ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

доктора технических наук, доцента

Мошака Николая Николаевича

на диссертационную работу Маркин Дмитрия Олеговича

по теме "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

Защита информационных ресурсов в корпоративной сети от несанкционированного доступа (НСД) является сложной проблемой и требует, как правило, комплексного применения различных механизмов защиты на нескольких логических уровнях ее архитектуры. Эта задача особенно усложняется в отношении организации защищенного удаленного доступа к информационным ресурсам сети различного уровня конфиденциальности современных мобильных абонентских устройств (МАУ), к которым относятся смартфоны, планшетные компьютеры, ноутбуки и т. п., что требует применения соответствующих средств защиты информации (СЗИ) с использованием адаптивного механизма настройки информационной безопасности. В настоящее время отсутствуют эффективные средства защиты информации для МАУ, позволяющие обеспечить организацию такого доступа с учетом определения нахождения МАУ в защищенных помещениях. В этой связи разработка моделей безопасности МАУ и эффективных СЗИ с учетом ограниченных вычислительных ресурсов этих устройств, позволяющих обеспечивать у правляемый защищенный доступ пользователей с единого МАУ к информационным ресурсам корпоративной сети, является

актуальной задачей, которой и посвящено диссертационное исследование соискателя.

Степень обоснованности научных положений выводов и рекомендаций

Тема диссертационной работы и полученные в ходе исследования результаты соответствуют пунктам 2, 8 и 13 паспорта специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность». Основные научные положения, приведённые в автореферате и вынесенные на защиту, а также выводы и результаты диссертационного исследования обоснованы и аргументированы. Обоснованность и достоверность научных положений, выводов и результатов диссертации обеспечивается корректностью используемых математических выражений, апробацией результатов диссертационной работы на международных и всероссийских конференциях. Работа в достаточной степени структурирована, в конце каждой главы присутствуют выводы, которые отражают поставленные в начале каждой главы цели.

Основные результаты

1. Модель безопасности мобильного абонентского устройства в корпоративных сетях с разными требованиями по защищенности.
2. Алгоритм управления безопасностью мобильного абонентского устройства, позволяющий определить оптимальную программно-аппаратную конфигурацию устройства с учетом атрибутов доступа и требований по безопасности и качеству услуг.
3. Система управления безопасностью мобильных абонентских устройств, обеспечивающая повышение вероятности обеспечения безопасности информации при доступе к инфокоммуникационным услугам и информации корпоративных

сетей с разными требованиями по защищенности при использовании единого МАУ.

Научная новизна и достоверность результатов

Научная новизна полученных результатов заключается в

- разработке модели безопасности МАУ, отличающейся от известных учетом его местонахождения в корпоративных сетях с разными требованиями по защищенности, обоснована ее корректность;

- разработке технологического решения, позволяющего повысить достоверность определения местоположения МАУ в помещениях с разными требованиями по защищенности за счет применения метода статистических испытаний;

- разработке алгоритма управления безопасностью МАУ, отличающегося от известного определения оптимальной с точки зрения обеспечения конфиденциальности информации и качества предоставляемых пользователю услуг программно-аппаратной конфигурации МАУ с учетом вероятности его нахождения в специальных помещениях и других атрибутов доступа.

- разработке системы управления безопасностью МАУ, отличающейся 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.

Достоверность полученных результатов подтверждается подробным анализом условий функционирования исследуемой системы, корректным и обоснованным выбором допущений и ограничений, проведением достаточного количества как натурных экспериментов, так и имитационного моделирования, подтверждающего основные выводы работы, а также использованием апробированного научно-методологического аппарата и достаточной полнотой

опубликования результатов в рецензируемых научных изданиях.

Новизна полученных автором решений также подтверждается тремя патентами на изобретения и шестью свидетельствами об официальной регистрации программ для ЭВМ.

Теоретическая и практическая значимость результатов исследования

Теоретическая значимость работы состоит в разработке новой модели безопасности мобильных устройств и доказательстве ее корректности на основе теории множеств и конечных автоматов, а также решения задачи вычисления вероятности местонахождения МАУ в специализированных помещениях с использованием метода статистических испытаний.

Практическая значимость работы обусловлена разработкой комплекса программных средств на основе предложенной модели и алгоритмов, который может быть применен при проектировании перспективных систем управления безопасностью МАУ в защищенных корпоративных сетях, а также полученными конкретными практическими результатами, подтверждаемыми актами внедрения в практических подразделениях ФСО и ФСТЭК России.

Степень обоснованности научных положений, выводов и рекомендаций

Обоснованность научных результатов обеспечена тем, что автором на достаточно высоком научном уровне используются различные подходы и методы обоснования полученных результатов, выводов и рекомендаций, изучаются и критически анализируются известные достижения, теоретические положения и технологические решения в области защиты информации при эксплуатации МАУ. Апробированный математический аппарат: теория вероятностей и математическая статистика, теории машинного обучения, управления, алгоритмов и оптимизации,

оценивания, а также численные методы и имитационное моделирование применяются в работе корректно. Формальные постановки задачи диссертационного исследования, а также задач на разработку модели и алгоритма, также осуществлены корректно с введением необходимых допущений и ограничений. Положительные результаты их решения обоснованы и подтверждены численными примерами, согласующимися с теорией и результатами известных решений в данной области, что подтверждает их достоверность.

Содержание диссертации и полученные результаты соответствуют соответствует пунктам 2, 8 и 13 паспорта научной специальности 05.13.19 "Методы и системы защиты информации, информационная безопасность" (технические науки).

