На правах рукописи

Маркин Дмитрий Олегович

УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ МОБИЛЬНЫХ АБОНЕНТСКИХ УСТРОЙСТВ В КОРПОРАТИВНЫХ СЕТЯХ

Специальность 05.13.19 – Методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ

диссертации на соискание ученой степени
кандидата технических наук

Санкт-Петербург – 2018

Работа выполнена в федеральном государственном казенном военном образовательном учреждении высшего образования "Академия Федеральной службы охраны Российской Федерации".

Научный руководитель: кандидат технических наук, доцент
Комашинский Владимир Владимирович

Официальные оппоненты: главный научный сотрудник
АО НИИ "Вектор", Санкт-Петербург
доктор технических наук,
старший научный сотрудник
Емелин Вадим Иванович

профессор кафедры безопасности информационных систем ФГАОУ ВО "Санкт-Петербургский государственный университет аэрокосмического приборостроения",
доктор технических наук, доцент
Мошак Николай Николаевич

Ведущая организация: ФГКОУ ВО "Томский государственный университет систем управления и радиоэлектроники"

Защита состоится " " _____ 2018 г. в _____ часов на заседании диссертационного совета Д 002.199.01, созданного на базе Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук по адресу:
199178, Санкт-Петербург, 14-а линия В.О., 39, комн. 401.

С диссертацией и авторефератом можно ознакомиться в библиотеке и на сайте Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук.
http://www.spiiras.nw.ru/dissovet/

Автореферат разослан " " _____ 20 ___ г.

Ученый секретарь
диссертационного совета Д 002.199.01
канд. техн. наук А. А. Зайцева

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность исследования. Развитие современных многофункциональных мобильных абонентских устройств (МАУ), к которым можно отнести смартфоны, планшетные компьютеры, ноутбуки и т. п., приводит к постоянному росту потребности в доступе к информации и инфокоммуникационным услугам. Эта тенденция затрагивает и корпоративные сети с разными требованиями по защищенности. Увеличивается потребность в удаленном доступе к ресурсам и услугам защищенных корпоративных сетей, при этом растет роль мобильных пользователей и потребность в доступе к услугам с использованием МАУ. Как правило, для доступа к защищенной корпоративной сети используются служебные МАУ, при этом использование личных МАУ существенно ограничено. Использование единого устройства в рамках концепции BYOD ("Bring Your Own Device") имеет много недостатков, обусловленных особенностями известных систем защиты информации (СЗИ) для мобильных решений. А применение известных мобильных решений, имеющих неизменный набор СЗИ, как правило, ограничивает его использование в рамках одной сети и не позволяет предоставлять весь спектр услуг, как открытых, так и защищенных, из-за неэффективности современных СЗИ. Это обусловлено тем, что перемещение пользователей и подключение их к различным сетям определяют вариативный спектр угроз информационной безопасности при работе с единым МАУ по сравнению со стационарными абонентскими пунктами и средствами вычислительной техники и требуют применения дополнительных и в каждом случае различных наборов средств защиты информации.

На основе анализа тенденций и перспектив развития современных корпоративных сетей выявлено противоречие между требованиями, предъявляемыми к безопасности информации при доступе к защищенным услугам и информации с использованием универсальных МАУ, и техническими возможностями СЗИ, позволяющих обеспечить безопасность информации при осуществлении такого доступа в сетях с разными требованиями по защищенности. При удаленном доступе к услугам и ресурсам корпоративных сетей с разными требованиями по защищенности возникает противоречие, заключающееся в недостаточном обеспечении безопасности такого доступа при использовании единого МАУ в виду недостаточной эффективности существующих СЗИ.. Следовательно, разработка новых алгоритмов защищенного доступа к услугам сетей с разными требованиями по защищенности с использованием единого МАУ является актуальной задачей.

