

## ОСОБЕННОСТИ ОРГАНИЗАЦИИ СОРЕВНОВАНИЙ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ФОРМАТЕ STF В ШКОЛЕ

### **Кулавский Иван Владимирович,**

учитель информатики ГБОУ «Школа № 1584», Москва,  
победитель конференции «Наука для жизни» по направлению «Многообразие науки»  
в секции для педагогических работников

### **Викторова Татьяна Анатольевна,**

учитель информатики ГБОУ «Школа № 1584», Москва,  
магистрант МГУ им. М.В.Ломоносова, победитель конференции «Наука для жизни»  
по направлению «Многообразие науки» в секции для педагогических работников

Информационная безопасность — междисциплинарный комплекс знаний и умений. Для того, чтобы обучающийся достиг приемлемого уровня знаний и умений в сфере информационной безопасности, он должен владеть знаниями и умениями в следующих сферах: математика, информатика, программирование, технические средства защиты информации, криптография, основы вирусологии.

Раннее начало изучения практической области информационной безопасности по отношению к теоретическим знаниям, получаемым в рамках таких дисциплин, как информатика, математика, введение в информационную безопасность, позволяют сформировать более высокий интерес к освоению этих теоретических дисциплин и показывают учащемуся практическое значение теоретических знаний.

Одной из важнейших проблем современного образования является подготовка учащихся классов информационно-технологического профиля к решению вопросов в области информационной безопасности. Сегодня понятие «информационная безопасность» является важным при изучении раздела «социальная информатика» в школе, а в контексте

формирования технологического суверенитета страны оно становится интегративным и сквозным для всего курса информатики в школе на разных этапах обучения: пропедевтическом, базовом и профильном.

Мы считаем, что одним из эффективных способов повышения качества обучения информационной безопасности в школе и в ВУЗе в ограниченные



сроки — это использование активных методов обучения, направленных для решения практических задач и освоение технологий администрирования, программирования, расследования инцидентов, криптографических преобразования и исследования уязвимостей информационных систем. Формы проведения занятий с использованием активных методов обучения несколько отличаются от общепринятых и представлены в таких видах, как: соревнования CTF (Capture The Flag), хакатоны, мастер-классы, квесты, деловые игры по управлению информационной безопасностью, деловые ситуации, деловая разведка и другие. Все они объединены наличием игровых ситуаций. Игровые

формы активного обучения школьников профильных классов и студентов позволяют овладеть эффективными технологиями компьютерной безопасности и современными программно-аппаратными средствами их обеспечения за короткие сроки.

Соревнования по информационной безопасности CTF в настоящее время завоевывают большую популярность среди школьников и студентов. Они активно поддерживаются ведущими компаниями, занимающимися вопросами компьютерной безопасности, как одним из способов найти «новые кадры», привлечь новых людей к отрасли и повысить общий уровень профессиональных компетенций.

Во-первых, они создают достаточно мощную систему мотивации молодежи к овладению технологиями взлома информационных систем. Можно в достаточно короткие сроки овладеть технологиями pen-testing (тестирование на проникновение), чтобы получить определенный статус хакера. Во-вторых, необычный формат игровой формы, соревнований, в которой можно проявить творческие способности и знание технологий, становится более приемлемой формой обучения у молодежи в период активного развития ИТ. В-третьих, эти знания достаточно универсальны и могут использоваться в любой стране, где есть информационные технологии. Они становятся привлекательными для ИТ-компаний и создают перспективу продвижения и оплаты труда. В-четвертых, эти знания могут найти применение и в смежных областях знаний и профессиях: разработчиков программного обеспечения, администраторов информационных систем, администраторов безопасности.

