

ОТЗЫВ

на диссертационную работу

Адилжановой Салтанат Альмуханбетовны

на тему: “Методы, модели и информационные технологии для динамического управления ресурсами кибербезопасности”,
представленной на соискание степени доктора философии PhD
по специальности 8D06301 – «Системы информационной безопасности»

Развитие информационной сферы в Республике Казахстан и соответствующий рост ее объемов, и стоимости сопровождается внедрением передовых информационных технологий во все сферы общественной жизни РК, что приводит к увеличению частоты атак и потенциального ущерба от утечек информации. Как результат - усложнение СЗИ и увеличения их стоимости. В этих условиях задача эффективного распределения ограниченных финансовых ресурсов на защиту информации субъектов хозяйственной деятельности становится все более важной, и, в значительной степени, определяет уровень информационной (кибернетической) безопасности государства. Особую актуальность приобретает разработка вопросов оптимизации показателей СЗИ в условиях динамического противостояния с атакующими. Такими показателями могут быть доля потерянной информации, которая определяет эффективность системы защиты, прибыль от внесения инвестиций в защиту информации, их рентабельность и тому подобное.

Одной из основных задач по распределению ограниченных ресурсов стороны защиты является разработка МГА, для решения многокритериальной задачи оптимизации распределения ресурсов стороны защиты в процессе реализации проектов по обеспечению КБ ОБИ. В то же время, одной из важнейших задач, которые может направить сторона (или стороны) нападения с учетом ожидаемой вероятности события; количество ресурсов, необходимых для достаточной защищенности ИР; количество ресурсов, которые может выделить сторона защиты объекта информатизации (ОБИ); допустимый уровень риска потери ИР является дополнить ГА для решения задачи, связанной с подбором и оптимизацией вариантов конфигураций СЗИ для контуров безопасности ИКС. Среди основных задач по обеспечению оптимального перераспределения ресурсов является задача динамического управления ресурсами кибербезопасности, в частности минимизация возможностей хищения ИР, искажения, утраты конфиденциальности, как следствия действий нападающей стороны. В тоже время у атакующих диаметрально противоположные задачи – распределение своих ресурсов таким образом, чтобы минимизировать затраты на получение доступа к информационным ресурсам (ИР) ОБИ.

В процессе подготовки диссертации использовались как общенаучные, так и специальные методы исследования. В работе использованы: аналитические и графические методы, применяемые в оптимизационных задачах исследования операций, в частности методы дробно-линейного и дробно-нелинейного программирования; метод динамического программирования Белмана-Заде – для нахождения оптимальных ресурсов

стороны защиты; эволюционные алгоритмы – для решение многокритериальной оптимизационной задачи распределения ресурсов стороны защиты в процессе реализации проектов по обеспечению КБ ОБИ; методы теории дискретных и непрерывных марковских цепей для определения состояний КБ ОБИ. Для математического моделирования использованы пакеты приложений – MathLab, MathCAD, а также парадигма ООП. Применялся также графический метод – для наглядного представления материалов диссертации.

Дополнена методика выбора целевой функции модели, описывающей причиненный ущерб от реализации угроз и уязвимость информационных ресурсов ОБИ, которая в отличие от существующих решений, обосновывает выбор дробно-нелинейных функций, отражающих свойства информации, циркулирующей в компьютерных системах, где для преодоления препятствия нужно потратить значительные ресурсы; впервые разработан МГА который в отличие от существующих, позволяет упростить решение многокритериальной оптимизационной задачи распределения ресурсов стороны защиты в процессе реализации проектов по обеспечению КБ ОБИ, что дает возможность оптимизировать распределение ресурсов на работы, связанные с мероприятиями, направленными на снижение уязвимостей компонентов в составе ОБИ и промоделировать разные варианты объемов ресурсов, обеспечивающих достижение заданных значений защищенности ОБИ в условиях отсутствия данных о ресурсах атакующей стороны; получил дальнейшее развитие ГА для решения задачи, связанной с подбором и оптимизацией вариантов конфигураций СЗИ для контуров безопасности ИКС, который в отличие от существующих решений в качестве критерия для оптимизации состава СЗИ использует суммарную величину рисков от потери информации, интегральные показатели СЗИ, а также стоимостные показатели для каждого класс СЗИ.

Диссертационная работа является законченным научным исследованием и содержит ценные научные результаты, которые опубликованы в печати.

Фактическое внедрение и применение результатов, полученных в ходе диссертационного исследования, подтверждено соответствующими актами о внедрении.

Считаю, что диссертационная работа Адилжановой Салтанат Альмуханбетовны на тему “Методы, модели и информационные технологии для динамического управления ресурсами кибербезопасности”, выполнена на высоком уровне, удовлетворяют требованиям, предъявляемым к докторской диссертации на соискание степени доктора философии (PhD) по специальности 8D06301 – «Системы информационной безопасности», а ее автор заслуживает присуждение степени доктора философии PhD.

Научный консультант,
Доктор технических наук, профессор

Лахно В.А.

