УДК 614.8+002.6:004.89

ПРИМЕНЕНИЕ ВЕРОЯТНОСТНО-РЕЛЯЦИОННЫХ МОДЕЛЕЙ КОМПЛЕКСА «КРИТИЧНЫЕ ДОКУМЕНТЫ – ИНФОРМАЦИОННАЯ СИСТЕМА – ПОЛЬЗОВАТЕЛЬ – ЗЛОУМЫШЛЕННИК» ДЛЯ АНАЛИЗА ЗАЩИЩЕННОСТИ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННЫХ СИСТЕМ ОТ СОЦИО-ИНЖЕНЕРНЫХ АТАК[1]

Азаров А.А.[*,**], **Абрамов М.В.**[*], **Тулупьева Т.В.**[*,****], **Фильченков А.А.**[***]

[*]СПИИРАН, г. Санкт-Петербург

[**]Институт гуманитарных технологий в сфере социального компьютинга Московского государственного гуманитарного университета им. М.А. Шолохова, г. Москва

[***]Университет ИТМО, г. Санкт-Петербург

[****]Санкт-Петербургский государственный университет, г. Санкт-Петербург

Поступила в редакцию 13.12.2014, после переработки 02.02.2015.

В статье описаны модели пользователей и профилей уязвимости, модель злоумышленника и социинженерных атак, модель информационной системы и программно-технических устройств. Тенденции развития современного бизнеса зачастую требуют сохранения конфиденциальности корпоративной информации, утечки которой могут привести к существенным финансовым потерям. Утечки конфиденциальной информации могут быть связаны как с проблемами и незащищенностью программно-технической составляющей информационной системы организации, так и с пользователями такой системы. Утечка конфиденциальной информации от пользователей информационных систем может быть осуществлена по нескольким причинам: из-за социо-инженерных атакующих воздействий злоумышленника, когда пользователь введен в заблуждение и злоумышленник получает требуемую конфиденциальную информацию, а также из-за инсайдерских атак самих пользователей информационной системы. Инсайдерские атаки пользователей информационных систем могут быть осуществлены также с привлечением социо-инженерных атакующих воздействий, но в данном случае источник социо-инженерного атакующего воздействия будет находится внутри организации.

Ключевые слова: вероятностно-реляционная модель, информационная безопасность, социо-инженерные атаки, защита пользователя.

Нечеткие системы и мягкие вычисления. 2015. Т. 10, № 2. С. 209–221.

[1]Статья содержит материалы исследований, частично поддержанных грантом РФФИ 15-01-09001-а — «Комбинированный логико-вероятностный графический подход к представлению и обработке систем знаний с неопределенностью: алгебраические байесовские сети и родственные модели».