УДК 378.14
В. В. Васькевич
г. Гомель, ГГУ имени Ф. Скорины

ВЛИЯНИЕ СОРЕВНОВАТЕЛЬНЫХ МЕХАНИК НА МОТИВАЦИЮ К САМОРАЗВИТИЮ БУДУЩИХ СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Современные киберугрозы характеризуются экспоненциальным ростом сложности атак. Согласно отчетам ведущих компаний в сфере информационной безопасности, время между публикацией информации об уязвимости и появлением первых эксплойтов сокращается, что требует от специалистов мгновенной реакции и глубокого понимания внутренних механизмов защищаемых систем. В этих условиях классическая система высшего образования, опирающаяся на утвержденные учебные планы, сталкивается с проблемой инерции: программы не всегда успевают обновляться с той же скоростью, с которой меняются технологии. Это порождает разрыв между теоретической подготовкой студентов и требованиями рынка труда. Работодатели ищут специалистов, обладающих не только дипломом, но и практическими навыками в области используемых средств защиты, а также навыком непрерывного самообучения. Наиболее эффективным инструментом стимулировать внутреннюю мотивацию студентов, становятся привлечение их к соревнованиям формата CTF (Capture The Flag).

CTF в контексте кибербезопасности – это командные или индивидуальные соревнования, в которых участники решают прикладные задачи по защите и взлому информационных систем. Участие в CTF-соревнованиях позволяет студентам перевести теоретические знания в плоскость реальных задач, с которыми ежедневно сталкиваются специалисты по защите информации [1–3]. В ходе турниров участники на практике осваивают такие сложные дисциплины, как реверс-инжиниринг, криптография, форензика и поиск веб-уязвимостей, работая в условиях, максимально приближенных к «боевым». Это развивает исследовательский азарт и нестандартное мышление, обучая студентов не просто следовать инструкциям, а понимать логику злоумышленника и быстро находить эффективные способы закрытия брешей в защите. Помимо технической подготовки, CTF являются мощным инструментом для карьерного старта и развития гибких навыков в области информационной безопасности. Многие крупные ИТ-компании и государственные структуры используют такие площадки для поиска талантливых кадров, предлагая лучшим игрокам стажировки прямо во время финалов. Командный формат соревнований учит студентов эффективно взаимодействовать в группе, распределять зоны ответственности и сохранять продуктивность в условиях жесткого дефицита времени. Более того, участие в подобных играх способствует формированию профессионального сообщества и непрерывному обновлению знаний в условиях стремительно меняющегося типа угроз. Поскольку задания CTF часто основаны на анализе свежих уязвимостей и актуальных векторов атак, студенты получают доступ к современным методам взлома и защиты гораздо раньше, чем те попадают в академические учебники. Это прививает привычку к постоянному самообразованию и позволяет будущему специалисту всегда оставаться на острие технологий, что критически важно в динамичной сфере кибербезопасности, где стагнация знаний равносильна потере квалификации.

В основе соревнований CTF лежит принцип геймификации – внедрения игровых механик в неигровые процессы. Для студентов специальности «Кибербезопасность» конкуренция выполняет функцию мощного психолого-педагогического драйвера.

CTF-соревнования создают уникальную образовательную среду, где процесс обучения происходит через игровые и конкурентные механики. Можно выделить три ключевых аспекта влияния соревнований на саморазвитие студентов:

1. Быстрая обратная связь. В отличие от экзамена, результат в CTF виден сразу.

Получение «флага» вызывает эмоции, закрепляя положительную ассоциацию с решением сложных задач. Это поддерживает интерес даже при изучении рутинных тем (анализ логов, изучение спецификаций протоколов).

2. Конкуренция как драйвер роста. Наличие динамической, постоянно меняющейся таблицы результатов в рамках соревнования пробуждает дух соперничества. Видя успехи других команд или участников, студент стремится сократить разрыв в знаниях. Это побуждает его самостоятельно осваивать новые инструменты, которые еще не рассматривались на лекциях.

3. Широкий спектр компетенций. CTF охватывает разнообразные категории: Web, Crypto, Pwn, Reverse, Forensics, OSINT. Чтобы быть конкурентоспособным, студент вынужден выходить из зоны комфорта своей узкой специализации, становясь специалистом с широким кругозором.

В рамках работы был проведен анализ профессионального развития студентов, принимавших активное участие в CTF-движении в течение 2024-2026 годов. В декабре 2024 года два студента 3 курса специальности «Компьютерная безопасность» приняли участие в кибер-тренировке по оценке эффективности защищенности объектов информационной инфраструктуры от кибератак на базе специализированного киберполигона «Национального центра обеспечения кибербезопасности и реагирования на киберинциденты». Студенты получили опыт позволивший им проанализировать свои знания и выделить приоритетные области дальнейшего саморазвития. В августе-сентябре 2025 года шесть студентов 4 курса приняли участие в отраслевых соревнованиях по информационной безопасности «Consyst-CTF» и «Студ-ИТ» проводимых при поддержке корпорации «Росатом».

Рисунок 1 – Студенты 4 курса дневной формы обучения с руководителем

В ноябре 2025 года уже более 15 студентов 2, 3 и 4 курсов специальностей «Компьютерная безопасность» и «Кибербезопасность» приняли участие в первом республиканском турнире по кибербезопасности «BSUIR:CTF» который проходил в 2 этапа: первый в онлайн-формате и второй с очным присутствием 20 лучших в личном

зачете участников. По результатам первого этапа четверо студентов перешли во второй этап и отправились в Белорусский государственный университет информатики и радиоэлектроники для участия в финале турнире. По результатам турнира студенты заняли с 6 по 9 место и были награждены сертификатами (рисунок 1).

На примере студентов специальностей «Компьютерная безопасность» и «Кибербезопасность» наблюдается корреляция между участием в CTF и профессиональной успеваемостью. Участники соревнований демонстрируют более глубокое понимание архитектуры систем и быстрее находят нестандартные решения проблем. Более того, конкурентная среда учит работать в стрессовых ситуациях и в условиях ограниченного времени, что имитирует реагирование на реальные инциденты информационной безопасности.

Студенты, регулярно участвующие в CTF-турнирах по сравнению со студентами, обучающиеся только по стандартной программе намного больше стали проявлять интерес к специализированным дисциплинам. Студенты, вовлеченные в CTF-движение, демонстрируют более высокий уровень мотивации к саморазвитию, обладают широким техническим кругозором и быстрее адаптируются к профессиональной деятельности. В связи с этим, вузам рекомендуется не просто поддерживать участие студентов в турнирах, но и интегрировать элементы CTF, например лабораторные работы в формате «Task-based challenges» в основные образовательные курсы. Это позволит выпускать специалистов, готовых к реальным вызовам современной кибербезопасности.

Литература

1. Что такое CTF и зачем это нужно? // Хабр [Электронный ресурс]. – 2023. – Режим доступа: https://habr.com/ru/companies/gaz-is/articles/777912/. – Дата доступа: 27.01.2026.
2. What is Capture the Flag (CTF) in Cybersecurity? // EC-Council [Electronic resource]. – Mode of access: https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/capture-the-flag-ctf-cybersecurity/. – Дата доступа: 27.01.2026.
3. Что такое CTF (Capture the Flag) в кибербезопасности // Блог Skillfactory [Электронный ресурс]. – Режим доступа: https://blog.skillfactory.ru/capture-the-flag-ctf-v-kiberbezopasnosti/. – Дата доступа: 27.01.2026.