**ИСПОЛЬЗОВАНИЕ КЕЙС-ТЕХНОЛОГИИ ПРИ ОРГАНИЗАЦИИ ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ ОБУЧАЮЩИХСЯ**

*Стефановская Е.О., Кетрова А.А., преподаватели*

*г.Красноярск, КГБПОУ «Красноярский колледж радиоэлектроники*

*и информационных технологий»*

В рамках ежегодно проводимого Единого урока безопасности в сети Интернет для обучения студентов специальности 09.02.07 Информационные системы и программирование правилам безопасного поведения в Сети авторами был выбран формат кейс-игры, где были поставлены следующие задачи:

* привлечение внимания обучающихся к проблеме безопасности в сети Интернет;
* обсуждение с обучающимися правил безопасной работы в Сети;
* формирование у обучающихся навыков этичного и ответственного поведения в Сети;
* разработка рекомендаций по созданию системы защиты пользователей Интернета от информации, причиняющей вред их здоровью, развитию и благосостоянию.

Под кейс-игрой понимают интерактивную технологию обучения, где в качестве кейсов выступают задачи, представляющие проблемные ситуации из реальной жизни. Данный формат нацелен, в первую очередь, на активное взаимодействие всех участников команды, что повышает уровень вовлеченности обучающихся в процесс поиска путей решения задачи.

Постепенное нарастание сложности выполнения заданий по ходу кейс-игры позволяет командам работать наиболее эффективно:

* первый этап позволяет консолидировать участников команды для достижения общей цели;
* второй этап побуждает участников команды к обмену эмпирическими знаниями и разработке общей стратегии решения поставленной задачи;
* третий этап стимулирует команды сгенерировать новые идеи, подходы к решению кейса и предложить механизмы их реализации.

Количество команд для участия – четыре. Каждая команда представлена пятью студентами из одной группы. Список участников формируется самими же студентами.

Как уже было сказано выше, процесс проведения кейс-игры разделен на три этапа.

В первом задании необходимо пройти онлайн-тестирование, состоящее из 10 закрытых тестовых заданий. Задания составлены как на знание основополагающих понятий информационной безопасности, так и общих правил и рекомендаций безопасного поведения каждого пользователя в сети Интернет. Некоторые вопросы содержали описание стандартных ситуаций, которые возникают в жизни каждого пользователя Сети. Ситуации простые, понятные, знакомые каждому пользователю Интернета.

Однако, по результатам тестирования стало очевидно, что не все студенты знают, как правильно нужно поступить в данной ситуации. Да, вопросы теоретического характера на знание базовых определений по теории информационной безопасности не вызвали сложности. А вот ответы на практикоориентированные вопросы заставляют задуматься – умеют ли студенты применять полученные знания в реальной жизни за пределами образовательного учреждения? В конкретной ситуации ответ на поставленный вопрос будет неудовлетворительным. Возможно, такие результаты были получены из-за достаточного сжатого времени на выполнение задания.

Второе задание предполагает решение кейс-задач. Ситуации, описанные в каждом кейсе, предложены на основе реальных задач, с решением которых сталкивается каждый пользователь Сети:

* совершение покупки в Интернет-магазине;
* онлайн-бронирование билетов, гостиниц и т.д.;
* покупка товаров в социальных сетях.

За отведенное время студенты должны предложить решение одной из задач: сформулировать этапы проверки безопасности совершения того или иного действия в Сети, подкрепляя свои варианты демонстрацией на ПК. Результаты оказались весьма впечатляющими – студенты предложили структурированную и достаточно полную последовательность действий, которые должен предпринять пользователь Сети в предполагаемой ситуации.

Осведомленность в данной аспекте именно этой категории населения РФ подтверждают и данные статистики [2]. По данным ВЦИОМ на 16 марта 2022 г. опыт совершения онлайн-покупок есть у 62% россиян, среди которых наибольший процент составляют молодые люди 18-24 лет (87%). ВЦИОМ утверждает, что за последние один-два года на 74% вырос спрос на совершение онлайн-покупок у населения в возрасте от 18 до 24 лет. Все эти статические данные говорят о том, что наиболее активный сегмент населения, которому хорошо знакома процедура онлайн-покупки в Сети, это и есть та самая возрастная аудитория, которая и принимала участие в кейс-игре по безопасности в Сети.

Однако, согласно исследованиям компании RTM Group [1] в 2021 году зарегистрировано 517722 преступлений, связанных с хищениями с использованием информационных технологий, в том числе и в Сети.