Сегодня не все учителя информатики в школах знакомы с направлением СТФ, понимают суть и формат мероприятия. Некоторые считают, что это пустое времяпровождение. Другие полагают, что соревнования позволяют держать себя в форме, тренируют мозг. Но, кто участвовал в этих соревнованиях, полагают, что решая сложные СТФ-задачи, с повседневными справляешься быстрее, креативнее и неординарно. Сегодня крупные компании ищут сотрудников именно с опытом игры в СТФ (Яндекс, лаборато-

рия Касперского). В России более тысячи игроков СТФ, и все они известны специалистам. В мировых играх СТФ сильными игроками традиционно являются корейцы, китайцы, японцы, они решают безумно сложные задачи.

Мы считаем, что необходимо поднимать уровень российских ИТ-специалистов в области информационной безопасности, начиная с обучения в школе, в среде городских проектов «ИТ-вертикаль», «ИТ-класс», «Инженерный класс». Именно в школьные годы знания, умения и навыки развиваются с легкостью и быстротой и начинают надолго закрепляться в памяти ученика. Период обучения информатике в школе можно считать подходящим для формирования знаний, умений и навыков в конкретной профессиональной области, именно этот период способствует ранней профориентации и дальнейшей успешной профессиональной деятельности, например, в области информационной безопасности.

В настоящее время при обучении информационной безопасности школьников отсутствует единый подход по формированию компетенций, кратко рассматриваются аспекты программно-технических средств защиты информации, упоминается о необходимости обеспечения информационной безопасности на уровне государства, делается акцент на этику в интернете, сетевой этикет, нормы поведения в сети, этичное поведение при использовании информации. Анализ учебной литературы по информатике и собствен-

ного опыта позволяет сделать вывод о недостаточно разработанности вопросов подготовки школьников в области информационной безопасности с учетом их возрастных особенностей, недостаточное отражение и использование практических методов обучения, отбор содержания образования не отражает актуального развития сферы ИТ.

Для повышения эффективности учебного процесса, формирования у учащихся прочных теоретических знаний, практических навыков, обеспечения их профессиональной компетентности в будущем целесообразно использовать современные педагогические методы, помогающие им усвоить необходимые навыки и знания, к которым можно отнести STF-соревнования, квест- и кейс-технологии, проектную деятельность и др., так как выпускник класса информационно-технологического профиля должен понимать не только теоретические основы информационной безопасности, но и обладать практическими навыками противостояния информационным угрозам, уметь защищать собственное информационное пространство, анализировать данные, эффективно организовывать поиск информации в сети Интернет. Решение актуальных задач в формате STF обеспечивает реализацию новых возможностей в обучении, решает проблему активной познавательной деятельности учащихся, вовлекает их в образовательный процесс, о чем свидетельствует результат опроса участников соревнований STF, организованных на базе ГБОУ «Школа № 1584» в 2022–2023 уч.г. (рис. 1).

Несомненно, организация соревнований в формате STF в школах отличается от соревнований для студентов и специалистов по информационной безопасности, и не только в области сложности заданий. Поэтому перед учителями ГБОУ «Школа № 1584» встала непростая задача по организации подобных соревнований применительно к московской школе.

Наш практический опыт показал, что соревнование STF как результативный метод обучения сегодня имеет различные направления и требует научного, методического и творческого развития с учетом возрастных, индивидуальных особенностей и возможностей школьников на разных ступенях обучения в классах информационно-технологического профиля. Учебные задания в форматах STF позволяют резко повысить эффективность обучения и обеспечить готовность будущего кадрового потенциала в сфере ИТ к решению новых возникающих задач в сфере компьютерной безопасности.

