УДК 004.021

ОПРЕДЕЛЕНИЕ ЗАЩИЩЕННОСТИ ОБЛАЧНЫХ СЕРВЕРОВ НА ОСНОВЕ МОДЕЛИРОВАНИЯ МЕХАНИЗМОВ РАСПРОСТРАНЕНИЯ ВИРУСНЫХ ИНФЕКЦИЙ

Житихин А.Е., Менисов А.Б. (Военно-космическая академия имени А. Ф. Можайского),
Казаков М.В. (Институт системного программирования им. В.П. Иванникова Российской академии наук)
Научный руководитель – к.т.н. Менисов А.Б. (Военно-космическая академия имени А. Ф. Можайского)

Аннотация
В докладе рассмотрена задача моделирования состояния защищенности виртуальных серверов облачных технологий. В качестве решения задачи представлен подход к определению состояния защищенности на основе взаимодействия виртуальных машин друг с другом.

Введение
Целью работы является демонстрация уязвимости виртуальных машин к распространению вредоносного программного обеспечения (ПО) внутри макета системы управления инфраструктуры как сервиса. Для решения проблемы уязвимости виртуальных машин к распространению вредоносного ПО применяется множество методов, таких как установка средств антивирусной защиты, средств пресечения компьютерной атаки, средств оповещения и мониторинга, однако на данный момент не существует модели способной учесть состояние иммунитета к компьютерным атакам и состояния проведения компьютерной атаки с машины на локальный хост. Учет этих состояний позволит сократить использование человеческих ресурсов и своевременно принимать меры по пресечению компьютерных атак на технологии облачных вычислений.

Основная часть
А работе рассмотрено конечное множество состояний безопасности виртуальных машин. Выделены состояние чувствительности к компьютерной атаке, частичной уязвимости, слабой уязвимости, зараженной и блокированной виртуальной машины. Так как в системе фиксированное число виртуальных машин, то с течением времени они приобретают разные состояния в соответствии с математической моделью основанной на коэффициентах защищенности. В соответствии с «Методикой оценки угроз безопасности», утвержденной ФСТЭК РФ 5 февраля 2021 года, коэффициенты защищенности определяются исходя из данных каждой виртуальной машины, таких как количество входов, время, прошедшее с момента обновления антивирусной базы данных, наличие/отсутствие систем защиты, появление аномальных действий внутри виртуальной машины.

Выводы
В результате работы была предложена математическая модель, позволяющая учесть все состояния виртуальных машин, для разработки средств защиты информации систем облачных вычислений.