Эти данные заставляют задуматься: если в большинстве своем Интернет-аудитория владеет в достаточной мере информацией о поведении в Сети, почему же так высок процент обманутых мошенниками? Конечно, участники игры не являются репрезентативной выборкой для проведения социологического исследования, и кейс-задачи не предполагают их реального выполнения (предложенные варианты решения кейсов носят исключительно теоретический характер). Возможно, эти результаты получены по причине того, что каждая пятая онлайн-покупка в РФ является незапланированной и сделана спонтанно [3], и в этот момент пользователь Сети пренебрегает правилами безопасности. Также результаты аналитической платформы GfK говорят о том, что для многих пользователей Сети онлайн-покупка – это хороший вариант времяпровождения. А в такие моменты, как известно, любой человек настроен только на позитивные мысли, не задумываясь о возможных последствиях предоставления своих персональных данных мошенникам. Стоит ли говорить, что данный этап игры вызвал наибольший интерес у студенческой аудитории и породил длительную дискуссию по каждому кейсу.

Задача третьего этапа игры заключается в том, чтобы студенты предложили свои дополнения к существующим законам РФ, регламентирующим права пользователей Сети. Среди большого количества предложений хотелось бы выделить следующие:

* разделение информационных ресурсов Сети согласно возрастному критерию пользователя с обязательным введением цензуры для несовершеннолетнего населения;
* введение единого реестра всех Интернет-ресурсов, предполагающих сбор и использование персональных данных пользователя;
* внедрение программы обучения нейросетей для распознавания в Сети контента, связанного с жестокостью и насилием, для дальнейшей блокировки;
* защита персональных данных пользователя социальных сетей от разглашения без его согласия (репост, сохранение фото, ссылка на аккаунт и тд);
* введение системы идентификации каждого пользователя Сети с последующим отслеживанием его действий.

При обсуждении была поднята тема буллинга в социальных сетях. Данную тему затронула лишь одна команда из четырех. Это была та команда, где трое из пяти участников были представителями женского пола. И это не удивительно, ведь по данным ЮНЕСКО психологической травле больше подвержены девочки [4]. Участники команд-соперников могли задавать вопросы выступающим, и вопросы по этой теме задавали только представители женского пола. Предложенное этой командой решение поставленной задачи разительно отличалось от подхода команд-соперников. Команды, состоящие преимущественно из представителей мужского пола, по данному кейсу четко выстроили последовательность вытекающих друг из друга предложений по модернизации системы безопасности пользователя в Сети, но не затронули вопросы защиты личности самого пользователя.

Подводя итоги кейс-игры, можно констатировать, что поставленная в самом начале цель - акцентировать внимание студенческой аудитории на проблеме безопасности в Сети - была достигнута. Задачи реализованы. Результаты игры подтверждают тот факт, что сегодня неконтролируемая глобальная сеть представляет из себя опасную среду для всех возрастных категорий пользователей. И становится очевидным, что остро необходимы изменения в вопросах использования Сети на законодательном уровне.

**Электронные ресурсы:**

1. Консалтинговая компания «RTM Group»: официальный сайт. – Обновляется в течение суток. – URL: <https://rtmtech.ru> (дата обращения: 19.04.2023);
2. Сетевое издание ВЦИОМ: официальный сайт. – Обновляется в течение суток. – URL: <https://wciom.ru> (дата обращения: 05.05.2023);
3. Аналитическая платформа «GfK»: официальный сайт. – Обновляется в течение суток. – URL: [https://www.gfk.com](https://www.gfk.com/ru/insights/issledovanie-jandeksmarket-i-gfk-razvitie-roznichnoi-onlain-torgovli-v-rossii) (дата обращения: 07.05.2023);
4. Организации Объединённых Наций по вопросам образования, науки и культуры ЮНЕСКО: официальный сайт. – Обновляется в течение суток. – URL: <https://www.unesco.org> (дата обращения: 11.04.2023).

**Список литературы:**

1. Райтман М. Информационная безопасность для пользователя. Правила самозащиты в Интернете. – СПб.: БХВ-Петербург, 2022. – 400 с.;
2. Самыгин С.И. Столяренко Л.Д., Алексеенко И.Н.: Педагогические технологии в образовании. Учебное пособие. - Ростов н/Д.: Феникс, 2022. – 319 с.;
3. Современные образовательные технологии: учебное пособие для вузов / Л. Л. Рыбцова [и др.]; под общей редакцией Л. Л. Рыбцовой. — Москва: Издательство Юрайт, 2022. - 92 с.