Существуют два формата проведения соревнований по компьютерной безопасности в формате STF:

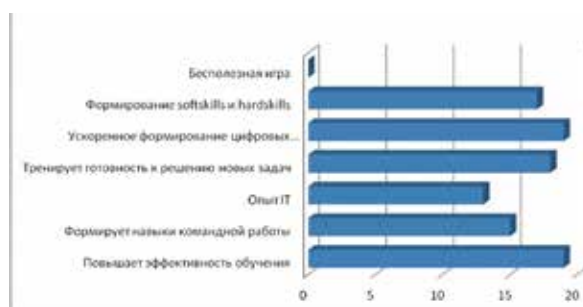


Рис. 1. Результат опроса участников соревнований STF на базе ГБОУ Школа № 1584

- *во-первых*, это формат task-based (или jeopardy) — когда игрокам предоставляется набор задач (заданий), к которым требуется найти ответ и отправить его. Ответ представляет собой флаг: это может быть набор символов или произвольная фраза. За верно выполненное задание команда получает определенное количество очков. Чем задание сложнее, тем больше очков предусмотрено за правильный ответ.

- *во-вторых*, это формат attack-defense — когда каждая команда получает выделенный сервер или небольшую сеть для поддержания её функционирования и защиты. Во время игры команды получают очки за корректную работу сервисов своего сервера и за украденную информацию (флаги) с серверов соперников. В лучшем случае, если эта работа выполняется командами (3–5 человек), когда идет некоторое распределение ролей обучаемых. В этом случае учитель выступает в роли эксперта и создает условия для управления игровой ситуацией.

Участие в CTF-соревнованиях требует поиска информации в открытых источниках — а этому тоже нужно научиться. В будущем такие задания плавно переходят к реальным кейсам, а участники уже имеют опыт, позволяющий им легче решать любые профессиональные задачи.

Предлагаемые участникам соревнований задания максимально приближены к реальным ситуациям (что и делает соревнования особенно интересными

и захватывающими) и должны обогащать знаниями и умениями, повышать квалификацию участников. В противном случае, работа с заданиями в условиях соревнований может вызвать «разочарование и недоумение».

В CTF-соревнованиях все задания разделяются по категориям:

1. Поиск и использование Web-уязвимостей (Web).
2. Анализ бинарного кода (Reverse).
3. Компьютерно-криминалистическая экспертиза (Forensic).
4. Криптография (Crypto).
5. Стеганография (Stego).
6. Поиск по открытым источникам (Osint).
7. Программирование (PPC)

Задания на поиск локальных уязвимостей часто связаны с поиском обходных путей или эксплуатацией недоработок программных и операционных систем. Это напрямую связано с изучением особенностей устройства операционных систем (ОС) и процессом администрирования ОС и ее политики безопасности. Полученные знания также помогут прогнозировать и предотвращать подобные проблемы в будущем на реальных рабочих системах.

Задания на поиск Web-уязвимостей основаны на некорректных программных реализациях Web-сервисов, часто связаны с применением SQL-инъекций, межсайтового взаимодействия и встраивания чужого кода. Работа с подобными проблемами позволяет получить более глубокие знания в области безопасного программирования, разработки надежных программных продуктов, анализа

программного кода, а также выполнения тестов на взлом и проникновение.

Задания, связанные с реверс-инжинирингом являются одними из самых сложных и требуют глубокого понимания низкоуровневого программного кода, особенностей работы современных компиляторов и функционирования программ в рабочем пространстве операционных систем.

Также напрямую с глубоким изучением и пониманием изучаемых в рамках направления информационно-технологического профиля в школе связаны задания на форензику, криптографию, стеганографию, Osint. Эти задания позволяют поддерживать в актуальном состоянии получаемые в ходе обычного обучения знания, а также проникать в более глубокие области каждой из перечисленных дисциплин.

В ходе работы над заданиями нет каких-либо ограничений на используемые инструментарий (сканеры, отладчики, специальные пакеты программ и т.п.) и подходы (техники).

Невозможно «уметь» решать практические задачи по всем направлениям соревнований CTF, поэтому выбирают 3–4 наиболее интересных и понятных направления, и начинают получение и развитие практических навыков, развитие умения анализировать, исследовать и работать в команде с другими людьми. В процессе поиска информации в интернете, большая ее часть — не очень полезна для решения,

но откладывается в голове на будущее. Чтобы успешно научиться решать задачи в формате CTF и извлекать из нее уроки, необходимо задействовать множество дополнительных областей знаний из разных разделов информатики.

