ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА
на диссертационную работу Корнева Дмитрия Александровича «Разработка и исследование средств взаимодействия приложений и методов защиты вычислительного комплекса транспортной системы», представленную на соискание ученой степени кандидата технических наук по специальности 05.13.15 – «Вычислительные машины, комплексы и компьютерные сети»

Повышение безопасности транспорта, в том числе и железнодорожного, является актуальным и постоянно осуществляемым процессом. Для контроля железнодорожных перевозок внедряются различные информационные системы, которые помогают или в некоторых случаях заменяют диспетчера. Использование информационных систем для управления железнодорожными составами позволяет снизить влияние человеческого фактора и связанных с ним ошибок. Однако такая автоматизация наряду с преимуществами имеет и недостатки. Информационные системы управления железнодорожным транспортом, как и другие информационные системы, могут использоваться злоумышленниками для достижения их целей. Поэтому другой актуальной проблемой является повышение информационной безопасности этих систем, от которых зависят жизни тысяч пассажиров. В связи с этим считаю тему диссертационной работы Корнева Дмитрия Александровича актуальной.

Диссертация состоит из введения, 4 глав, заключения, списка литературы, содержащего 196 наименований, и двух приложений.

В первой главе описана структура системы диспетчерской централизации и системы автоведения локомотива. Предложено с целью интеграции системы автоведения локомотива в систему диспетчерской централизации ввести дополнительный вычислительный комплекс, с помощью которого осуществляется взаимодействие этих систем при рациональном использовании вычислительных ресурсов. Задачами вычислительного комплекса является прием, обработка и передача оперативных данных между локальной вычислительной сетью диспетчерской централизации и системами автоведения локомотивов, находящихся на участке железной дороги.

Во второй главе разработана математическая модель вычислительного комплекса. Функционирование модели описано в терминах сетей Петри. Проведено моделирование функционирования вычислительного комплекса при получении запроса от системы автоведения локомотива и моделирование функционирования вычислительного комплекса при взаимодействии виртуальных машин с ресурсом при управлении локомотивом. Верификация модели вычислительного комплекса выполнялась в двух режимах работы комплексной системы управления движением поездов: при минимальной и максимальной нагрузке. Проведены расчеты оптимальной длины участка, на котором ресурсы вычислительного комплекса будут использоваться наиболее эффективно.

В третьей главе рассмотрены способы резервирования вычислительного комплекса. Сделан вывод о целесообразности использования мажоритарного резервирования с голосованием «2 из 3». Предложена модель передачи данных между вычислительным комплексом и ресурсом. Модель описана сетями Петри; приведена система логических уравнений, описывающих сеть. Смоделированы процессы, происходящие при MITM-атаке. На основе методики Б. Шнайера определены маршруты возможных атак на вычислительный комплекс.

В четвертой главе разработаны математическая модель, описывающая динамические процессы в информационной системе с шифрованной информацией при проведении атаки, и методика определения количественных показателей эффективности защиты вычислительного комплекса на основе метода Монте-Карло с учетом структуры дерева атак. Данная методика позволила сравнить эффективность различных систем защиты и сделать выбор системы защиты для разработанного вычислительного комплекса.

Наиболее интересным в работе является использование сетей Петри для описания моделируемых процессов.

Степень обоснованности научных положений, выводов и рекомендаций

Разработанная структура вычислительного комплекса и его взаимодействие с участниками перевозочного процесса обоснованы практической реализацией системы автоведения современных локомотивов.

Модель функционирования вычислительного комплекса, разработанная автором, корректна, поскольку базируется на алгоритме работы системы автоведения поезда с учетом информации, получаемой от системы диспетчерской централизации, и использует математический аппарат сетей Петри, позволяющий адекватно описывать дискретные процессы работы сложных систем.

Для выбора типа защиты вычислительного комплекса в работе разработано дерево возможных алгоритмов атак, которое учитывает виртуальную структуру вычислительного комплекса и существующую закрытую реализацию системы связи, используемую для передачи информации по сети железных дорог. Математическая модель атаки, представленная автором в третьей главе, соответствует ее практической реализации и базируется на известных алгоритмах.

Разработанная методика расчета вероятности доступа к ресурсу вычислительного комплекса в результате проведения информационных атак базируется на теоретически подтвержденном методе Монте-Карло и учитывает характеристики параметров атак. Это позволило автору получить теоретически обоснованный результат по эффективности применения различных типов защит и предложить подтвержденные рекомендации по обеспечению защиты высокого уровня для вычислительного комплекса системы управления движением поездов.

Ряд теоретических результатов нашли в работе практическое обоснование, в частности результаты моделирования разворачивания виртуальной машины на базе резерва вычислительного комплекса.

