ОБРАЗОВАТЕЛЬНЫЙ ХАБ ДЛЯ ПОДГОТОВКИ СПЕЦИАЛИСТОВ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

Маршалова К.Ц., Биюмен Е.А., студенты гр.361401

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Белоусова Е.С. – канд. техн. наук, доцент

Аннотация. Разработана обучающая CTF-платформа в формате Point-and-Click квеста на базе движка Unity 6. Архитектура объединяет внутриигровой ролевой интерфейс и практическое решение задач в физической операционной системе (ОС) пользователя. Навигация включает локации с неигровыми персонажами (NPC) для выдачи заданий и виртуальный «хаб». Хаб представляет собой терминал, интегрирующий модули управления квестами, мониторинга глобального рейтинга (Leaderboard) и верификации CTF-флагов. Базовая механика заключается в экспорте тренировочных артефактов (PCAP-дампов, криптографических контейнеров) на реальный ПК. Обучающийся анализирует артефакты с помощью профессиональных утилит информационной безопасности, возвращая найденный флаг в клиент игры.

Ключевые слова. обучающий хаб, защита информации, геймификация, Unity, Capture The Flag, кибербезопасность, неигровые персонажи, системное администрирование, анализ артефактов.

Разрабатываемый хаб представляет собой интерактивный обучающий комплекс, реализованный в формате Point-and-Click квеста. В качестве базовой среды разработки выбран кроссплатформенный игровой движок Unity 6. Выбор 2D-перспективы продиктован необходимостью минимизации когнитивной нагрузки на пространственное ориентирование: обучающийся не тратит ресурсы на управление камерой в трехмерном пространстве, концентрируя внимание исключительно на аналитических и технических задачах. Для обеспечения высокого качества визуализации при низких системных требованиях задействован конвейер рендеринга Universal Render Pipeline (URP), позволяющий реализовать ресурсоэффективное динамическое освещение и постобработку, стилизующие интерфейс под жанр киберпанк.

Фундаментальным отличием предложенного хаба от классических образовательных симуляторов (киберполигонов) является отказ от внутренней программной эмуляции операционных систем и специализированного программного обеспечения. Платформа функционирует по гибридной модели взаимодействия. Игровой клиент берет на себя роль интерактивного распределителя задач (Task Manager), системы нарратива и контроллера прогресса, тогда как непосредственный анализ уязвимостей и работа с артефактами осуществляются на стороне физической хост-машины обучающегося (например, в среде ОС Kali Linux). Схематическое представление потоков данных в рамках гибридной архитектуры приведено на рисунке 1.

Рисунок 1 – Схема взаимодействия игрового клиента и физической операционной системы обучающегося

Программная архитектура приложения обладает высокой степенью модульности и декомпозирована на три ключевых компонента, взаимодействие между которыми реализуется через систему диспетчеризации событий UnityEvents и двумерные физические коллайдеры (Box Collider 2D).

1. Модуль пространственной навигации и генерации квестов. Игровое пространство разделено на тематические локации (галерея, библиотека, серверная и др.). Получение заданий формата Capture The Flag (CTF) интегрировано в систему ветвящихся диалогов с неигровыми персонажами (NPC). Программная логика диалоговой системы спроектирована с использованием паттерна ScriptableObjects. Данное архитектурное решение выносит данные о квестах за пределы исполняемого кода, позволяя масштабировать банк заданий, добавлять новые сценарии и корректировать тексты диалогов через инспектор Unity без необходимости перекомпиляции проекта. Подобный нарративный подход эффективно эмулирует начальные этапы аудита безопасности – социальную инженерию и сбор информации (Reconnaissance) [1].

2. Модуль экспорта артефактов и интеграции с ОС. Данный модуль является связующим звеном между игровой симуляцией и реальной практикой. При акцептовании задания от NPC скрипты платформы инициируют выгрузку тренировочного файла-артефакта. На программном уровне

используется функционал пространства имен System.IO, обеспечивающий бинарное копирование файлов (зашитых в ресурсы игры или загружаемых с удаленного сервера) в пользовательскую директорию (например, Downloads) на физическом диске компьютера. В качестве учебных артефактов могут выступать:

– дампы сетевого трафика в формате .pcap для анализа протоколов;

– бинарные исполняемые файлы (.exe, .elf) для базового реверс-инжиниринга;

– зашифрованные криптографические контейнеры и дампы оперативной памяти;

– фрагменты скомпрометированного исходного кода.

