ИСПОЛЬЗОВАНИЕ ВЕРОЯТНОСТНОГО МЕТОДА ДЛЯ АНАЛИЗА СЕТЕВОЙ АКТИВНОСТИ ПОЛЬЗОВАТЕЛЯ ПЕРСОНАЛЬНОГО КОМПЬЮТЕРА А.М. Мажейко, Е.С. Белоусова

Авторизация пользователей компьютерных систем в классическом варианте представляет собой однократный этап аутентификации. Это значит, что после получения пользователем прав доступа не производится каких-либо промежуточных проверок и сессия считается легитимной до момента ее завершения. В этом случае кража либо утеря ключа доступа может предоставить злоумышленнику возможность пользования ресурсами без ограничений. При предварительной разведке такая ситуация способствует получению более широких прав доступа, вплоть до уровня администратора либо владельца системы. Таким образом ввод дополнительных элементов управления доступом является актуальным. В настоящее время попытки ввода систем защиты информации с использованием поведенческого анализа предприняты на базе антивирусных продуктов и межсетевых экранов следующего поколения (Next-Generation Firewall). Применение подхода подобного типа для аутентификации пользователей представляется перспективным направлением. Анализ поведения пользователя предоставляет возможность более быстрой реакции на инциденты незаконного проникновения, сканирования структуры сети передачи данных и действий, не связанных с выполнением непосредственных рабочих задач. Математическим инструментом данного подхода может служить вероятностный метод [1]. Определение вероятностей подключения от имени определенного пользователя к различным ресурсам и элементам сети передачи данных создает дополнительный контроль в управлении доступом. К примеру, подключение бухгалтера к сервису начисления заработной платы происходит по определенному расписанию ежемесячно. В этом случае создаются временные метки, содержащие различные величины вероятности подключения бухгалтера к данному сервису. Сопоставление активности данного пользователя и ранее определенной вероятности подключения предоставляет возможность принятия решения об аномальном поведении, и соответственно, принятии мер о блокировке доступа.

Таким образом, проведение оценки сетевой активности пользователя персонального компьютера позволит применять автоматические меры ограничения либо полной блокировки доступа при аномальной активности до момента анализа ситуации администратором информационной безопасности.

Литература

1. Вероятностные методы для выявления аномальной активности в компьютерных сетях / А.А. Шевченко [и др.] // Нейрокомпьютеры и их применение: XVII Всероссийская научная конференция, Москва, 19 марта 2019 г. – 2019. – С. 285–287.