ТЕСТИРОВАНИЕ ТЕХНОЛОГИЙ СОЦИОИНЖЕНЕРНЫХ АТАК НА ПОЛЬЗОВАТЕЛЕЙ СЕТЕВЫХ РЕСУРСОВ КРЕДИТНО-ФИНАНСОВЫХ ОРГАНИЗАЦИЙ

В.В. Маликов, А.В. Макатерчик

В настоящее время в мире и Республике Беларусь значительно возрастает число инцидентов, связанных с несанкционированных доступом к сетевым ресурсам кредитно-финансовых организаций (КФО). В ходе исследования авторами описана базовая структура проведения социоинженерных (социотехнических) атак, которая включает детализацию каждого из 5-ти ее этапов.

Предложен подход к оценке вероятности успеха многоходовой социоинженерной (социотехнической) атаки, а также описана модель базового профиля уязвимости цели (объекта атаки). Для оценки применимости существующих методик/алгоритмов социоинженерных (социотехнических) атак, авторами статьи было проведено практическое тестовое исследование (fair use / fair dealing). В качестве объектов атаки были выбраны два пользователя сервисов двух разных КФО (согласие пользователей сервисов КФО на исследование получено и проведен дополнительный инструктаж, Ф.И.О. пользователей – заменены порядковыми номерами, фишинг эмулировал адресные данные сервисов КФО, срок возможного проведения цикла атаки – до 10-ти дней). Оценка полноты информации по базовому профилю уязвимости цели атаки осуществлялась на основе метода экспертных оценок.

Предложены рекомендации для противодействия ряду способов, используемых для проведения социоинженерных (социотехнических) атак.