На рис. 2 представлена модель организации соревнований в формате CTF.

Для организации соревнований в формате CTF необходима программная платформа, позволяющая запускать одновременно несколько взаимодействующих между собой приложений. На самом абстрактном уровне архитектура представлена на рис. 3.

Персональным местом участника CTF-соревнования является рабочая станция с развёрнутой операционной системой. Над операционной системой, как правило, надстраивается средство виртуализации с программным контейнером. Программный контейнер в свою очередь уже содержит графическую оболочку с формой для регистрации, набором заданий, а также специальной формой для вставки ответов в виде цифровой последовательности, называемой флагом. Как правило, программные



Рис. 2. Модель организации соревнований в формате CTF



Рис. 3. Архитектурные слои CTF-платформы

платформы для организации соревнований сами по себе не являются полигоном для решения задач. Платформы служат интерфейсом управления процессом соревнований, неким связующим звеном между организаторами и участниками.

Основные функции CTF-платформ:

- регистрация отдельных участников или команд;
- размещение текста заданий и дополнительной информации;
- размещение объявлений и подсказок;
- проверка флагов;
- подсчёт командных очков;
- составление таблицы рейтинга в реальном времени.

Опишем схематично общий принцип построения соревнований CTF (рис. 4). Участники соревнований могут быть как отдельными игроками, так и командами. Они взаимодействуют как с CTF-платформой, так и с vulnbox. На CTF-платформе участники проходят регистрацию, получают задания и подсказки, а также вставляют флаги для

получения очков. Основные действия, связанные с демонстрацией практических навыков, выполняются учащимися на vulnbox. Перечень заданий определяет модели цифровых навыков кибербезопасности.

CTF предполагает знание большого объёма информации на тему компьютерной/информационной безопасности. Являясь командной игрой, Capture the Flag развивает умение работать в команде, прислушиваться к мнению товарищей. Различные методы защиты, атаки, шифрование и дешифровка, маскировка данных, программирование и т.д. — все эти темы будут познаваться по ходу игры и подготовки к ней. И это действительно похоже на игру, хотя знания, полученные в ходе подготовки, применимы к реальным задачам, позволяют ускоренно формировать цифровые компетенции участников для завершения полного цикла образования.

Чтобы организовать соревнование в формате CTF для школьников необходимо обратить внимание на четкую организацию — залог его качества

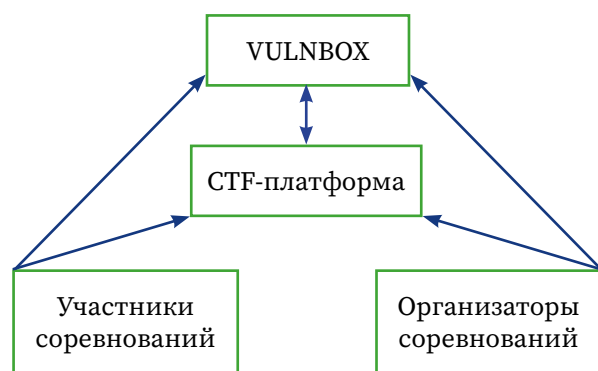


Рис. 4. Общая модель CTF-соревнований

и эффективности. Необходимо определить цели и задачи соревнования, разработать критерии оценок, создать условия проведения, обозначить время начала соревнований и примерное время окончания (на выполнения заданий соревнований было отведено 90 минут), обозначить критерии оценивания, как будут подводиться итоги мероприятия и награждения победителей. В основном мы разрабатывали 5–6 заданий, с учетом возраста учеников.

