УДК 004.056.53

МОДЕЛЬ АНАЛИЗА ПОВЕДЕНИЯ ПОЛЬЗОВАТЕЛЯ ИНТЕРНЕТ-СИСТЕМЫ

Зернов В.В. (Университет ИТМО)
Научный руководитель – к.т.н., доцент факультета ИКТ Карманов А.Г.
(Университет ИТМО)

В современных интернет-системах обмена данными «Vicious Employees» являются основной угрозой информационной безопасности. В докладе рассматривается модель, которая анализирует поведение пользователя интернет-системы и позволяет выявить нелегитимного пользователя, а также нарушение конфиденциальности и целостности информации.

Введение. Регулярные утечки конфиденциальной информации под воздействием человеческого фактора стали новой реальностью современного цифрового пространства. За последние 5 лет произошло несколько громких утечек персональных данных граждан: в государственных банках, частных телекоммуникационных компаниях и электронных сервисах, оказывающих государственные услуги.
В современных масштабных интернет-системах для обеспечения их безопасности используется анализ поведения пользователей. Существует множество решений от зарубежных вендоров программного обеспечения (Forcepoint, Fortscale, Gurucul, Securonix), а также несколько продуктов от отечественных компаний (модуль Prediction от InfoWatch, центр профилирования от SearchInform и система UBA от Zecurion).

Основная часть. Модель анализа поведения пользователя интернет-системы предназначена для предотвращения утечек конфиденциальной информации и попыток несанкционированного доступа к информации. Определенный набор действий отдельно взятого пользователя интернет-системы так или иначе является уникальным. Данная модель позволяет выявить отклонения от нормального поведения легитимного пользователя, рассчитать вероятность определения реальности угрозы безопасности системы и самостоятельно принять решение для ее предотвращения.
В отличие от существующих решений, такая модель не требует огромного количества вводных данных о пользователе из разных источников за счет своей автономности, которая достигается благодаря применению передовых технологий машинного обучения.

Выводы. Внедрение модели анализа поведения пользователя в интернет-системы обмена данными государственного назначения позволит предотвратить утечки конфиденциальной информации, а также снизить количество успешных попыток несанкционированного доступа к информации под воздействием человеческого фактора и, как следствие, сократит количество успешных кибер-преступлений (совершение противоправных действий от лица легитимного пользователя) в таких системах.

Зернов В.В. (автор)

Карманов А.Г. (научный руководитель)