ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА
доктора технических наук, старшего научного сотрудника
Емелина Вадима Ивановича
на тему "Управление безопасностью мобильных абонентских устройств в корпоративных сетях", представленную на соискание ученой степени кандидата технических наук по специальности 05.13.19 – "Методы и системы защиты информации, информационная безопасность"

Актуальность темы диссертации

В современных защищенных корпоративных сетях в настоящее время очень остро стоит вопрос допустимости и безопасности использования их пользователями единого мобильного абонентского устройства (МАУ) к услугам с разными требованиями по защищенности. Современные МАУ обладают серьезными вычислительными и коммуникационными возможностями, однако существующие системы и средства защиты информации (СЗИ) не позволяют достаточно эффективно обеспечивать информационную безопасность при использовании подобных устройств для защищенного доступа к услугам сетей с разными требованиями по защищенности. В связи с этим диссертационная работа Маркина Дмитрия Олеговича на тему "Управление безопасностью мобильных абонентских устройств в корпоративных сетях", целью которой является как раз повышение результативности защиты информации при доступе к услугам связи и информации в сетях с разными требованиями по защищенности при использовании единого МАУ, является актуальной, имеющей важное значение для развития отрасли знаний в области вопросов обеспечения информационной безопасности.

Основные результаты

В работе проведен детальный анализ современного состояния научных исследований и технических решений в области защиты информации при эксплуатации МАУ. Выявлены основные особенности МАУ, влияющие на защищенность доступа, условия функционирования МАУ в корпоративных сетях с различными требованиями по защищенности и требования, предъявляемые к ним. Предложена модель угроз и нарушителя безопасности информации. На основе проведенного в работе анализа сделан вывод, что основной проблемой, требующей решения для повышения результативности защиты информации при работе с МАУ, является необходимость учета местоположения МАУ в помещениях внутри здания и необходимости удаленного автоматического управления программно-аппаратной конфигурацией МАУ, позволяющего гарантировано обеспечить перевод МАУ в состояния, отвечающее требованиям безопасности для текущих условий осуществления доступа.

Для разрешения данного противоречия автором получены следующие результаты:

1. Предложена модель безопасности мобильного абонентского устройства в корпоративных сетях с разными требованиями по защищенности, и обоснована ее корректность.

2. Разработан алгоритм управления безопасностью мобильного абонентского устройства, позволяющий определить оптимальную программно-аппаратную конфигурацию устройства с учетом атрибутов доступа и требований по безопасности и качеству услуг, проведена оценка его свойств, доказана его эффективность.

3. Разработана система управления безопасностью МАУ, отличающаяся возможностью удаленного управления программно-аппаратной конфигурацией МАУ в зависимости от условий доступа, требований политик безопасности и качества предоставляемых услуг для обеспечения защищенного доступа к инфокоммуникационным услугам и информации корпоративных сетей с разными требованиями по защищенности.

Полученные результаты позволяют получить положительный эффект в виде повышения вероятности обеспечения безопасности информации при доступе к

инфокоммуникационным услугам и информации в корпоративных сетях с разными требованиями по защищенности при использовании единого МАУ.

Степень обоснованности научных положений, выводов и рекомендаций

Содержание диссертации и полученные результаты соответствуют пунктам паспорта научной специальности 05.13.19 "Методы и системы защиты информации, информационная безопасность" (технические науки) в части: п.2. Методы, аппаратно-программные и организационные средства защиты систем (объектов) формирования и предоставления пользователям информационных ресурсов различного вида, п.8. Модели противодействия угрозам нарушения информационной безопасности для любого вида информационных систем, п.13. Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности.

В целом обоснованность научных результатов обеспечивается:

- корректным применением апробированного математического аппарата: теории вероятностей, математической статистики, интеллектуального анализа данных и теории оптимизации;
- корректностью постановок решаемых задач, вводимых допущений и ограничений, формулировок и выводов;
- положительными результатами их использования и внедрения;
- апробацией результатов на всероссийских конференциях и опубликовании в рецензируемых научных изданиях, рекомендованных ВАК при Минобрнауки России.

Научная новизна и достоверность результатов

Научная новизна полученных результатов заключается в обосновании на основе теории множеств и конечных автоматов корректности предложенной модели безопасности мобильного абонентского устройства, позволяющего учитывать условия доступа к сетям корпоративных сетей с разными требованиями по защищенности, включая местоположение и другие атрибуты;

разработке нового технологического решения на основе метода статистических испытаний, позволяющего повысить достоверность определения местоположения МАУ в помещениях с разными требованиями по защищенности;

разработке рекомендаций по формированию оптимальных параметров системы определения местоположения МАУ, основанной на использовании сигналов беспроводных сетей передачи данных, позволяющих повысить достоверность вычисления его местонахождения в специальных помещениях

и подтверждается, в том числе, тремя патентами на изобретения.

Достоверность результатов работы и выводов подтверждается:

- непротиворечивостью полученных теоретических результатов ранее известным экспериментальным данным, данным предшествующих исследований в области определения местоположения МАУ в помещениях внутри здания;
- достаточно большим объемом статистического материала, полученного в рамках исследования в имитационной модели системы определения местоположения МАУ и управления его конфигурацией;
- актами внедрения, подтверждающими эффективность полученных результатов.

Теоретическая и практическая значимость результатов

Теоретическая значимость работы состоит в разработке формального аппарата моделирования безопасности МАУ в корпоративных сетях с учетом его местоположения в специальных помещениях, формализации алгоритма управления программно-аппаратной конфигурацией МАУ на основе метода целочисленного динамического программирования.