Задания в формате CTF должны быть им понятны и интересны, раскрывать ит-компетенции. На каждом задании должна быть указана сложность и количество баллов за ответ. За более простые решения должны присваиваться меньшее количество баллов. Проверку выполненных заданий рекомендуется проводить в автоматическом режиме, так как с помощью компьютера легче учитывать объективно скорость выполнения. Команда учителей ГБОУ «Школа № 1584» разработала сводную систему автоматизированной проверки ответов участников соревнований CTF. Сводная таблица должна находиться в общей видимости, чтобы участники видели результаты других команд. На рис. 5 представлена сводная таблица.

Обобщая выше сказанное, для организации соревнований CTF необходимо следовать определенным методическим рекомендациям:

1. Определить цели и задачи соревнования. Определить, какие навыки должны быть проверены у участников соревнований, какие задачи

будут предложены и какой уровень сложности они будут иметь.

2. Разработать задачи, которые будут предложены участникам. Задачи должны быть интересными, актуальными, иметь разный уровень сложности. Обязательно протестировать задачи.
3. Определить формат соревнований: очный, онлайн, офлайн, индивидуальный, командный. Определить продолжительность соревнования.
4. Подготовить инфраструктуру для проведения соревнования в формате CTF: сервер, рабочие станции, виртуальную машину, сеть, программное обеспечение, программу автоматизированной проверки результатов соревнования.
5. Подготовить правила соревнования, которые будут ясны и понятны всем участникам.
6. Подготовить наградные материалы для победителей и участников соревнований.
7. Провести тестирование инфраструктуры, чтобы убедиться, что все работает.

№	Название команды	Кол-во баллов
1	RedTeam	20
2	BlueTeam	18
3	GreenTeam	14
4	Yellow	11
5	WhiteTeam	2
6	DarkTeam	1
7	BlackTeam	1

Рис. 5. Сводная автоматизированная система проверки ответов в формате CTF, разработанная учителями ГБОУ Школа № 1584

8. Провести соревнования в соответствии с правилами и задачами, которые были разработаны.
9. Провести анализ результатов соревнования для выявления победителей и призеров.
10. Наградить победителей и призеров.

Следуя этим методическим рекомендациям, можно успешно организовать соревнования STF и проверить знания и навыки у школьников, изучающих основы информационной безопасности.

В ходе планомерной работы в течении 2022–2023 уч.г. учителя ГБОУ «Школа № 1584» пришли к выводу, что важный аспект формирования среды инженерного IT-образования — организация системы непрерывного научно-практического образования на всех уровнях школьного образования с подготовкой к обучению на специальностях вузов технического и информационно-технологического профилей. Главной целью обучения становится не освоение некоторого определенного объема информации, а деятельностное развитие обучающегося с использованием активных методов обучения, в частности, в организации соревнований по информационной безопасности в формате STF.

В данном контексте целесообразно привести мнение И.И. Калины, который считает, «что функционирование любой образовательной системы должно быть подчинено цели — обеспечение высокого качества образования. В настоящее время качество образования включает в себя качество образовательного процесса и качество образовательных результатов».

В проекте городского проекта «ИТ-Вертикаль» на базе ГБОУ «Школа № 1584» мы стремимся к достижению этих условий. Для оценки эффективности разработанной методики в рамках курса внеурочной деятельности проводились соревнования в формате STF для учащихся «ИТ-вертикали» ГБОУ «Школа № 1584», для школ округа, для школ города Москвы.

Результаты соревнований на базе ГБОУ «Школа № 1584» для учащихся школ города Москвы: 1, 3 место учащиеся экспериментальной группы ГБОУ Школы № 1584.

Результаты соревнований STF на базе МИРЭА: учащиеся экспериментальной группы ГБОУ «Школа № 1584» заняли 2 место (22.04.2023).

Представляем результаты выполнения целевых показателей в среде проекта «ИТ-Вертикаль» ГБОУ «Школа № 1584».

Независимая оценка знаний учащихся проекта «ИТ-Вертикаль» ГБОУ «Школа № 1584» в формате МЦКО по информатике в 2023 уч.г. составила 82%,



**Рис. 6.** Соревнований STF на базе ГБОУ «Школа № 1584» для учащихся информационно-технологического профиля

что отображает высокий уровень подготовки учащихся по информатике и информационным технологиям.

