УДК 004.05

Дьяконов В.С.,
старший инженер отдела кибербезопасности ПАО «Сбербанк»
Россия, г. Барнаул
Шишкин Н.Д., старший инженер отдела кибербезопасности ПАО «Сбербанк»
Россия, г. Барнаул
Саповатова В.Ю.,
преподаватель
СПО, ФГБОУ ВО «Алтайский государственный университет», Колледж
Россия, г. Барнаул
Деева К.С.,
студент
1 курс, факультет «Информационных технологий»
Алтайский Государственный Технический Университет им. И.И. Ползунова
Россия, г. Барнаул
Научный руководитель Шарлаев Е.В.,
кандидат технических наук, доцент кафедры ИВТиИБ Алтайский Государственный Технический Университет им. И.И. Ползунова
Россия, г. Барнаул

ОТ CTF К ПРОФЕССИИ: КАК ИГРОВЫЕ ДИСЦИПЛИНЫ ФОРМИРУЮТ СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация: *Статья посвящена анализу взаимосвязи между соревнованиями Capture The Flag (CTF) и профессиональными ролями в сфере информационной безопасности. В работе рассматривается эволюция ИБ от*

монолитной дисциплины к экосистеме узких специализаций, систематизируются основные направления CTF-соревнований и проводится детальное сопоставление игровых компетенций с реальными профессиональными задачами. Автор демонстрирует, что CTF выступает не просто развлекательным мероприятием, а эффективным тренировочным полигоном, где навыки, отрабатываемые в игровой среде, напрямую транслируются в практические умения, востребованные в таких областях, как пентест, анализ инцидентов, криминалистика, threat intelligence и безопасность приложений. Статья обосновывает необходимость включения CTF-ориентированного подхода в системы профессиональной подготовки и оценки компетенций специалистов по информационной безопасности.

Ключевые слова: *информационная безопасность, Capture The Flag, CTF, профессиональные компетенции, пентест, кибербезопасность, образовательные технологии, специализации ИБ.*

Annotation: *The article is devoted to the analysis of the relationship between Capture The Flag (CTF) competitions and professional roles in the field of information security. The paper examines the evolution of information security from a monolithic discipline to an ecosystem of specialized areas, systematizes the main CTF categories, and provides a detailed mapping of game competencies to real professional tasks. The author demonstrates that CTF is not merely entertainment but an effective training ground where skills honed in a gaming environment directly translate into practical abilities demanded in areas such as penetration testing, incident analysis, forensics, threat intelligence, and application security. The article substantiates the necessity of incorporating CTF-oriented approaches into professional training and competence assessment systems for information security specialists.*

Key words: *information security, Capture The Flag, CTF, professional competencies, penetration testing, cybersecurity, educational technologies, information security specializations.*

Информационная безопасность за последние десятилетия трансформировалась из узкоспециализированной технической дисциплины в сложную, многослойную экосистему профессиональных ролей и направлений. Сегодня невозможно представить себе «универсального специалиста по безопасности» — каждый аспект защиты информации требует глубоких знаний в своей области: от сетевых протоколов до человеческой психологии, от криптографических алгоритмов до облачных архитектур.

Параллельно с этим развивалась уникальная культура практического обучения, ключевым элементом которой стали соревнования Capture The Flag (CTF). То, что начиналось как неформальные состязания энтузиастов, превратилось в международное движение, объединяющее тысячи участников по всему миру и признанное эффективным инструментом подготовки ИБ-специалистов. CTF предлагает не просто теорию — это симуляция реальных атак и защитных сценариев, где каждый участник может столкнуться с вызовами, максимально приближенными к повседневной работе профессионала.

Современный ландшафт информационной безопасности представляет собой разветвлённую систему специализаций, каждая из которых решает конкретную задачу в общем контуре защиты организации. Сетевая безопасность занимается защитой инфраструктуры передачи данных — межсетевые экраны, системы обнаружения вторжений, VPN и сегментация сетей остаются фундаментом корпоративной защиты. Безопасность приложений смещает фокус на жизненный цикл разработки: статический и динамический анализ кода, безопасная разработка, проверка зависимостей и интеграция безопасности в DevOps-процессы.

Конечные точки — ноутбуки, серверы, мобильные устройства — защищаются средствами класса EDR и NGAV, тогда как безопасность данных сосредоточена на шифровании, маскировании и предотвращении утечек через DLP-системы. Управление идентификацией и доступом (IAM) решает

фундаментальную задачу аутентификации и авторизации, внедряя многофакторную аутентификацию, единый вход и контроль привилегированных учётных записей.

Облачная безопасность приобретает всё большее значение в связи с миграцией бизнеса в AWS, Azure и GCP, требуя понимания модели общей ответственности и специфических инструментов защиты рабочих нагрузок. На операционном уровне Security Operations Centre (SOC) ведёт непрерывный мониторинг, анализ и реагирование на инциденты с использованием SIEM и SOAR-платформ. Отдельного внимания заслуживают критическая информационная инфраструктура и АСУ ТП, где безопасность ставит во главу угла доступность и физическую целостность систем, а не конфиденциальность — и где устаревшие протоколы и оборудование создают уникальные вызовы.

