## ОБЗОР И АНАЛИЗ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ

О.С. Коваль, В.А.Вишняков

В докладе представлены результаты анализа средств защиты информации в системе управления предприятия, основанные на использовании искусственных нейронных сетей. Рассмотрены основы нейронных сетей, принцип их работы и архитектура. Выделены следующие модели сетей, успешно используемые в задачах защиты информации: многослойный персептрон, рециркуляционная нейронная сеть, нейросетевой детектор.

Угроза информации: обеспечение работоспособности сети и функционирующих в ней информационных систем зависит от способности сети противостоять целенаправленным воздействиям по нарушению ее работы. Данные преднамеренно перехватываются, читаются или изменяются; пользователи идентифицируют себя неправильно (с мошенническими целями); пользователь получает несанкционированный доступ из одной сети в другую. Действия по защите. Обнаружение атак. Методы обнаружения аномалий, методы обнаружения злоупотреблений.

Многослойный персептрон, входные параметры: временные интервалы запросов к объектам компьютерной системы, доступ к файлам, количество процессов, вход/выход пользователей, количество и номенклатура открытых портов, запущенные сетевые службы.

Объединение рециркуляционной нейронной сети и многослойного персептрона. Уменьшение размерности вектора входных данных. Нелинейный репликатор. Нейросетевой детектор. Играет ключевую роль при обнаружении вредоносных программ. После стадий обучения и отбора приобретает способность реагировать на вредоносные программы, сканируя их структуру, и игнорировать чистые файлы.

## ОБЗОР И АНАЛИЗ БЕЗОПАСНОСТИ РАБОТЫ ПОЛЬЗОВАТЕЛЕЙ В КОРПОРАТИВНЫХ СИСТЕМАХ УПРАВЛЕНИЯ

Моздуоани Шираз М.Г., В.А. Вишняков

Традиционные парадигмы безопасности в корпоративных системах управления (КИС) предусматривают уровни защиты по периметру безопасности, такие как межсетевые экраны, системы предотвращения вторжений (Intrusion Prevention Systems − IPS), зашифрованное сетевое туннелирование.

Информационно-ориентированная сеть (Information-Centric Networking — ICN) в последнее время рассматривается как перспективная парадигма для следующего поколения КИС, работающих в Интернете. В ICN контент важнее, чем хост, что дает такие преимущества, как сокращение загрузки сети, низкая задержка распространения, масштабируемость и т.д. Сети, ориентированные на данные (Named Data Networking − NDN) являются представителем ICN архитектуры. В докладе представлены четыре вопроса наиболее важные для безопасности в NDN для защита информации: от новых форм неизвестных атак, обеспечения конфиденциальности, блокировки вредоносного сетевого трафика, обнаружения аномалий и DoS/DDoS атак.

Облачные вычисления (ОВ) используются в КИС из-за экономической эффективности, экономии времени и эффективного использования вычислительных ресурсов. Но вопросы конфиденциальности и безопасности являются одними из основных препятствий, сдерживающих внедрение этой технологии. Рассматривается применение новой технологии − безопасность ориентированная на данные (Data-Centric Networking − DCS), которая обеспечивает владельцев данных полным контролем их безопасности на протяжении всего жизненного цикла данных работы в ОВ.