УДК 004.056

АЛГОРИТМ ОПТИМИЗАЦИИ КОНФИГУРАЦИИ СИСТЕМЫ ЗАЩИТЫ КОРПОРАТИВНЫХ ДАННЫХ

М. А. Филимонова, *магистрант, БГАС*
Научный руководитель – С. И. Половеня, канд. техн. наук, доцент

Резюме – синтезирован алгоритм оптимизации конфигурации системы защиты корпоративных данных, который позволяет оперативно перестраивать систему для предотвращения негативных последствий.

Resume – the algorithm for optimizing the configuration of the corporate data protection system has been synthesized, which allows you to quickly rebuild the system to prevent negative consequences.

Введение. Одним из наиболее значимых классов информационных систем выступают корпоративные информационные системы (КИС) [1].

Как следствие, увеличивается количество сетевых атак, осуществляемых на данные системы. Однако скорость создания новых методов защиты КИС от негативных воздействий не удовлетворяет потребностям рынка. В таком случае оптимальным решением проблемы будет создание системы, которая быстро реагирует и адаптировано подбирает необходимые методы защиты от деструктивных воздействий.

Основная часть. В основе рассматриваемого алгоритма лежит модель системы адаптивной защиты корпоративной информационной системы от деструктивных воздействий (рисунок 1).

Данная модель позволяет в автоматическом режиме обнаруживать и ликвидировать дестабилизирующие информационные влияния на прикладную систему. Принцип действия системы заключается в процессе реконфигурирования, т. е. перестройки блоков системы в зависимости от ситуации, и выборе соответствующего метода защиты.

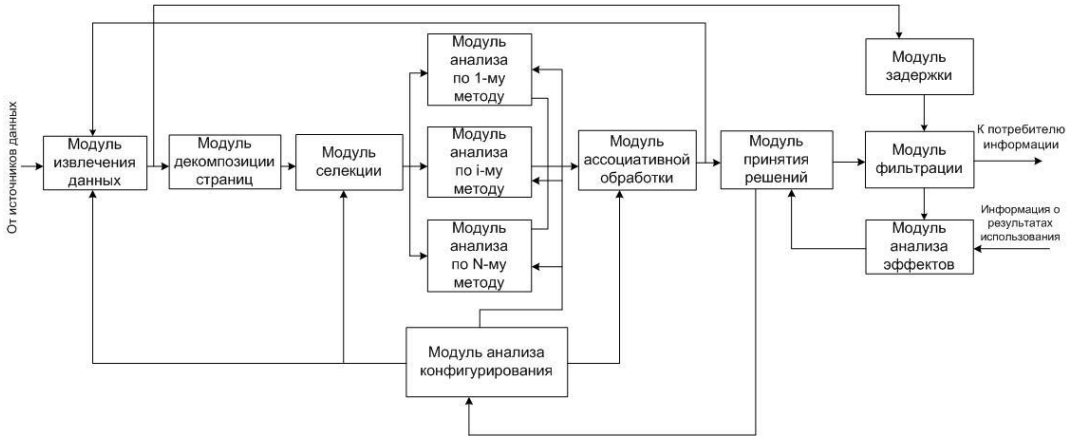

Рисунок 1 – Структурная схема реконфигурирующейся системы

Суть предложенного алгоритма заключается в нахождении подходящей конфигурации и перестройки системы для максимально возможной защиты в данной ситуации. Блок-схема алгоритма представлена на рисунке 2.

При перестройке системы следует принимать во внимание не только текущее состояние системы, но и прогнозы построенных с помощью моделей функционирования систем, защищаемых КИС [2].

Реконфигурирование системы могут осуществлять корректировку процессов обработки данных.

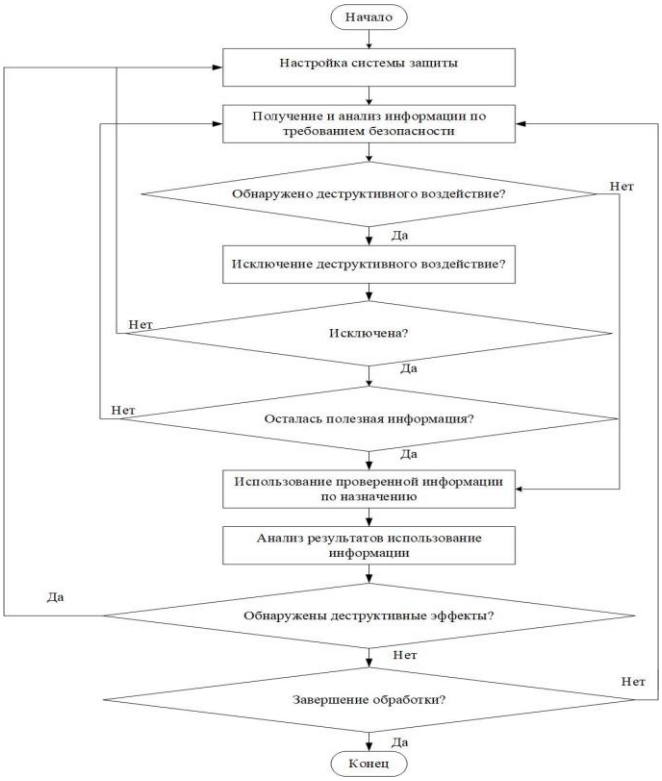

Рисунок 2 – Алгоритм адаптивной защиты от комплексных деструктивных воздействий

Реконфигурирование имеет возможность добавлять и исключать способы обработки информации, а также трансформировать параметры этих способов для увеличения точности обработки информации.

Заключение. Предложен алгоритм оптимизации конфигурации системы защиты корпоративных данных, в основе которого реконфигурирующая модель системы адаптивной защиты. Рассмотренный алгоритм способствует расширению потенциала системы для нахождения и исключения негативных воздействий на систему.

ЛИТЕРАТУРА

1. Осипов, В. Ю. Проблемы защиты от ложной информации в компьютерных сетях / В. Ю. Осипов, В. И. Воробьев, Д. К. Левоневский // Труды СПИИРАН. – 2017. – Вып. 53. – С. 97–117.

2. Осипов, В. Ю. Обоснование мероприятий информационной безопасности / В. Ю. Осипов // Информационно-управляющие системы. – 2013. – № 2. – С. 48–53.