Типичный сценарий выполнения лабораторной задачи реализуется в четыре этапа. На первом этапе обучающийся получает от NPC сюжетную информацию о перехваченном сетевом трафике (легенда задания). На втором этапе игровая платформа аппаратно экспортирует файл дампа на рабочий стол игрока. На третьем этапе обучающийся сворачивает окно игры, запускает профессиональный анализатор протоколов (например, Wireshark) в своей реальной ОС, производит фильтрацию пакетов, декодирует полезную нагрузку и извлекает искомые данные. На финальном этапе полученный ответ форматируется в стандартный CTF-флаг [2].

3. Модуль виртуального хаба и рейтинговой верификации. Вектор возврата в игру осуществляется через личную комнату главного героя (виртуальный хаб). В хабе реализован интерфейс персонального компьютера (терминала), выполняющий функцию личного кабинета обучающегося. Через данный терминал студент вводит найденный флаг. Проверка валидности флага производится не путем прямого сравнения строк в коде, а через сопоставление криптографических хэш-сумм (например, алгоритмом SHA-256). Это полностью исключает возможность извлечения правильных ответов путем реверс-инжиниринга исходного кода самого образовательного хаба.

Дополнительно в виртуальном терминале интегрирована система мониторинга академического прогресса и глобальная рейтинговая таблица (Leaderboard). За каждое корректно выполненное задание системе начисляются баллы, формирующие позицию студента в рейтинге. Для поддержания объективного соревновательного баланса в платформе реализована система динамического ценообразования задач (Dynamic Scoring).

Суть данного алгоритма заключается в постепенном снижении стоимости задания пропорционально количеству обучающихся, успешно его решивших. При этом стоимость снижается не бесконечно, а лишь до установленного минимального порога, гарантирующего получение базовых баллов даже при позднем решении. Для дополнительного стимулирования соревновательной активности предусмотрен статический бонус за первоочередное решение задачи – «First Blood» (первая кровь), который не зависит от общей статистики прохождений.

Математическая модель расчета итогового количества рейтинговых баллов (R), начисляемых обучающемуся за сдачу флага, описывается следующей формулой:

$$R = \max(P_{min}, P_{max} – ((P_{max} - P_{min}) / S_{decay}) \cdot N) + FB, \quad (1)$$

где P_{max} – начальная (максимальная) стоимость задания в баллах; P_{min} – минимальный порог баллов, ниже которого стоимость задания не опускается; N – текущее количество пользователей, успешно решивших данную задачу; S_{decay} – пороговое количество решений, при достижении которого стоимость задания фиксируется на минимальном уровне; FB – статический бонус «First Blood», принимающий заданное значение строго для первого решившего и равный 0 для всех последующих.

Наличие динамической рейтинговой системы выступает критически важным фактором внутренней мотивации обучающихся. Алгоритм автоматически балансирует сложность: задачи, которые решают все, быстро теряют в «цене», в то время как действительно сложные артефакты остаются высокобалльными, объективно отражая технические компетенции лидеров таблицы.

Таким образом, интеграция подлинного инструментария аудита информационной безопасности в логику 2D-квеста позволяет трансформировать рутинный образовательный процесс в исследовательскую работу. Механика экспорта артефактов в синергии с динамическим CTF-рейтингом обеспечивает бесшовный переход от академической теории к прикладной практике системного администрирования.

Список использованных источников:

1. Геймификация в образовательном процессе подготовки специалистов по защите информации / А.А. Шелупанов [и др.] // Безопасность информационных технологий, 2021. – Т. 28. – № 2. – С. 115-125.

2. Образовательный хаб для подготовки специалистов в области защиты информации / К.Ц. Маршалова, Е.А. Биюмен // Технические средства защиты информации 2026. – С. 318–321.