Секция «Психология интернета и информационных технологий»

Особенности делинквентного поведения административного персонала организаций, обрабатывающих персональные данные граждан РФ

Зарубин Юрий Сергеевич

Студент (бакалавр)

Балтийский федеральный университет имени Иммануила Канта, Институт социально-гуманитарных технологий и коммуникации, Калининград, Россия

E-mail: Felis.zh@gmail.com

Актуальность исследования объясняется распространенностью и очевидной ролью информационных систем в современном мире, а соответственно, и теми рисками, которые обусловлены нарушением безопасности информационных систем. При этом стоит отметить, что именно угрозы не технического, а организационного типа, так называемый человеческий фактор, играют ведущую роль в составе успешных информационных атак на критические узлы информационных систем. Например, именно он составляет 80% успешных атак на финансовые организации по данным одного из ведущих разработчиков программно-аппаратного обеспечения [1].

В ходе данного исследования была предпринята попытка моделирования потенциального нарушения периметра информационной безопасности предприятия, обрабатывающего персональные данные граждан РФ методом естественного эксперимента.

Основным методом исследования при этом выступили эксперимент и включенное наблюдение экспериментатора за особенностями делинквентного поведения административного персонала компаний, занимающихся в ходе своей деятельности обработкой персональных данных.

В данном случае под социальным поведением (далее - поведением), подразумевается поведение, выражающееся в совокупности поступков и действий индивида или группы в обществе и зависящее от социально-экономических факторов и господствующих норм [2]. Под делинкветными же его формами, вслед за Зимановской Е.В. [3] понимается как антисоциальные девиации - действия или бездействие противоречащие существующим правовым нормам, угрожающих социальному порядку и благополучию окружающих, да и не только окружающих, людей.

Видеофиксация хода эксперимента не велась по причине ограниченности ресурсов и возможности нарушения хода эксперимента, а также по причине частичного ограничения на ведение видеосъемки на объектах, в которых проводилось исследование.

Выборка напрямую связана с выбранным видом исследования - естественным экспериментом и представляла собой 30 лиц женского пола в возрасте от 20 до 45 лет, работающих в должности административного персонала, по 15 соответственно в торговых центрах в г. Калининграде и г. Москве.

Особенностью выборки может быть более высокая суггестивность женщин относительно мужчин [4], а также не техническая направленность образования, что объясняется спецификой деятельности - обработкой персональных документов.

Экспериментатор в ходе эксперимента, согласно процедуре, обращался к персоналу выбранной организации с просьбой вставить flash-накопитель в соответствующий разъем их рабочего компьютера и распечатать файл, имеющий двойное расширение и по своей конфигурации напоминающий компьютерный вирус (однако это был простой документ, приведенный к подобному виду, ни в коей мере не содержащий вредоносный программный код).

В двух московских организациях физически отсутствовала возможность произвести данную процедуру поскольку подключение к usb-портам было заблокировано системным администратором, что говорит о выполнении минимальных мер обеспечения информационной безопасности на данном предприятии.

Успешное внедрение произошло в 8 случаях из 13 возможных в Москве и в 11 из 15 в Калининграде.

Сознательная предварительная проверка накопителя антивирусом проводилась только три раза — два раза в Калининграде и один раз в Москве.

Ни в одной из успешно проведенных итераций параметры файла не вызвали подозрений пользователя в злонамеренности процедуры. Соответственно, ни в одном из этапов проведения эксперимента служба безопасности организации не была оповещена о попытке проникновения в информационную систему предприятия, однако в ходе одного из прецедентов оказывала активное содействие проникновению.

Полученные в ходе исследования данные позволяют сделать вывод, что социальное поведение, наблюдаемое в ходе естественного эксперимента, можно отнести к делинквентному, т.е. компрометирующему персональные данные граждан РФ, за которые данный административный персонал несет персональную административную и уголовную ответственность [5].

Такие результаты можно предположительно объяснить несформированностью социальных установок об информационной безопасности у административного персона, низкой значимостью задачи обеспечения защищенности персональных данных, недостаточной технической грамотностью и незаинтересованностью в технических аспектах работы информационных систем.

Источники и литература

1) Cisco 2013 Annual Security Report, ASR;
2) Социологический энциклопедический словарь // Ред.-координатор Г. В. Осипов. — М., 1998;
3) Змановская Е. В. Девиантология: Психология отклоняющегося поведения: Учебное пособие для студентов ВУЗов. — 2 изд, исправл. — М.: Академия, 2004;
4) Крысько В.Г. Секреты психологической войны//Минск, Харвест 1999;
5) «О персональных данных» (152-ФЗ), М., Кремль.