Научная новизна и достоверность результатов

Научная новизна представленных результатов состоит в обосновании корректности предложенной формальной модели безопасности, отличающейся от известных учетом оценки его местонахождения в специальном помещении, других атрибутов доступа, а также реализацией требований мандатной и ролевой политик безопасности в корпоративных сетях с разными требованиями в отношении единого МАУ, а также разработке нового способа определения помещения, в котором находится мобильный пользователь, в условиях высокой погрешности определения местоположения известными методами на основе сигналов беспроводных сетей.

Достоверность полученных результатов подтверждается подробным анализом условий функционирования исследуемой системы, корректным и обоснованным выбором допущений и ограничений, проведением достаточного количества как натурных экспериментов, так и имитационного моделирования, подтверждающего основные выводы работы, а также использованием

апробированного научно-методологического аппарата и достаточной полнотой опубликования результатов в рецензируемых научных изданиях.

Новизна полученных автором решений также подтверждается тремя патентами на изобретения и шестью свидетельствами об официальной регистрации программ для ЭВМ.

Полнота публикаций научных результатов

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, достаточно 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, что в полной степени соответствует п. 13 «Положения о присуждении учёных степеней».

Содержание автореферата отражает суть диссертационной работы и позволяет достаточно ясно оценить основные полученные результаты и степень их обоснованности и достоверности.

Замечания

1. В диссертационной работе в качестве моделей угроз и нарушителя акцент делается на внутреннем нарушителе и недостаточно обоснован отказ от внешнего нарушителя. В связи с этим не учитывается ряд принципиальных факторов, в том числе, активных воздействий внешнего нарушителя, способных привести к нарушению режима ИБ в условиях функционирования предлагаемой системе и других. Данное обстоятельство ограничивает применения полученных решений в

ряде существующих современных защищенных сетях.

2. В диссертационной работе обосновывается применения технологий беспроводных сетей доступа в качестве основы для определения местоположения мобильных устройств и недостаточно корректно проведен сравнительный анализ с другими возможными способами решения данной задачи, например, с технологиями на основе радиочастотных меток (RFID) и технологий сотовой связи, применение которых может быть в ряде случаев экономически более оправдано.

3. При решении оптимизационной управления безопасностью МАУ (формула 3.4) недостаточно обосновано использование только одного параметра QoS - информационной скорости в беспроводном канале доступа (норматив информационной скорости для *i*-й услуги в беспроводном радиоканале между *l*-м МАУ и *m*-й точной доступа; оценочная максимально возможная информационная скорость в беспроводном радиоканале между *l*-м МАУ и *m*-й точной доступа). Не учитывается ряд параметров QoS, специфических для отдельных информационных услуг, таких как речь и видео.

4. Не обоснован выбор неполной гамма-функции в выражении вероятности предоставления информации или услуг (формула 1.5, стр.51).

5. Не обосновано почему вероятность НСД к информации при условии корректно заданной политики безопасности, будет определяться величиной вероятности ошибки 2-го рода при определении местоположения МАУ (формула 1.8, стр.52).

6. Не обосновано почему дополнительно новое свойство системы защиты - *as* – свойство атрибутной безопасности (attribute security) – позволяет повысить адекватность формальной модели условиям эксплуатации компьютерной системы с МАУ (стр.67).

7. Введенные в работе ограничения и допущения в условиях современного уровня импортозамещения элементной базы и доверенных программно-

аппаратных платформ, особенно мобильных, делает предложенные технические решения практически не применимыми к реальным условиям эксплуатации в сетях с достаточно высокими требованиями по защищенности.

Заключение по диссертации в целом

В диссертационной работе Маркина Д. О. изложено решение актуальной научной задачи разработки модели безопасности МАУ, базирующаяся на классической модели Белла-ЛаПадулы, элементах ролевой и атрибутной моделях управления доступом, а также и моделях безопасности, учитывающих местоположение субъектов, и алгоритма управления безопасностью МАУ, на основе которых построена система управления безопасностью МАУ, позволяющая повысить эффективности обеспечения безопасности информации при эксплуатации МАУ в защищенных корпоративных сетях.

Научные результаты, полученные в ходе выполнения работы, являются новыми и практически значимыми, что доказано актами внедрения. Отмеченные выше недостатки не снижают научной новизны и практической полезности работы, носят частный характер и не влияют на общую положительную оценку проведённого исследования.

Рукопись диссертационного исследования и автореферат представлены в соответствии с требованиями. Личный вклад автора по решению поставленных задач не вызывает сомнения. Автореферат характеризуется логичностью представления материалов и корректностью используемой терминологии, написан ясным лаконичным языком и вместе с опубликованными работами дает достаточно полное представление о теме и содержании диссертации.

Диссертационная работа Маркина Д. О. "Управление безопасностью мобильных абонентских устройств в корпоративных сетях" является завершенной научно-квалификационной работой, обладает научной новизной и практической полезностью. Содержание диссертационной работы отвечает требованиям, установленным в п. 9 Положения о присуждении учёных степеней, утверждённого

постановлением Правительства Российской Федерации от 24 сентября 2013 года № 842 в редакции от 28.08.2017 года, предъявляемым к кандидатским диссертациям.

В связи с этим считаю, что соискатель Маркин Дмитрий Олегович заслуживает присуждения учёной степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Официальный оппонент
Доктор технических наук, доцент

Н. Н. Мошак

"15" мая 2018 г.

Подпись Мошака Николая Никол

"15" мая 2018 г.

Сведения о составителе отзыва:

Мошак Николай Николаевич
Доктор технических наук
Доцент
Место работы: Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения».
Должность: профессор кафедры безопасности информационных систем ГУАП СПб.
Почтовый адрес: 190000, Санкт-Петербург, ул. Большая Морская, д. 67, лит. А
Телефон: +7 (812) 710-65-10.
Адрес электронной почты: nnmoshak49@mail.ru.