ПОДХОД К ВЫЯВЛЕНИЮ ИНСАЙДЕРОВ НА ОСНОВЕ МЕТОДОВ ВИЗУАЛЬНОЙ ПСИХОДИАГНОСТИКИ В ЦЕЛЯХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ

Снегуров А.В., Романчук Е.Ю.
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Ленина, каф. телекоммуникационных систем, тел. (057) 702-13-06,
E-mail: arksn@rambler.ru ; факс (057) 702-11-13

In this report the issue of fighting with insiders is considered, and the method of assessment of employees emotional condition is offered, which is based on the mathematic apparatus of the fuzzy logic.

Постановка проблемы. В настоящее время одной из ключевых угроз информационной безопасности продолжает оставаться инсайдерская деятельность. Так, например, в результате опроса, проведенного корпорацией Symantec и сообществом Профессионалы.ru. выяснилось [1], что 70% сотрудников российских компаний выносят с работы конфиденциальные данные. 68% опрошенных допустили утечку через социальные сети, 56% сознались, что выносили секреты на флешке. По результатам онлайн-опроса, проведенного компанией SailPoint [2] 29% американцев и 23% британцев, меняя место работы, готовы украсть у предыдущих работодателей базы данных клиентов. 15% американцев и 17% британцев могут взять с собой внутреннюю документацию, планы компании и дизайн продуктов. Опрос с участием 500 айтишников, проведенный Government Technology [3] показал, что примерно 40% IT-специалистов в случае чего могут взять в заложники сеть работодателя. Исследование, проведенное компанией Venafi, также показало, что треть респондентов уверена в том, что их знаний и полномочий достаточно, чтобы парализовать работу компании.

По ряду проводимых исследований [1] причины утечек кроются в небрежности (у 37% опрошенных корпоративные ноутбуки лежали без присмотра в общественных местах), беспечности (50% используют простые пароли, а 10% и вовсе приклеивают их возле компьютера), излишней доверчивости (68% не гнушаются попросить друзей помочь с особо трудным корпоративным файлом). Около 9% сознались, что подумывали продать конфиденциальную информацию на сторону, 6% так и сделали, а 45% отправляли данные по запросу клиентов.

В настоящее время существует следующая классификация инсайдеров в зависимости от механизма реализации ими зловредных действий и мотивации на нарушение информационной безопасности [4]. Халатные - сотрудники, которые по своей халатности допустили нарушение конфиденциальности, целостности или доступности информации (КЦД). Манипулируемые - сотрудники, подвергшиеся атакам методами социальной инженерии. Обиженные - сотрудники, которые по личным мотивам стремятся нанести вред компании. Нелояльные - сотрудники, как правило, меняющие место работы и уносящие всю информацию, до которой были доступны. Завербованные - сотрудник изначально лояльный, а затем подкупленный либо запуганный. Внедрённые - сотрудники специально устроенный в организацию для похищения информации.

Решение проблемы борьбы с инсайдерами имеет несколько направлений:

1. Выявление предрасположенности к инсайдерству. Данные механизмы позволяют определить возможность сотрудников стать халатными, манипулируемыми, обиженными, нелояльными инсайдерами.

2. Определение того факта, что сотрудник стал инсайдером. Механизмы, реализующие данное направление, должны позволять выявлять все типы инсайдеров. При этом наиболее сложно выявить внедренного инсайдера, который может быть специально подготовлен к такой деятельности.

3. Реализация организационно-технических мероприятий по защите информации от инсайдеров.

Одним из перспективных механизмов борьбы с инсайдерством является использование методов визуальной психодиагностики как для выявления предрасположенности анализируемого сотрудника к инсайдерской деятельности, так и для выявления инсайдера. Следует заметить, что результаты визуальной психодиагностики должны использоваться в рамках комплекса организационно-технических мероприятий борьбы с инсайдерами. Определение психологических характеристик человека по его телесным (внешним), подсознательным проявлениям позволяет повысить адекватность принятия решения руководителей, особенно при допуске сотрудников к критической для организации информации.

Целью исследования является рассмотрение проблемы борьбы с инсайдерством, разработка методов визуальной психодиагностики для повышения эффективности обеспечения информационной безопасности организаций.

Согласно исследованиям учёных в данной области, широко известны данные о том, что в течение первых 12 секунд общения, при знакомстве, на долю невербальных сигналов приходится примерно 92 % всего объема принимаемой информации. Кинесические исследования Ф. Селже говорят о том, что при разговоре значимость слов составляет лишь 7%, интонация — 38%, а на жесты и мимику приходится 55% [5]. Жесты могут рассказать: о характере, о темпераменте, об отношении к партнеру, об эмоциональном состоянии человека, о попытке обмана и т.д. Невербальные движения, используемые человеком, трудно им контролируются, что позволяет использовать их для оценки ситуаций в сфере информационной безопасности.

В исследовании были рассмотрены и классифицированы наиболее часто используемые основные жесты и позы. Рассмотрены следующие виды жестов: жесты-симптомы, выполняющие функцию самовыражения: выражают состояние, процессы, модальные (выражают оценку субъектом чего-либо); жесты-регуляторы, которые выполняют регулятивно-коммуникативную функцию воздействия на партнера; жесты-информаторы, выполняющие информативно-коммуникативную функцию. В ходе исследования были рассмотрены шесть основных эмоциональных состояний (гнев, радость, страх, печаль, удивление и отвращение) универсальных для всех людей. Для каждого эмоционального состояния были приведены их основные мимические проявления. В исследовании предложен способ описания эмоциональных состояний человека и их распознавания на основе математического аппарата нечеткой логики.

Направлениями дальнейших исследований является выявление всех особенностей поведения инсайдеров, автоматизация процессов съема информации при осуществлении визуальной психодиагностики, автоматизация процессов комплексной обработки информации при выявлении инсайдеров.

Литература:

1. Ульянов В.В. Динамика безопасности: от внешних угроз – к внутренним [Текст] / В.В.Ульянов // Защита информации. INSIDE. – 2008. - № 4. – С. 34 – 38.

2. 70% сотрудников крадут корпоративные секреты [Электронный ресурс] / Securitylab - Режим доступа: URL: http://www.securitylab.ru/news/405499.php. - 27 апреля, 2011. - Загл. с экрана.

3. Уволенные офисные сотрудники чаще воруют данные, чем вещи [Электронный ресурс] / Securitylab - Режим доступа: URL:http://www.securitylab.ru/news/396974.php. - 23 августа, 2010. - Загл. с экрана.

4. 40% IT-специалистов готовы взять в заложники сеть работодателя [Электронный ресурс] / Securitylab - Режим доступа: URL:http://www.securitylab.ru/news/405783.php. - 01 июня, 2011. - Загл. с экрана.

5. Петрова Е.А. Жесты в педагогическом процессе. [Текст] / Е. А. Петрова. - М.: Педагогическое общество России , 1998. – 222 с.