Анализ категорий задач и профессиональных компетенций участников в соревнованиях Capture The Flag (CTF) по информационной безопасности

М.Н. Юсупов, Т.В. Хоменко, Г.А. Попов

Астраханский государственный технический университет, Астрахань, Россия

Аннотация **– Представлен всесторонний анализ категорий задач, используемых в соревнованиях Capture The Flag (CTF), а также рассматриваются профессиональные компетенции, необходимые участникам для их решения. Особое внимание уделяется критериям выбора задач, соответствию актуальным угрозам информационной безопасности, а также этическим и техническим аспектам проведения CTF. Статья демонстрирует, как различные категории задач способствуют развитию профессиональных навыков, необходимых для карьеры в сфере информационной безопасности, и подчеркивает важность сбалансированного и актуального наполнения задач для повышения эффективности образовательных и профессиональных программ.**

Ключевые слова **– Capture The Flag, информационная безопасность, категории задач, профессиональные компетенции, выбор задач, технические навыки, этика, квалификация специалистов.**

I. ВВЕДЕНИЕ

Современные соревнования Capture The Flag (CTF) выступают как мощный инструмент формирования и оценки профессиональных компетенций в области информационной безопасности. Одним из ключевых элементов таких соревнований является разнообразие задач, которые позволяют выявить уровень знаний, аналитические способности и креативность участников. Правильный подбор и формулировка задач способствуют развитию необходимых навыков и стимулируют интерес к профессиональному росту. В данной статье рассматриваются основные категории задач, используемые в CTF, а также критерии их выбора и соответствующие профессиональные компетенции, что позволяет понять, как данный формат способствует подготовке компетентных специалистов [1, 2].

II. ОБЗОР И АНАЛИЗ КАТЕГОРИЙ ЗАДАЧ

В рамках проведения CTF-соревнований выделяют несколько ключевых категорий задач, каждая из которых направлена на развитие определенных навыков и знаний у участников. Ниже подробно рассмотрены основные категории [3].

1. Веб-безопасность

Задачи, связанные с анализом веб-приложений и серверных конфигураций, обнаружением уязвимостей, SQL-инъекций, межсайтовых скриптовых атак (XSS) и др. Веб-приложения — одна из наиболее распространенных целей атак, поэтому умение выявлять и устранять уязвимости в них является критически важным навыком для специалиста по информационной безопасности.

2. Реверс-инжиниринг

Задачи на анализ бинарных файлов, декомпиляцию, понимание внутренней структуры программных продуктов, выявление скрытых функций и флагов. Позволяет участникам понять внутренние механизмы программ, что важно для обнаружения уязвимостей и анализа вредоносных программ.

3. Криптография

Задачи, связанные с расшифровкой сообщений, криптоанализом, использованием алгоритмов шифрования и их взломом. Обеспечение конфиденциальности данных — краеугольный камень информационной безопасности; навыки работы с криптографическими протоколами востребованы у специалистов.

4. Форензика

Анализ дампов памяти, сетевых трафиков, восстановление удаленных данных, расследование инцидентов. Необходимость быстрого реагирования и расследования киберинцидентов делает данный тип задач ключевым для специалистов по инцидент-менеджменту.

5. Стеганография

Обнаружение скрытых сообщений и данных в изображениях, аудиофайлах, текстах и др. Умение находить скрытые данные важно как для защиты информации, так и для проведения разведывательных операций.

6. Эксплуатация уязвимостей

Задачи на поиск, разработку и применение эксплойтов, а также создание автоматизированных средств атаки. Это фундаментальные навыки для оценки уязвимостей систем и разработки методов защиты.

7. Пентестинг (проверка на проникновение)

Проведение моделируемых атак на системы и сети, подготовка отчетов о результатах. Позволяет участникам понять слабые места систем и научиться их устранять.

8. OSINT (Open Source Intelligence)

Исследование открытых источников информации для сбора данных и анализа. Навыки работы с публичными источниками необходимы для разведки и оценки угроз.

9. MISC (разные задачи)

Задачи, не входящие в другие категории, например, анализ логов, социальная инженерия и др. Разностороннее развитие навыков и подготовка к нестандартным ситуациям.

10. Безопасность ОС

Задачи, связанные с анализом защиты операционных систем, выявлением уязвимостей и их устранением. Ключевые навыки для специалистов по защите инфраструктуры.

Проведение задач разного типа требует от участников наличия определенных профессиональных компетенций. Согласно Приказу Минобрнауки РФ № 1515 от 01.12.2016 [4], выделяют следующие компетенции и соответствующие им навыки (см. Табл. 1):

1. Криптография

Задачи на расшифровку зашифрованных сообщений, криптоанализ, реализация и взлом шифров.

Необходимые профессиональные компетенции:

- Способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1).
- Способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2).
- Способность принимать участие в проведении экспериментальных исследований системы защиты информации (ПК-12).

