УДК 004.056.5

К.В. Курносов, А.И. Пестунов, Т.М. Пестунова, Я.В. Юракова

Новосибирский государственный университет экономики и управления

КОНЦЕПЦИЯ CTF-КВЕСТА ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ СТУДЕНТОВ НЕПРОФИЛЬНЫХ СПЕЦИАЛЬНОСТЕЙ

В статье представлена концепция соревнований FinCTF – квеста по информационной безопасности для пользователей, не являющихся IT-специалистами, но активно применяющих информационные технологии при решении своих профессиональных и частных задач. В основу квеста положены задания, связанные с использованием информационных технологий, типичных для экономико-финансовой сферы. Формат игры способствует практическому освоению правил безопасной работы в ИТ-среде, развитию коммуникативных навыков, навыков принятия коллективных решений в стрессовых ситуациях и условиях ограниченного времени.

Ключевые слова: CTF, capture the flag, соревнование, FinCTF, квест, информационная безопасность, информационные технологии в экономико-финансовой сфере, формирование компетенций.

Введение

В настоящее время проблемы информационной безопасности затрагивают не только специалистов этой области, но и людей, чья профессиональная и личная жизнь напрямую не связана с IT-сферой. Работа с многочисленными электронными сервисами при несоблюдении правил информационной безопасности чревата неприятными последствиями для пользователей. В частности, выявление «подводных камней» при подписании кредитных и иных договоров за счет их внимательного прочтения, адекватная современным угрозам работа в социальных сетях, умение распознать манипуляции, осуществляемые с использованием инфокоммуникационных технологий, грамотная работа с лицензиями на ресурсы сети Интернет становятся во многих ситуациях жизненно необходимыми, что далеко не всегда осознаются социумом.

В большинство образовательных стандартов высшего образования включены компетенции, связанные с выработкой навыков безопасной работы в информационно-коммуникационной среде не только у тех, чья профессиональ-

ная деятельность связана с информационными технологиями, но и у людей совершенно разных профессий, в том числе, экономико-управленческой и социально-гуманитарной направленности. Практико-ориентированное формирование этих компетенций возможно в форме привлечения студентов (а также и других категорий граждан) к соревнованиям CTF (capture the flag). Игры такого формата активно используются для совершенствования профессиональных навыков специалистов по информационной безопасности во всем мире. Однако, несмотря на признанную эффективность этой технологии, с одной стороны, и неослабевающую актуальность проблемы формирования у пользователей навыков соблюдения требований информационной безопасности, с другой стороны, подобные соревнования для студентов непрофильных направлений практически не проводятся. В силу отсутствия навыков, необходимых для решения традиционных CTF-задач, задания для неспециалистов должны требовать лишь некоторых базовых навыков. Кроме того, для того, чтобы сформировать заявленные компетенции, задачи и игровая среда должны адекватно отражать действительность и моделировать ситуации и сценарии, встречающиеся на практике и в повседневной жизни.

В настоящей статье предлагается концепция CTF-соревнований в форме квеста «FinCTF», ориентированных на неспециалистов в области информационных технологий с целью формирования у них компетенций, необходи-мых для безопасного использования информационных технологий в своей профессиональной деятельности и повседневной жизни. Пилотный запуск та-ких соревнований состоялся в Новосибирском государственном университете экономики и управления и опробован на студентах НГУЭУ. Концепция квеста и технология его проведения разработаны кафедрой информационной безо-пасности НГУЭУ при активном участии членов университетской CTF-команды FoXXeS [1]. При проведении соревнований задействован функцио-нал экспериментальной сетевой среды учебно-исследовательского полигона лаборатории компьютерной и сетевой безопасности НГУЭУ [2].

1. Цели, задачи и формат соревнований

Основной целью квеста является формирование у участников *навыков решения задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований ин-формационной безопасности*. Выполнение заданий квеста позволяет участни-кам углубить понимание причин возникновения угроз, типичных для инфор-мационных технологий в экономико-финансовой сфере, что способствует по-

вышению мотивации к изучению и соблюдению на практике правил информационной безопасности. Это повышает грамотность пользователей по безопасности информационных технологий, способствует совершенствованию коммуникативных навыков, расширяет кругозор и позволяет приобрести опыт принятия коллективных решений в стрессовых ситуациях и условиях ограниченности времени, развивая так называемые гибкие навыки, или «soft skills», что крайне важно в современном обществе.

Целевая аудитория FinCTF – студенты, обучающиеся по экономическим, управленческим и юридическим профилям. Поскольку квест ориентирован на развитие именно базовых навыков использования общедоступных информационных технологий с учетом требований информационной безопасности, а компетенции, соответствующие цели квеста, есть практически во всех образовательных стандартах высшего образования, то аудитория участников может быть расширена студентами других направлений, активно использующих информационные технологии.

