются информационные системы и процессы, характерные для предприятий определенной отрасли — торговых фирм, банков, телеком-операторов, промышленных предприятий. Каждая отрасль может включать в себя один или несколько сервисов, которые регулируют деятельность организации или обеспечивают ее информационную безопасность. Сервисами могут быть, например, почтовый сервер, FTP-сервер, база данных клиентов, система документооборота, межсетевой экран, система управления светофорами, ветрогенераторы.

Участники распределены по командам и объединены общей целью. В Standoff предусмотрены два типа команд — команда атакующих и команда защитников. Цель атакующих — реализовывать недопустимые события, например парализовать работу АСУ ТП или получить доступ к конфиденциальной информации. Задача защитников — своевременно выявлять и расследовать инциденты.

Команды атакующих за свои действия получают баллы, а действия команд защитников оцениваются в виде метрик.

Информация о ходе киберучений, оценки действий участников и задания отображаются на платформе Standoff 365, доступ к которой предоставляет организатор.

# 2. Правила для атакующих

Этот раздел содержит информацию о подготовке к киберучениям, подключении к полигону и правила участия в киберучениях для команды атакующих.

### В этом разделе



## 2.1. Подготовка

Команда атакующих получает доступ к полигону перед началом мероприятия. Команде предоставляются конфигурационные файлы, данные учетной записи для подключения и другая информация, необходимая для участия.

## 2.2. Подключение

Подключение осуществляется через VPN-сервер с помощью данных, полученных от организаторов в процессе подготовки.

## 2.3. Ход киберучений

В ходе киберучений атакующие должны реализовать недопустимые события, выполняя предоставленные задания, и получать за это баллы.

Киберучения ограничены по времени. Оставшееся до конца киберучений время отображается на платформе Standoff 365. В киберучениях предусмотрена возможность технических перерывов.

Разрешается атаковать только сервисы информационной инфраструктуры, расположенные по адресам, предоставленным организаторами. Атаки на адреса, не входящие в список предоставленных, не учитываются при начислении баллов. Сервисы, расположенные за пределами инфраструктуры, предоставленной организаторами, не входят в рамки полигона и запрещены для атак.

> Внимание! За использование служебных учетных записей или попытку получения доступа к ним организаторы могут отстранить команду от киберучений. Список учетных записей будет опубликован во время мероприятия.

> Внимание! Командам атакующей стороны запрещено исправлять обнаруженные уязвимости или блокировать попытки эксплуатации. За это организаторы вправе оштрафовать или дисквалифицировать команду.

Внимание! За атаку на адреса, не входящие в предоставленный список, организаторы могут отстранить команду атакующих от киберучений. Кроме того, командам запрещается проводить DoS- и DDoS-атаки на службы, сервисы и приложения инфраструктуры полигона. Организаторы могут отстранить от киберучений команду, которая проводит такие атаки.

Баллы можно получать следующими способами:

— **Выполнять задания, предложенные организаторами.** Задания могут быть связаны, например, с получением конфиденциальной информации, выводом из строя одного или нескольких сервисов или подменой информации на официальных сайтах компаний.

— **Находить уязвимости.** Команда атакующих может представить отчет об уязвимостях, найденных в информационной инфраструктуре. Список подсетей для поиска уязвимостей ограничивается отдельно, его можно получить на игровом портале.

— **Выполнять другие задания, представленные в личном кабинете участника.**

## 2.4. Задания

В киберучениях в качестве заданий используются приближенные к реальности ситуации. Задание дано в карточке уязвимости или недопустимого события, там же указана стоимость задания в баллах.

## 2.5. Подсчет баллов

Выполнение заданий оценивается организаторами. На основе полученных баллов формируется рейтинг команд. Выигрывает команда, набравшая наибольшее число баллов.

Внимание! Организаторы вправе дисквалифицировать команду, если она пытается выдать отчет другой команды за свой.

### В этом разделе

Баллы за выполнение заданий (см. раздел 2.5.1)

Баллы за поиск уязвимостей (см. раздел 2.5.2)

## 2.5.1. Баллы за выполнение заданий

Задание считается выполненным, если ответ на него был принят как верный. Чтобы отправить ответ на проверку, нужно представить отчет в определенном формате (шаблон отчета вы можете скачать на странице недопустимого события).