2. Социальная инженерия

Задачи на умение вести себя с мошенниками, манипулирование, и так далее.

Необходимые профессиональные компетенции:

- Способность организовывать работу малого коллектива исполнителей в профессиональной деятельности (ПК-14).

3. WEB-безопасность

Задачи на защиту WEB-сервисов от атак, анализ WEB-сервисов, и так далее.

Необходимые профессиональные компетенции:

- Способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2).
- Способность принимать участие в проведении экспериментальных исследований системы защиты информации (ПК-12).

4. Форензика

Задачи на анализ дампов памяти, сетевых трафиков, восстановление удаленных данных, а также расследование инцидентов.

Необходимые профессиональные компетенции:

- Способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2).
- Способность принимать участие в проведении экспериментальных исследований системы защиты информации (ПК-12).
- Способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений (ПК-7).

5. Стеганография

Задачи на поиск скрытых данных в изображениях, аудиофайлах, текстах и так далее. Необходимые профессиональные компетенции:

- Способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю (ПК-15).

6. OSINT

Задачи на исследование открытых источников информации. Необходимые профессиональные компетенции:

- Способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений (ПК-7).

7. MISC

Задачи не похожие не на один из других разделов задач. Необходимые профессиональные компетенции:

- Способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений (ПК-7).

8. Безопасность ОС

Задачи, связанные с защитой операционной системы, анализа ОС, и так далее.

Необходимые профессиональные компетенции:

- Способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2).
- Способность принимать участие в проведении экспериментальных исследований системы защиты информации (ПК-12).

ТАБЛИЦА I
РАЗДЕЛ И СООТВЕТСТВУЮЩАЯ КОМПЕТЕНЦИЯ

Раздел	Требуемые профессиональные компетенции
Исследование открытых источников (OSINT)	Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений (ПК-7).
Разное (MISC)	Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений (ПК-7).
Скрытая передача информации (стеганография)	Способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю (ПК-15).
Безопасность ОС	Способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2). Способность принимать участие в проведении экспериментальных исследований системы защиты информации (ПК-12).
Криптография	Способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1).

Данные категории задач, а также соответствующие профессиональные компетенции для их решения демонстрируют, как CTF-соревнования способствуют развитию различных навыков, необходимых для профессиональной карьеры в области информационной безопасности.

Изучим различные критерии выбора задач для CTF-соревнований, которые определяются следующими факторами:

1. Соответствие актуальным угрозам ИБ

Задачи должны отражать актуальные угрозы, с которыми сталкиваются различные организации и пользователи.

2. Оценка профессиональных навыков

Задачи должны обеспечивать проверку профессиональных навыков, необходимых для профессионалов в области ИБ.

3. Баланс сложности заданий

Задачи должны быть сбалансированы по уровню сложности, для участия, как новичков, так и опытных специалистов в области ИБ.

4. Инновационность и интерес

Задачи должны быть интересными, чтобы участники соревнований были мотивированы их решать.

Для составления заданий для различных CTF-соревнований необходимо учитывать следующие факторы:

1. Этичность и легальность

Задачи должны быть этичными и легальными, то есть не провоцировать участников соревнований на незаконные действия с их стороны. Необходимо избегать задачи, которые могут быть связаны как призыв к нарушению законодательства.

2. Техническая сложность

Задачи должны быть технически сложными, но выполнимыми, чтобы мотивировать участников соревнований к развитию своих профессиональных навыков. Необходимо обеспечивать возможность проверки решений и корректности выполнения данных задач.

3. Образовательная ценность

Задачи должны иметь образовательную ценность, а именно помогать участникам соревнований улучшить свои навыки и знания в области информационной безопасности. Адекватно спроектированные задачи включают аспекты обучения и практического применения теоретических знаний в области ИБ.

Рассмотрим пример задачи для CTF и соответствующую профессиональную компетенцию, необходимую для решения данной задачи:

- Раздел – социальная инженерия.
- Трудоемкость решения задачи – низкая.
- Формат ответа на задание – выбор из нескольких вариантов.
- Способ проверки – автоматическая проверка.

Условие задачи: Вы получили сообщение в социальных сетях от незнакомца, который утверждает, что он из популярного бренда одежды. Они предлагают вам эксклюзивную скидку на их продукцию, если вы перейдете по ссылке и

предоставите свою электронную почту и номер телефона.

Варианты ответа: 1) Перейдите по ссылке и предоставьте свои данные. 2) Проверьте подлинность бренда, связавшись с ними по официальным каналам. 3) Сообщите о сообщении как о фишинге. 4)Удалите сообщение и заблокируйте отправителя.

Правильный ответ: 2.

Для решения данной задачи необходима профессиональная компетенция (ПК-14), а именно - способность организовывать работу малого коллектива исполнителей в профессиональной деятельности.

