МОДЕЛИРОВАНИЕ СОЦИОИНЖЕНЕРНЫХ АТАК

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Высокович Д. В., Ладеева А. С.

Давыдовский А.Г. – канд. биол. наук, доцент

Одной из задач в сфере информационной безопасности является обеспечение защищенности пользователей информационных социотехнических систем (ИСТС) от социоинженерных атакующих воздействий, которые предполагают социопсихологическое воздействие на пользователя ИСТС с целью влияния на процесс принятия управленческих решений и получение доступа к критически важным информационным ресурсам. Проявления уязвимостей пользователей ИСТС различны и индивидуальны, а их реакция на социопсихологические воздействия недетерминированы и мало прогнозируемы.

Предложена гипотеза о влиянии психологических особенностей пользователя социальных сетей предрасположенность к определенным особенностям поведения при восприятии, обработке и передаче информации. Модель распространения информации в виртуальном пространстве включает: 1) виртуальное пространство, представленное набором участников виртуальных социальных сетей, по которым могут распространяться мемы; 2) социальные контакты i-го предъявителя информации, включающие Ni, т.е. непосредственно соединенные ребрами социальных взаимодействий с предъявителем, — именно они могут увидеть предъявляемую информацию; 3) предъявитель информации, который является участником социальной сети; 4) предъявляемая информация, которая обладает таким свойствами, как ироничность, иносказательность, эмоциональная окраска и т.д.; 5) психологические характеристики i-го участника социальной сети F, которые должны учитывать особенности информации и степень проявления которых должна отражать восприимчивость участника социальной сети к характеристикам информации; 6) при моделировании социальных сетей образование связи между пользователями формируются стохастически.

Возможные варианты реализации атаки имитируются с помощью последовательностей атакующих действий, причем сведения о таких последовательностях впоследствии организуются в виде особой структуры, получившей название «деревьев атак» (и в более общей ситуации — графов атак). Имитация атаки осуществляется в рамках некоторой сцены или контекста, которые отражают состояния комплекса «информационная система–персонал» и их изменения в ответ на атакующие действия. Информационная модель сцены воздействия социоинженерной атаки включает описание: набора документов, хранящихся в информационной системе и характеризующихся различной степенью критичности по отношению к раскрытию, утрате и изменению; набора программно-технических компонент информационной системы; коллектива пользователей; связей между вышеуказанными компонентами.

Факторы уязвимости пользователя ИСТС к социоинженерным атакам: возможность подкупа пользователя; возможность шантажа пользователя; социальные и личностные проблемы пользователя; его стремление к самореализации и самоактуализации в своей референтной группе.

Рассмотрим ситуацию, когда атака осуществилась, т.е. пользователя оказалось возможным подкупить. Он получает информацию о том, какие данные ему надо найти и передать злоумышленнику, и начинает действовать. В таком случае возможны две ситуации. Допустим, что:

1) Если доступ к искомой информации возможен. Пользователь может либо отдать сетевой логин-пароль злоумышленнику (что позволяет извне получить доступ к искомой информации), либо скопировать информационный объект, необходимый злоумышленнику, и позже передать ему копию объекта;

2) Если прямой доступ к искомой информации невозможен. При этом пользователь может совершить следующие действия: а) пытается отсканировать информационную систему, чтобы выявить ее структуру, тем самым облегчая задачу злоумышленнику; б) пробует предположить (перебирая доступные варианты), где может находиться интересующая злоумышленника информация; в) установит программное обеспечение для удаленного доступа к защищенным информационным ресурсам.

Список использованных источников:

1. Новиков Д.А. Теория управления организационными системами. М.: МПСИ, 2005. – 584 с.
2. Грановская Р.М., Крижанская Ю.С. Творчество и преодоление стереотипов. СПб.: OMS, 1994. 180 с.
3. Котенко И. В., Степашкин М. В., Богданов В. С. Анализ защищенности компьютерных сетей на этапах проектировании и эксплуатации // Изв. вузов. Приборостроение. 2006. Т. 49, № 5. С. 3–8.