За каждое выполненное задание атакующим начисляются баллы. Кроме того, организаторы могут оценить работу команды и начислить дополнительные или снять штрафные баллы. Команда, которая выполнила задание первой, получает максимальный балл. В случае если две команды выполнили задание одновременно, организаторы могут начислить обеим командам максимальный балл.

Если в отчете недостаточно информации о том, как было выполнено задание, отчет не принимается и баллы не начисляются. В этом случае организаторы оставляют в личном кабинете соответствующий комментарий с замечаниями к сданному отчету. После исправления недостатков отчет можно сдать повторно.

## 2.5.2. Баллы за поиск уязвимостей

Чтобы найденная уязвимость была зачтена организаторами, нужно представить отчет в произвольной форме. В отчете необходимо привести пример эксплуатации уязвимости и — в зависимости от типа обнаруженной уязвимости — получить баннер с версией СУБД, прочитать локальный файл, отправить произвольный HTTP-запрос или показать вывод команд `ipconfig`/`ifconfig`, `whoami` или `id`.

Принимаются только определенные классы уязвимостей — RCE, SQLi, Path Traversal, XXE, SSRF.

За каждую найденную и принятую организаторами уязвимость команда получает баллы.

# 3. Правила для защитников

Этот раздел содержит информацию о подготовке к киберучениям, подключении к полигону и правила участия в киберучениях для команды защитников.

### В этом разделе



## 3.1. Подготовка

Команда защитников заранее (обычно за месяц) получает доступ к полигону и может с ним ознакомиться. Команде предоставляются конфигурационные файлы, данные учетной записи для подключения и другая информация, необходимая для участия.

При ознакомлении с инфраструктурой полигона команды защиты получают доступ к сканеру уязвимостей. Учетные записи от объектов инфраструктуры для запуска процедуры инвентаризации и сканирования командам выдаются организаторами. Команда может использовать любой другой сканер уязвимостей, но устанавливает его самостоятельно.

После ознакомления с полигоном команда предоставляет организаторам список средств защиты, которые она планирует использовать, а также схему их размещения. В общем случае команды ограничены следующими классами средств защиты: next-generation firewalls, application firewalls, системы security information and event management. Использование иных средств защиты согласовывается с организаторами отдельно.

## 3.2. Подключение

Подключение осуществляется через VPN-сервер с помощью данных, полученных от организаторов в процессе подготовки.

## 3.3. Ход киберучений

Основная цель защитников — обнаружение и расследование инцидентов, вызванных действиями атакующих. В ходе киберучений команда защитников получает опыт по защите инфраструктуры в условиях, максимально приближенных к реальным.

Киберучения ограничены по времени. Оставшееся до конца киберучений время отображается на платформе Standoff 365.

Для оценки действий команд защитников учитываются количество зафиксированных инцидентов и среднее время расследования одной атаки.

В этом разделе



## 3.3.1. Количество зафиксированных инцидентов

Перед командой защитников в первую очередь стоит задача выявления инцидентов на защищаемых ими предприятиях. В процессе противостояния команды защитников могут отправлять отчеты о выявленных ими инцидентах в определенном формате (шаблон отчета и пример заполнения доступны на платформе Standoff 365).

Отчеты оцениваются организаторами. Если в отчете недостаточно информации, организаторы не принимают такой отчет и оставляют соответствующий комментарий к нему на игровом портале. Отчет можно скорректировать и сдать повторно.

В истории защищаемого объекта на платформе Standoff 365 будет периодически обновляться информация о том, какое количество инцидентов было зафиксировано командой защитников. Если команда защитников не зафиксировала инциденты, но их зафиксировали организаторы, будет выводиться информация от организаторов.

## 3.3.2. Среднее время расследования атаки

После того как организаторы примут отчет о реализации недопустимого события от команды атакующих, команде защитников предоставляется информация о том, какое недопустимое событие было реализовано. Задачей команды защитников становится расследование этого недопустимого события. На игровом портале появляется таймер, который ведет отсчет времени проводимого расследования. Команда защитников должна представить организаторам отчет о расследовании реализации недопустимого события в определенном формате (шаблон отчета и пример заполнения доступны на платформе Standoff 365).