III. Выводы и заключение

Таким образом, анализ задач в различных CTF-соревнованиях показывает, что они охватывают большинство актуальных тем и угроз в области информационной безопасности. Данные задачи требуют от участников соревнований технических знаний, аналитического мышления, креативности, и так далее.

Категории задач, используемые в CTF, формируют комплексный набор навыков, необходимых специалистам по информационной безопасности. Правильный подбор и баланс задач по сложности, актуальности и этическим стандартам позволяют не только проверять уровень профессиональной подготовки участников, но и стимулировать их развитие, что способствует формированию квалифицированных кадров в области ИБ. Внедрение разнообразных задач, соответствующих современным угрозам, повышает эффективность CTF как образовательного инструмента и способствует развитию профессиональных компетенций.

Литература

[1] Михалева А. Capture the Flag (CTF) в кибербезопасности: все, что нужно знать об этой игре / Анастасия Михалева // SKILLFACTORY MEDIA : URL: [https://blog.skillfactory.ru/capture-the-flag-ctf-v-kiberbezopasnosti/] (дата обращения: 03.06.2025).

[2] Григорьев А., Крюкова У. CTF в кибербезопасности: все, что нужно знать об игре Capture the flag / Григорьев А., Крюкова У // Start X: URL [https://startx.team/blog/statyi/capture-the-flag-v-kiberbezopasnosti/] (дата обращения: 06.06.2025).

[3] Лапонина О.Р., Матошенко В.А. СРАВНИТЕЛЬНЫЙ АНАЛИЗ CTF-ПЛАТФОРМ ДЛЯ ОБУЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ / Лапонина О.Р., Матошенко В.А. // CYBERLENINKA: URL [https://cyberleninka.ru/article/n/sravnitelnyy-analiz-ctf-platform-dlya-obucheniya-kiberbezopasnosti] (дата обращения: 04.06.2025).

[4] Минобрнауки РФ. Приказ № 1515 от 01.12.2016 «Об утверждении профессиональных стандартов в области информационной безопасности». — М.: Минобрнауки РФ, 2016.

Информация об авторах

Хоменко Татьяна Владимировна – д.т.н., профессор, заведующий кафедрой «Автоматизированные системы обработки информации и управления» Астраханского государственного технического университета, Астрахань, Россия, г. Астрахань, Россия, e-mail: t_v_khomenko_stud@mail.ru

Попов Георгий Александрович – д.т.н., профессор кафедры «Информационная безопасность» Астраханского государственного технического университета, г. Астрахань, Россия, e-mail: kaf_ib@astu.org

Юсупов Майербек Назарбекович – магистрант направления «Информатика и вычислительная техника» Астраханского государственного технического университета, г. Астрахань, e-mail: boss.maerbek@mail.ru

Analysis of task categories and professional competencies of participants in Capture The Flag (CTF) information security competitions

M.N. Yusupov, T.V. Khomenko, G.A. Popov

Astrakhan State Technical University, Astrakhan, Russia

***Abstract* – Presents a comprehensive analysis of the problem categories used in Capture The Flag (CTF) competitions and discusses the professional competencies required to solve them. Particular attention is paid to the criteria for choosing problems, their relevance to current information security threats, and the ethical and technical aspects of conducting CTFs. The article demonstrates how different problem categories contribute to the development of professional skills required for a career in information security and highlights the importance of balanced and relevant problem content for improving the effectiveness of educational and professional programs.**

***Keywords* – Capture The Flag, information security, task categories, professional competencies, task selection, technical skills, ethics, specialist qualifications.**

References

[1] Mikhaleva A. Capture the Flag (CTF) in cybersecurity: everything you need to know about this game / Anastasia Mikhaleva // SKILLFACTORY MEDIA: URL: [https://blog.skillfactory.ru/capture-the-flag-ctf-v-kiberbezopasnosti/] (date accessed: 06/03/2025).

[2] Grigoriev A., Kryukova U. CTF in cybersecurity: everything you need to know about the game Capture the flag / Grigoriev A., Kryukova U // Start X: URL [https://startx.team/blog/statyi/capture-the-flag-v-kiberbezopasnosti/] (date accessed: 06.06.2025).

[3] Laponina O.R., Matoshenko V.A. COMPARATIVE ANALYSIS OF CTF PLATFORMS FOR TRAINING CYBERSECURITY / Laponina O.R., Matoshenko V.A. // CYBERLENINKA: URL [https://cyberleninka.ru/article/n/sravnitelnyy-analiz-ctf-platform-dlya-obucheniya-kiberbezopasnosti] (date accessed: 04.06.2025).

[4] Ministry of Education and Science of the Russian Federation. Order No. 1515 of 01.12.2016 "On approval of professional standards in the field of information security". - M .: Ministry of Education and Science of the Russian Federation, 2016.