

1. Проведен анализ процесса обеспечения информационной безопасности КИС от КДВ и разработка на его основе математической модели КИС как объекта защиты в условиях информационных угроз.

2. Разработан метод оценивания эффективности функционирования КИС в условиях КДВ.

3. Разработан метод адаптивной защиты КИС от информационных угроз.

4. Разработана архитектура программной среды адаптивной защиты КИС от информационных угроз.

5. Разработаны рекомендации по повышению эффективности защиты КИС от КДВ.

Научная новизна полученных результатов.

Научная новизна результатов диссертационной работы заключается в том, что диссертантом впервые разработаны и получены:

1) Математическая модель КИС, функционирующей в условиях КДВ, отличающихся новым пространством состояний и множеством переходов между ними.

2) Метод оценивания эффективности функционирования КИС с использованием предложенной математической модели, отличающийся новым показателем эффективности КИС и правилами его расчета, которые расширяют возможности оценивания влияния информационных угроз на функционирование системы.

3) Метод адаптивной защиты КИС от информационных угроз.

4) Архитектура системы адаптивной защиты КИС от КДВ, которая отличается новой совокупностью связанных блоков сбора, предобработки и анализа данных и выбора контрмер для защиты от сетевых атак.

5) Запатентованные способы и средства, отличающиеся принципиально новыми последовательностями действий по обоснованию и реализации мероприятий защиты, позволяющие повысить эффективность функционирования КИС.

Научная значимость заключается в том, что полученные результаты вносят вклад в развитие научно-методического аппарата оценивания эффективности и обоснования мероприятий защиты КИС от КДВ.

Практическая значимость подтверждается тем, что полученные результаты позволили усовершенствовать систему защиты КИС и повысить эффективность ее функционирования.

Достоверность и обоснованность работы, выводов и предложений по ней подтверждается:

успешной апробацией на семинарах, всероссийских и международных конференциях, тематика которых совпадает с предметной областью исследований;

непротиворечивостью обоснованных выводов и результатов вычислительных экспериментов (при оценивании показателей качества в рамках предлагаемого метода).

По материалам автореферата необходимо сделать следующие замечания:

1. Из автореферата остается неясным, как осуществляется переход между состояниями процесса функционирования КИС $S_1 \rightarrow S_2 \rightarrow S_3 \rightarrow \dots \rightarrow S_{10}$ (нет признаков и правил).

2. В автореферате не представлен набор правил адаптивной конфигурации системы защиты КИС.

3. Автор не указывает, какие именно величины он использует в качестве базовых для расчёта эффективности функционирования КИС.

4. Присутствуют незначительные погрешности в оформлении: наличие некорректной ссылки [65] на странице 9, очень мелкий шрифт на рисунке 2.

Указанные замечания не снижают общей ценности диссертационной работы и не влияют на основные научные и практические результаты диссертации.

Полученные автором результаты достоверны, выводы и заключения обоснованы.

Выводы:

1. В целом, судя по автореферату и публикациям, диссертация Левоневского Д.К., выполненная на тему: «Методы и модели защиты корпоративных информационных систем от комплексных деструктивных воздействий» представляет собой самостоятельную научно-квалификационную работу, в которой поставлена и решена актуальная научная задача по повышению эффективности защиты КИС от КДВ за счет разработки методов и моделей адаптивной защиты этих систем от таких воздействий.

2. Работа соответствует требованиям Положения о присуждения ученых степеней, предъявляемым к диссертациям на соискание ученой степени кандидата технических наук, а её автор заслуживает присуждения ученой степени кандидата технических наук по специальности 05.03.19 – «Методы и системы защиты информации, информационная безопасность».

Отзыв обсужден и одобрен на заседании 61 кафедры Военно-космической академии имени А.Ф. Можайского 10 марта 2020 г., протокол № 20.

Начальник 61 кафедры
доктор технических наук, доцент
полковник

Д.Бирюков

Преподаватель 61 кафедры
кандидат технических наук
майор

В.Данилов

Адъюнкт 61 кафедры
капитан

М.Беляков

Сведения о составителях отзыва:

Бирюков Денис Николаевич
доктор технических наук, доцент,
полковник, начальник 61 кафедры
ФГБВОУ ВО ВКА им. А. Ф. Можайского
197198, г. Санкт-Петербург, ул. Ждановская, д. 13
Тел.: 8 (812) 347-97-70
E-mail: vka@mil.ru

Данилов Виталий Валерьевич
кандидат технических наук,
майор, преподаватель 61 кафедры
ФГБВОУ ВО ВКА им. А. Ф. Можайского
197198, г. Санкт-Петербург, ул. Ждановская, д. 13
Тел.: 8 (812) 347-97-70
E-mail: vka@mil.ru

Беляков Максим Игоревич
капитан, адъюнкт 61 кафедры
ФГБВОУ ВО ВКА им. А. Ф. Можайского
197198, г. Санкт-Петербург, ул. Ждановская, д. 13
Тел.: 8 (812) 347-97-70
E-mail: vka@mil.ru