Отчеты оцениваются организаторами. Если в отчете недостаточно информации о действиях команды атакующих, отчет не принимается, о чем делается пометка на игровом портале. По оставленному организаторами комментарию команда защитников может провести дополнительное расследование, доработать отчет и повторно отправить его на проверку.

После того как организаторы приняли от команды защитников отчет о расследовании реализации недопустимого события, фиксируется время, за которое расследование было выполнено. При этом время, которое отчет находился на проверке у организаторов, не учитывается.

# Глоссарий

### Standoff

Открытые киберучения, которые проводятся несколько раз в год и могут быть приурочены к конференции по информационной безопасности.

### Standoff 365

Платформа для специалистов по информационной безопасности, которая включает в себя киберполигон, программы bug bounty, социальную сеть, тематические блоги и платформу для организации CTF-соревнований.

### атака

Комплекс действий атакующих, приводящий к реализации недопустимого события. По итогам успешной атаки «красные» сдают отчет о реализации недопустимого события.

### атакующие

Команда или отдельный участник, целью которых являются поиск уязвимостей и реализация недопустимых событий на полигоне.

### задание

Описание целей, которых должны достичь участники.

### защитники

Команда или отдельный участник, целью которых являются защита информационной инфраструктуры, обнаружение и расследование атак.

### игровой портал

Веб-приложение для управления процессом киберучений: добавления заданий, проверки отчетов атакующих и защитников, просмотра статистики.

### инцидент

Одиночное действие атакующих, направленное на нарушение доступности, целостности или конфиденциальности информации. По итогам расследования «синие» сдают отчет об отдельных инцидентах.

### киберучения

Комплекс мероприятий, организуемый для повышения уровня подготовки и развития навыков специалистов по информационной безопасности.

### недопустимое событие

Событие, в результате которого становится невозможным достижение операционных и стратегических целей организации или которое приводит к длительному нарушению ее основной деятельности. На платформе Standoff 365 цель атакующих — реализовать недопустимые события, а цель защитников — расследовать случаи их реализации.

### отчет о расследовании реализации недопустимого события

Отчет команды защитников, содержащий описание предполагаемых действий, выполненных атакующими для реализации недопустимого события. Шаблон для заполнения отчета находится в файле investigation_report_BLUE.xlsx.

### отчет о реализации недопустимого события

Отчет команды атакующих, содержащий описание действий, которые позволили реализовать недопустимое событие. Шаблон для заполнения отчета находится в файле unacceptable_event_report_RED.xlsx. Пример заполненного отчета находится в файле sample_unacceptable_event_report_RED.xlsx.

### отчет об инциденте

Отчет команды защитников, содержащий описание зафиксированного действия атакующих, влияющего на доступность, целостность и конфиденциальность информации. Шаблон для заполнения отчета находится в файле incident_report_BLUE.xlsm.

### отчет об уязвимости

Отчет команды атакующих об обнаруженной уязвимости.

### сегмент полигона

Отдельная виртуальная часть инфраструктуры киберполигона, в которой воссоздаются информационные системы и процессы, характерные для предприятий определенной отрасли.

### сервис

Объект инфраструктуры киберполигона, который управляет тем или иным процессом в информационной системе.

### уязвимость

Недостаток в системе, используя который, можно намеренно нарушить целостность, доступность и конфиденциальность информации.

Standoff 365 — это социальная платформа, позволяющая общаться и обмениваться опытом, киберполигон для проведения киберучений и исследовательская площадка для проверки защищенности систем и оборудования. В основе платформы лежит технология быстрого развертывания и доступа к информационной инфраструктуре и подключения к ней внешних систем и оборудования.

На киберполигонах Standoff воссоздается инфраструктура реальных предприятий различных отраслей мировой экономики. Атакующим и защитникам будет предоставлена возможность отработать свои навыки на объектах транспортной, нефтяной, добывающей и энергетической промышленности. Помимо этого, кибербитва развернется вокруг систем умного городского хозяйства, финансовых структур и многого другого.

Участие в Standoff позволяет протестировать возможность реализации кибератак и оценить масштабы их последствий в безопасной среде, получить новые знания и практические навыки выявления кибератак и противодействия им, изучить сценарии реагирования на известные и неизвестные риски, исследовать взаимосвязи кибербезопасности и бизнеса.

org@standoff365.com standoff365.com