Главная цель игры для участников заключается в получении максимально возможного количества средств на игровом счете команды. Перед началом игры количество средств на счетах каждой из команд одинаково. В начале игры участники имеют доступ только к стартовому заданию, а после его прохождения получают доступ к таск-борду (task-board), где они могут отслеживать свое текущее положение в общем зачете и состояние своего игрового счета. Продолжительность квеста – около 4 часов.

2. Категории предлагаемых заданий

Участникам квеста предлагаются кейсовые задания, относящиеся к различным ситуациям, возникающим в профессиональной деятельности или повседневной жизни. Они призваны научить корректной установке программного обеспечения, грамотной работе с паролями, внимательному отношению к условиям договора, умению распознавать финансовые мошенничества в сетевой среде, эффективно использовать поисковые системы и т.д. Постановка задачи сопровождается легендой, вводящей в курс дела, и в ненавязчивой и доступной форме доносит до участников факт того, что подобные проблемы возникают в реальной практике. Далее в статье приведены некоторые типичные примеры заданий, предлагаемые участникам.

2.1. Корректная установка программного обеспечения

Целью данного задания является выработка навыков внимательного отношения к процессу установки лицензионного и свободно распространяемого программного обеспечения. Проблема, вклад в решение которой призвано внести данное задание, состоит в том, что зачастую пользователи невнимательно читают лицензионное соглашение и, не вникая в его суть, просто подтверждают согласие. Однако такая невнимательность и безответственность может повлечь за собой серьезные последствия. В рамках задания участники должны корректно установить программное обеспечение с оптимальными параметрами. Так, в самом простом случае, в лицензионное соглашение или в некоторые настройки по умолчанию (которые можно изменить при установке) может быть добавлен пункт, согласно которому со счета пользователя списывается некоторая сумма (в игре – это средства на счету команды) или возникают другие нежелательные последствия. Задача команды – заметить подобные вставки и отреагировать на них оптимальным для себя образом, поэтому команды, лучше справившиеся с подобным заданием, увеличат средства на своих счетах или получать какие-либо другие преимущества по сравнению с теми, кто, не читая, примет все условия.

2.2. Распознавание фактов Интернет-мошенничества

Цель задания состоит в изучении одного из наиболее распространенных видов Интернет-мошенничества, называемого фишингом, и в получении навыков выявления признаков фишинговых ресурсов. Как правило, при фишинге создается подложный сайт, внешне не отличимый от оригинального. С его помощью злоумышленники под различными предлогами пытаются заставить клиента предоставить им конфиденциальную информацию (например, номер кредитной карты или пароль для доступа к аккаунту социальной сети или электронной почты) для дальнейшего ее использования в своих интересах.

Согласно одной из возможных легенд, участники получают несколько ссылок на web-ресурсы, например, на страницы Интернет-банка, где размещена некая памятка безопасности. Игроки должны выявить все фишинговые признаки и определить подлинный сайт банка. Задание считается выполненным при прохождении процедуры авторизации на подлинном сайте. За попытку пройти авторизацию на поддельных сайтах с игрового счета будет списываться некоторая сумма.

2.3. Соблюдение парольной политики

Данное задание призвано сформировать у участников представление о парольной политике и необходимости ее соблюдения. Идея такого задания возникла вследствие того, что по статистике более 30% пользователей используют слабое пароли к своим учетным записям. Это часто приводит к взлому не только личных аккаунтов, но и корпоративных информационных систем, что может иметь крайне серьезные последствия как для конкретного человека, так и целых организаций. В рамках задания участникам может быть предложено зарегистрировать почтовый ящик на указанном ресурсе, причем система отслеживает стойкость пароля и снимает деньги со счета команды при вводе слабой комбинации. Проверка на стойкость может производиться различными способами, но главный – это возможность алгоритма подобрать введенный пароль, что будет означать взлом аккаунта.

2.4. Сбор информации из открытых источников

Выполнение этого задания должно позволить участникам проверить и развить свои навыки поиска информации в открытых источниках. В контексте современной ситуации проблема заключается в том, что, с одной стороны, сейчас посредством сети Интернет доступно большое количество информации, но, с другой, – для поиска релевантных данных, действительно относящихся к какому-либо вопросу, необходимы определенные умения. В рамках таких заданий участникам предлагается некая легенда с описанием проблемы, решить которую можно, используя открытую информацию. Задание заключается в поиске этой информации. Например, целью может стать адрес ме-стонахождения преступника с использованием геометок, встроенных в фото-графии, размещенные в социальных сетях.

Литература

1. Сайт CTF-команды FoXXeS (НГУЭУ) // https://foxxes.ru/

2. Лисс А.А., Соловьев Д.Н., Пестунова Т.М. Создание экспериментальной сетевой среды для изучения компьютерной и сетевой безопасности // Информационное противодействие угрозам терроризма. 2015. № 24. С. 243-251.