Стратегические функции выполняет GRC — управление рисками, аудит и соответствие регуляторным требованиям, связывающие техническую безопасность с бизнес-целями. Криптография остаётся фундаментальной наукой, обеспечивающей все современные механизмы защиты, а threat intelligence занимается проактивным сбором информации о тактиках и процедурах киберпреступников. Наконец, наступательная безопасность — пентест и Red Teaming — представляет собой активную проверку защитных механизмов через моделирование действий реальных злоумышленников.

Capture The Flag представляет собой не единую дисциплину, а целый спектр направлений, каждое из которых требует специфических навыков и инструментов. Reverse Engineering — анализ исполняемых файлов без исходного кода — учит читать ассемблер, работать с дизассемблерами (IDA Pro, Ghidra) и понимать логику скомпилированных программ. Эта дисциплина напрямую готовит специалистов к анализу вредоносного ПО и поиску уязвимостей в проприетарном коде.

Pwn — эксплуатация уязвимостей бинарных приложений — погружает в архитектуру памяти программ, стек, кучу и защитные механизмы вроде

ASLR и DEP. Участники учатся писать шелл-код, строить ROP-цепочки и преодолевать современные средства защиты. Web-категория охватывает всё многообразие уязвимостей веб-приложений — от классических SQL-инъекций и XSS до серверного шаблонного инжиниринга и небезопасной десериализации, формируя навыки, критически важные для специалистов по AppSec и пентестеров.

Криптографические задачи требуют понимания математических основ шифрования и умения находить слабости в реализациях алгоритмов — от классических шифров до современных RSA и AES. Forensics учит анализировать цифровые артефакты: файловые системы, сетевой трафик, дампы памяти, скрытые данные в изображениях и документах. OSINT развивает навыки сбора информации из публичных источников — поисковые системы, социальные сети, архивы интернета. Категория Misc объединяет задачи на смекалку и программирование, формируя гибкость мышления и умение быстро осваивать новые технологии.

Между профессиональными ролями в ИБ и направлениями CTF существует прямая и очевидная корреляция. Пентестер и специалист Red Team ежедневно занимаются тем же, чем в CTF занимаются в категориях Pwn, Web и Reverse Engineering — поиском и эксплуатацией уязвимостей. Аналитик SOC, работающий с инцидентами, использует весь спектр навыков Forensics для анализа логов, трафика и дампов памяти, а также должен понимать векторы атак, отрабатываемые в Web и Cryptography.

Специалист по безопасности приложений применяет знания из Web и Reverse для анализа кода и поиска уязвимостей на этапе разработки. Криптограф работает на стыке своей специализации и CTF-криптографии — поиск слабостей в алгоритмах и их реализациях составляет суть обеих дисциплин. Цифровой криминалист опирается на Forensics и OSINT для расследования инцидентов и извлечения улик. Инженер по безопасности сетей получает в CTF глубокое понимание сетевых атак через анализ трафика.

Аналитик Threat Intelligence использует OSINT для сбора информации об угрозах и Reverse Engineering для анализа вредоносного ПО.

Примечательно, что даже для стратегических ролей — GRC-менеджеров и аудиторов — понимание технической сути задач из разных CTF-категорий позволяет более эффективно оценивать риски и выстраивать процессы защиты, общаясь с техническими специалистами на одном языке. Таким образом, CTF выступает универсальным полигоном, формирующим компетенции для всех уровней ИБ-профессий.

Проведённый анализ демонстрирует глубокую и неразрывную связь между профессиональными ролями в информационной безопасности и дисциплинами CTF-соревнований. CTF выступает не просто увлечением, но мощным инструментом профессионального развития, позволяющим в контролируемой и безопасной среде отрабатывать критически важные навыки — от взлома приложений и расследования инцидентов до анализа угроз и криптоанализа.

Понимание этой взаимосвязи даёт будущим специалистам возможность осознанно строить карьерную траекторию, выбирая для углублённого изучения те направления CTF, которые наиболее точно соответствуют выбранной профессиональной роли. Для работодателей участие кандидатов в CTF становится объективным индикатором практических компетенций, недостижимым при традиционном образовании. Именно на пересечении игры и реальной работы, теории и практики формируется новое поколение специалистов, способных эффективно противостоять современным киберугрозам в условиях постоянно меняющегося ландшафта атак.

Использованные источники:

1. CTF в кибербезопасности: все, что нужно знать об игре Capture the flag // Startx URL: https://startx.team/blog/statyi/capture-the-flag-v-

kiberbezopasnosti/https://startx.team/blog/statyi/capture-the-flag-v-kiberbezopasnosti/ (дата обращения: 06.07.2026).

2. Матрица профессий в ИБ: исчерпывающий гид по карьере в кибербезопасности // securitylab URL: https://www.securitylab.ru/analytics/559147.php (дата обращения: 07.07.2026).

3. С чего начать и как стать практикующим специалистом по информационной безопасности в конце 2025 года // habr URL: https://habr.com/ru/articles/953350/ (дата обращения: 07.07.2026).