ПРОБЛЕМА НАДЕЖНОСТИ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННЫХ СИСТЕМ В УСЛОВИЯХ СОЦИОИНЖЕНЕРНЫХ АТАК

Пашкина М.Г.
Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь
Давыдовский А.Г. – к.б.н.,доцент

Представлена и охарактеризована проблема многофакторности надежности пользователей информационно-телекоммуникационных систем в условиях социоинженерных атак.

Цель работы – обоснование проблемы многофакторности надежности пользователей информационно-телекоммуникационных систем в условиях социоинженерных атак.

В связи с быстрым ростом количества информационных систем, а так же повышением их уровня сложности, актуальным становится вопрос надежности пользователей и их защиты от социоинженерных атак. Надежность пользователя включает надежность информационно-телекоммуникационной системы (ИТС) и надежность личности пользователя.

Надежность личности пользователя ИТС непосредственно зависит от комплекса его профессионально-важных качеств, уровня и качества его профессиональной подготовки, особенностей аксиосферы, эмоционально-волевой и когнитивной сферы, которые характеризуются собственными детерминантами, доступными для исследования и прогностической оценки с помощью методов дифференциальной психологии личности, психологии труда, инженерной психологии.

Надёжность ИТС характеризуется безотказностью, долговечностью, ремонтопригодностью, а также конфиденциальностью, сохранностью и доступностью информационных ресурсов. К внешним угрозам для пользователей ИТС относятся: обновления и сбои в работе программного обеспечения; уязвимости программного обеспечения и аппаратной части ИТС; несовместимость различных версий и платформ программного обеспечения, с одной стороны, и аппаратной части, с другой стороны; труднопредсказуемые флуктуации плотности передачи информации в телекоммуникационной сети; некорректная реализация протоколов передачи информации в функционировании сетей и интерфейсных систем; разрушение иерархических отношений ИТС; распространение разрушающих программных средств (компьютерных вирусов, сетевых червей и др.); реализация DDoS-атак, хакерских и крэкерских атак.

Наиболее распространенными уязвимостями пользователей являются: слабый пароль, техническая неопытность или некомпетентность, халатность и установка на получение личной выгоды, принадлежность определенным социальным группам; интенсивное использование социальных сетей и высокий уровень активности (количество задействованных аккаунтов, подписчиков, групп и т.д), активное потребление контента в том числе вредного, стратегии формирования медиазависимого поведения, семейный фактор.

Для успешной социоинженерной атаки профиль злоумышленника должен включать набор необходимых технических навыков для взлома системы, а так же способностей анализировать и использовать характеристики и уязвимости пользователя.

Например, при слабом пароле пользователя либо технической неосмотрительности вредоносное программное обеспечение, а так же хакерская атака имеют больше шансов на успех, чем при использовании надежного пароля, и внимательной работе внутри системы.

Таким образом, вероятность успеха реализации социоинженерной атаки зависит как от интенсивности, последовательности, продолжительности, интервальной периодичности, так и от характеристик контекста социоинженерных воздействий, осуществляемых с различными целями. В свою очередь, эти же факторы в значительной мере детерминируют надежность пользователей ИТС в условиях реализации комплексных (гибридных) социоинженерных атак.

Дальнейшие перспективы развития настоящего исследования связаны с разработками и исследованиями математических моделей зависимости комплексной надежности пользователя от многих факторов состояния ИТС в условиях социоинженерных атак.

Список использованных источников:

1. Митник, К.Д. Искусство обмана / К.Д. Митник, В.Л. Саймон. – АйТи, 2004. – 360 с.

2. Краткое введение в социальную инженерию. – [Электронный ресурс]. – Режим доступа: https://habr.com/ru/post/83415/. – Дата доступа: 16.01.2020.

3. Мартынова, Л. Е. Социальная инженерия и информационная безопасность / Л. Е. Мартынова, К. Е. Назарова, С. М. Попков, А. А. Белозёрова и др. // Молодой ученый. – 2017. – №1. – С. 61-63.

4. Багров, Е.В. Мониторинг и аудит информационной безопасности на предприятии / Е.В. Багров. – Вестник ВолГУ. – 2011. - Серия 10. Вып. 5. .– С.54–56.

5. Чурилина, А.Е. Программный комплекс обнаружения атак на основе анализа данных реестра / А.Е. Чурилина // Вестник ВолГУ. Серия 10. Инновационная деятельность. Выпуск 6. 2012 г. – стр. 152–155.