Практическая значимость работы обусловлена доведением разработанных алгоритмов до комплекса программных средств для ЭВМ, в том числе, на основе архитектуры ARM, и возможностью их практического применения при разработке систем

определения местоположения МАУ в помещениях внутри зданий, а также систем управления безопасностью МАУ для предоставления доступа к услугам сетей с различными требованиями по защищенности.

Полнота публикаций научных результатов

Анализ полноты содержания диссертации позволяет утверждать, что диссертация Маркина Д. О. является завершенной научно-квалификационной работой, имеет внутреннее единство и логическую взаимосвязь изложения материала, написана грамотным научным языком и свидетельствует о личном вкладе автора в науку.

Представленная работа имеет законченный характер, уровень проведенных исследований является высоким, а полученные результаты полезны для науки и практики. Автором проведен достаточный анализ известных результатов, полученных другими исследователями в данной области, о чем свидетельствует список использованных источников (150 наименований).

Диссертация написана автором единолично, в достаточной степени опубликована и апробирована. Результаты диссертационной работы изложены в 8 изданиях, рекомендованных ВАК при Минобрнауки России для публикации основных научных результатов диссертаций на соискание ученых степеней кандидата и доктора наук ("Вопросы кибербезопасности", "Телекоммуникации", "Информационные технологии", "Вестник РГРТУ", "Известия ТулГУ", "Промышленные АСУ и контроллеры", "Проблемы информационной безопасности. Компьютерные системы"), что в полной степени соответствует п. 13 "Положения о присуждении ученых степеней".

Содержание автореферата достаточно полно отражает основные научные результаты, изложенные в диссертации. Автореферат оформлен в соответствии с требованиями. Стиль изложения материала в автореферате позволяет ясно представить сформулированные в диссертации задачи исследования, основное содержание и идеи работы, а также выводы и рекомендации.

Замечания

К основным недостаткам диссертационной работы необходимо отнести следующие:

1. При доказательстве корректности предложенной формальной модели безопасности МАУ не в полной мере учитываются возможные факторы, оказывающие воздействие на безопасность информации. В частности, не учитываются возможности нарушителя по внедрению программно-аппаратных закладок на этапе проектирования и разработки аппаратной составляющей МАУ, использование уязвимостей программного обеспечение и других, что не позволяет гарантировать защищенность мобильной платформы от угроз утечки информации.

2. Согласно формальной постановке задачи в соответствии с выражением (1.2) достижение цели исследования обеспечивается выполнением критерия превосходства для показателя вероятности обеспечения безопасности информации по сравнению с требуемой величиной, при этом значения требуемой величины, не уточняется.

3. При оценивании качества разработанной модели и эффективности полученных результатов приведены данные (таблица 2.14), указывающие на снижение вероятности ошибок 2-го при определении местоположения МАУ до уровня 1% и менее. При этом не приводятся нормативные значения для данного показателя и, в то же время, ошибка 2-го рода, равная 1%, соответствующая вероятности утечки информации, для ряда систем обеспечения информации является недопустимой.

4. В работе не рассматриваются вопросы обеспечения целостности информации. Учитывая, что по ГОСТ Р ИСО/МЭК 17799 – 2005 целостность определяется как достоверность и полнота информации, а также методов ее обработки, необходимо дополнить модель угроз и нарушителя ИБ, представленную на рис. 1.6, описанием взаимосвязей между процессами обеспечением целостности и НСД к информации в соответствии с темой диссертационной работы.

5. Обеспечение доступности информации в работе предлагается оценивать по показателю своевременности обработки запросов на доступ к услугам и ресурсам корпоративных сетей с разными требованиями по защищенности на основе требований ГОСТ РВ 51987–2002, что не позволит в полном объеме провести такую оценку при расширении пространства угроз, уязвимостей и реализующих их воздействий.

Однако указанные недостатки в определенной степени показывают направления дальнейших исследований автора и не снижают теоретической и практической значимости полученных результатов.

Заключение по диссертации в целом

Диссертация Маркина Д. О. является законченной научно-квалификационной работой, выполненной самостоятельно на высоком научном уровне. В работе решена актуальная и новая научно-техническая задача и получены результаты, имеющие существенное значение для повышения эффективности обеспечения безопасности информации при использовании единого мобильного абонентского устройства при доступе к услугам корпоративных сетей с разными требованиями по защищенности. Полученные результаты строго аргументированы, критически оценены по сравнению с другими известными решениями. По каждой главе и полученным результатом приведены обоснованные выводы, подкрепляемые, в том числе, численным обоснованием и примерами расчетов. Автореферат соответствует основному содержанию диссертации.

Диссертация отвечает требованиям Положения "О порядке присуждения ученых степеней", утвержденного постановлением Правительства Российской Федерации от 24.09.2013 года № 842 в редакции от 28.08.2017 года, предъявляемым к кандидатским диссертациям, а ее автор Маркин Дмитрий Олегович, заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 – "Методы и системы защиты информации, информационная безопасность".

Официальный оппонент
Доктор технических наук, старший научный сотрудн

"18" мая 2018 г. З. И. Емелин

Подпись Емелина Вадима Ивановича ЗАВЕРЯЮ.
Начальник отдела кадров АО "НИИ "Вектор" А. Валькова

"18" мая 2018 г.

Сведения о составителе отзыва:
Емелин Вадим Иванович
Доктор технических наук
Старший научный сотрудник
Место работы: Акционерное общество "Научно-исследовательский институт "Вектор", научно-технический отдел (Санкт-Петербург).
Должность: главный научный сотрудник.
Почтовый адрес: Россия, 197342, Санкт-Петербург, Кантемировская улица, д. 10.
Телефон: +7 (812) 295-10-97.
Адрес электронной почты: emelin0841@yandex.ru