УДК 004.056

ПРОЕКТИРОВАНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ С ФУНКЦИЕЙ ДЕЦЕНТРАЛИЗОВАННОГО УПРАВЛЕНИЯ ЧЕРЕЗ ПРИЗМУ ДИНАМИЧЕСКОГО МОДЕЛИРОВАНИЯ

Конаков А.М. (ИТМО)

Научный руководитель – доктор технических наук, профессор Лившиц И.И. (ИТМО)

Введение. Проектирование системы защиты информации на основе динамического моделирования заключается в построении некоторого структурного математического объекта (или взаимосвязанных между собой объектов) с «плавающими» исходными данными и представляет собой комплексное решение различных проблем обеспечения информационной безопасности. Такой подход включает в себя создание моделей динамического поведения информационной среды, анализ и оценку угроз и уязвимостей, разработку оптимальных стратегий защиты и реагирования на инциденты [1]. Реализация такой системы защиты требует междисциплинарного подхода, включающего знания в области защиты информации, математического моделирования, анализа данных, а также функциональных возможностей технологий информационной безопасности, их развития и перспектив использования.

Основная часть. Основополагающие принципы подхода заключаются в использовании современных методов анализа и оценки для создания вероятностно - временных моделей, учитывающих динамику изменения информационной среды. Данные модели позволяют оценить вероятность и временной диапазон возникновения определённых негативных событий на основе экспертных оценок, и в соответствии с этим принять соответствующие меры по защите циркулирующей в системе информации ещё до того, как это произойдёт и тем самым нанесёт ущерб [2].

Поведенческие характеристики пользователей системы и злоумышленников играют важную роль в таком подходе, поскольку позволяют учитывать особенности поведения субъектов информационной среды и соответственно, адаптировать стратегии защиты. Например, анализ на основе поведенческих паттернов субъектов, находящихся в поле зрения системы мониторинга, позволяет выявить и оценить несанкционированные действия или аномалии, что позволит своевременно предотвратить утечку информации или атаку на систему.

Децентрализованное управление, как завершающий элемент предлагаемого подхода, позволяет распределить управленческие и технические функции по различным уровням системы защиты информации, что в свою очередь, повышает её гибкость и устойчивость к различного рода атакам [3]. Это также способствует более оперативному реагированию на угрозы и быстрой адаптации к новым условиям и динамически изменяющимся внутренним/внешним факторам информационной среды.

Выводы. Предложен подход к проектированию системы защиты информации с возможностью децентрализованного управления при различных условиях и основанного на динамическом моделировании с уклоном на вероятностно - временные модели и поведенческие паттерны как основополагающие структурные элементы.

Список использованных источников:

1. Курилов, Ф. М. Моделирование систем защиты информации. Приложение теории графов / Ф. М. Курилов. — Текст : непосредственный // Технические науки: теория и практика : материалы III Междунар. науч. конф. (г. Чита, апрель 2016 г.). — Чита : Издательство Молодой ученый, 2016. — С. 6-9.

2. Карганов В. В., Липатников В. А., Дементьев В. Е. Вероятностно-временная модель нарушителя при обеспечении информационной безопасности информационно-вычислительной сети //Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. – 2017. – №. 9-10. – С. 3-7.
3. Дилигенская А.Н., Золотарев В.В., Карпова Н.Е., Селигеев С.В. Децентрализованное управление информационной безопасностью на основе эмерджентного интеллекта в информационных системах // Прикаспийский журнал: управление и высокие технологии. 2023. № 2 (62). С. 42-50.