Результаты московского мероприятия по информационным технологиям «IT-Марафон» как выполнение целевых показателей проекта «IT-Вертикаль» ГБОУ «Школа № 1584»: 7 победителей из 9 участников.

В рамках эффективной реализации проекта «IT-Вертикаль» учителя информатики ГБОУ «Школа № 1584» прошли сертификацию на базе Центра независимой оценки и сертификации профессиональной деятельности педагогических работников и управленческих кадров Москвы: 4 учителя из 5.

Все учителя информатики ГБОУ «Школа № 1584» прошли курсы повышения квалификации в области информационных технологий для проекта «IT-Вертикаль».

75% учащихся экспериментального класса «IT-Вертикаль» для прохождения дополнительного обучения информационным технологиям с 11.01.2023-20.02.2023 уч.г. на базе Проектного центра «Детский технопарк» ФГБОУ ВО РГСУ по выбранным направлениям: графический дизайн, разработка виртуальной и дополненной реальности, 3D-моделирование, инженерный дизайн CAD.

Два учителя информатики ГБОУ «Школа № 1584» И.В. Кулавский и Т.А. Викторова стали победителями конференции «Наука для жизни. Многообразие наук-2023 г.» в секции



*Рис. 7. Соревнований STF на базе ГБОУ «Школа № 1584» для учащихся информационно-технологического профиля*

для педагогических работников с целью демонстрации опыта организации направления в формате STF на базе ГБОУ «Школа № 1584» для классов проекта информационно-технологического профиля.

Считаем, что учителя московских школ должны активно разрабатывать и внедрять в учебный процесс современные методы, формы, технологии обучения и участвовать в конференциях для обмена опытом с целью установления сотрудничества с другими педагогами-единомышленниками, администраторами, учеными и экспертами в образовательной сфере. Это позволит педагогам быть в курсе последних тенденций в педагогике и применять передовые технологии в своей работе.

### **Список литературы**

1. Бочаров М.И., Симонова И.В. Методика обучения информационной безопасности старшеклассников // Пространство и Время. 2013. № 4(14). С. 237–244.

2. Калина И.И. Высокоэффективная образовательная система: основания и признаки // Электронный ресурс: <https://cyberleninka.ru/article/n/vysokoeffektivnaya-obrazovatel'naya-sistema-osnovaniya-i-priznaki/viewer>

3. Лапина М.А. и др. Ctf – соревнования, как технология ускоренного формирования цифровых компетенций в области информационной безопасности // Дистанционные образовательные технологии. Сборник трудов VI Международной науч-

но-практической конференции. Симферополь, 2021. С. 376–377.

4. Данильчук Е.В., Лукичева А.В., Касьянов С.Н. Методические особенности формирования понятия «Информационная безопасность» на разных этапах обучения информатике в школе. Электронный ресурс: <file:///C:/Users/admin/Downloads/metodicheskie-osobennosti-formirovaniya-ponyatiya-informatsionnaya-bezopasnost-na-raznyh-etapah-obucheniya-informatike-v-shkole.pdf>



*«Хочется выразить особую благодарность за организацию и проведение столь значимой для учителей научно-практической конференции «Наука для жизни» по направлению «Многообразие науки» на базе МГТУ «СТАНКИН».*

*Площадка МГТУ «СТАНКИН» стала для московских учителей местом обмена опытом, дискуссиями, укрепления научных связей – центром педагогической мысли и идей.*

*На следующий год учителя ГБОУ Школа № 1584 обязательно планируют участвовать в этой конференции снова, но уже в большем количестве и не только по информатике».*

*И.В. Кулавский,  
учитель информатики ГБОУ «Школа № 1584»,*

*Т.А. Викторова,  
учитель информатики ГБОУ «Школа № 1584»*