Достоверность и новизна научных положений, выводов и рекомендаций

Новыми научными положениями диссертации являются:

1. Структура комплексной системы управления движением поездов как единого информационно-коммуникационного пространства, вычислительный комплекс которой обеспечивает высокий уровень

взаимодействия участников перевозочного процесса для возможности повышения эффективности работы железнодорожного транспорта.

2. Разработанные модели функционирования вычислительного комплекса и MITM-атаки на вычислительный комплекс с использованием математического аппарата сетей Петри. Эти модели образуют комплексную модель работы системы как в нормальном режиме, так и во внештатных ситуациях – при внезапных отказах элементов вычислительного комплекса и при проведении атаки на систему.

3. Разработанный вероятностный метод, позволяющий определить количественные показатели эффективности применяемой защиты при различных алгоритмах и параметрах атак для вычислительного комплекса заданной структуры.

Перечисленные научные положения получили в диссертации глубокую проработку.

Достоверность научных положений основывается на теоретически обоснованных результатах и данных экспериментальных исследований, в частности, полученных при определении времени разворачивания элементов вычислительного комплекса.

В теоретических основах диссертации используются положения теории вероятностей и математической статистики, математический аппарат расширенных сетей Петри.

Достоверность экспериментальных данных обеспечивается использованием современных средств и методик проведения исследований.

Автореферат полно и объективно отражает содержание диссертации.

Содержание диссертации полно представлено в двенадцати публикациях, пять из которых опубликованы в изданиях, рекомендованных ВАК Минобрнауки России.

По диссертационной работе имеются следующие замечания

1. Во второй главе была получена оптимальная длина участка железной дороги, обслуживаемая вычислительным комплексом. Однако в главе не указано, как полученный результат соотносится с длиной участка дороги, обслуживаемой системой диспетчерской централизации, так как именно данные, поступающие на вычислительный комплекс от системы

диспетчерской централизации, определяют взаимодействие участников перевозочного процесса.

2. Во второй, третьей и четвертых главах для моделирования процессов предложены сети Петри, имеющие сложную структуру и большое количество узлов и переходов. Следовало бы привести примеры функционирования, показав соответствие процессам, описываемым этими сетями.

3. Третья глава изобилует терминами, связанными с информационной безопасностью, (MITM-атака, сниффер, фишинг). Для понятности изложения необходимо было привести определения данных терминов и пояснения.

Отмеченные замечания в целом не снижают высокого качества проведенного диссертационного исследования.

Заключение

1. Принимая во внимание актуальность темы диссертации, научную новизну и практическую значимость ее результатов, считаю, что диссертационная работа «Разработка и исследование средств взаимодействия приложений и методов защиты вычислительного комплекса транспортной системы» является законченной научно-квалификационной работой, в которой содержится новое решение задачи по совершенствованию методов взаимодействия участников перевозочного процесса на сети железных дорог, имеющей существенное значение для повышения эффективности работы железнодорожного транспорта.

2. Работа выполнена на высоком уровне, имеет элементы новизны, характеризуется теоретической и практической значимостью, удовлетворяет требованиям ВАК РФ, предъявляемым к кандидатским диссертациям, и соответствует паспорту специальности 05.13.15 – «Вычислительные машины, комплексы и компьютерные сети».

3. Автор диссертации Корнев Дмитрий Александрович заслуживает присуждения ему ученой степени кандидата технических наук по специальности 05.13.15 – «Вычислительные машины, комплексы и компьютерные сети».

Доцент кафедры «Вычислительная
и прикладная математика»
ФГБОУ ВПО «Рязанский государственный
радиотехнический университет»,
кандидат технических наук,
доцент Пруцков Александр Викторович
02. 04. 2015 г.

Адрес: 390005, г. Рязань, ул. Гагарина, д. 59/1, Рязанский государственный радиотехнический университет, кафедра «Вычислительная и прикладная математика»
Рабочий телефон: (4912) 46-03-64
Электронная почта: mail@prutzkow.com

Подпись Пруцкова Александра Викторовича удостоверяю
Секретарь ученого совета
ФГБОУ ВПО «Рязанский государственный
радиотехнический университет»,
заведующий кафедрой «Информационная безопасность»
ФГБОУ ВПО «Рязанский государственный
радиотехнический университет»,
кандидат технических наук,
доцент Пржегорлинский Виктор Николаевич

Адрес: 390005, г. Рязань, ул. Гагарина, д. 59/1, Рязанский государственный радиотехнический университет, кафедра «Информационная безопасность»
Рабочий телефон: (4912) 46-03-64