Степень разработанности темы исследования. В данном направлении исследований существенные результаты в области изучения моделей безопасности управления доступом в отечественных и зарубежных научных трудах получены под руководством Девянина П. Н., Зегжды Д. П., Гайдамакина Н. А., Бочкова М. В., Герасименко В. А., Бородакий Ю. В., Маклина Дж., Самарати П., Сандху Р. Исследования проблем защиты информации, в том числе и проблем анализа защищенности информации проводились под руководством Ломако А. Г., Молдовяна А. А., Стародубцева Ю. И., Окова И. Н, Остапенко А. Г., Шелупанова А. А., Котенко И. В. В области вопросов мобильной радиосвязи и радиодоступа, средств широкополосного доступа, безопасности беспроводных сетей доступа известны работы Челышева В. Д., Кловского Д. Д., Коржика В. И., Вишневского В. М., Шахновича И. В., Баскакова С. И., Зюко А. Г. и др. В области защиты информации при эксплуатации МАУ известны работы Гузаирова М. В., Машкиной И. В.,

Бабикова А. Ю., Десницкого В. А. и Карпеева Д. О. Однако вопросы управления безопасностью МАУ для обеспечения безопасности доступа к услугам сетей с разными требованиями по защищенности рассмотрены недостаточно полно.

Объект исследования*:* система управления безопасностью МАУ в корпоративных сетях с разными требованиями по защищенности.

Предмет исследования*:* модели и алгоритмы управления безопасностью МАУ.

Цель исследования*:* повышение вероятности обеспечения безопасности информации при доступе к инфокоммуникационным услугам и информации в корпоративных сетях с разными требованиями по защищенности при использовании единого МАУ.

Для достижения данной цели в поставлены и решены следующие **задачи**:

1. Проведен анализ условий функционирования и требований, предъявляемые к мобильным абонентским устройствам, формальным моделям безопасности, описывающим политику безопасности компьютерных систем (КС) с МАУ; проведен анализ моделей угроз и нарушителя в КС с МАУ, способов построения комплексной СЗИ при работе в сетях с разными требованиями по защищенности; разработана система показателей качества, позволяющая оценить эффективность процесса защиты информации при эксплуатации системы управления безопасностью МАУ в корпоративных сетях с разными требованиями по защищенности.

2. Разработана формальная модель безопасности МАУ, учитывающая местоположение устройства и иные условия доступа, влияющие на состояние защищенности, обоснована ее корректность, доказано отсутствие возможности возникновения информационных потоков от объектов с более высоким уровнем конфиденциальности к объектам с более низким уровнем, предложено технологическое решение, позволяющее оценить местоположение МАУ, определяемое с помощью известных способов, а также повысить достоверность определения местоположения МАУ до требуемых значений уровней ошибок 1-го и 2-го родов.

3. Разработан алгоритм управления безопасностью МАУ, учитывающий требования к качеству предоставляемых услуг и требования по защищенности, и позволяющий формировать управляющее воздействие на доверенное МАУ, переводящее в программно-аппаратную конфигурацию, отвечающую указанным требованиям. Осуществлена оценка свойств разработанного алгоритма.

4. Разработаны научно-технические предложения по практической реализации системы управления безопасностью мобильных абонентских устройств в корпоративных сетях, а также рекомендации по формированию оптимальных параметров подсистемы определения местоположения МАУ в помещениях для известной карты расположения помещений и технологий определения местоположения МАУ на основе БСПД.

Основные положения, выносимые на защиту*:*

1. Модель безопасности мобильного абонентского устройства в корпоративных сетях с разными требованиями по защищенности [2, 5, 7, 14].

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, 6, 13].

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 [1, 4, 10–12, 15].

Научная новизна диссертационной работы состоит в следующем:

1. Разработана модель безопасности МАУ, отличающаяся от известных учетом его местонахождения в корпоративных сетях с разными требованиями по защищенности, обоснована ее корректность.

2. Разработано технологическое решение, позволяющее повысить достоверность определения местоположения МАУ в помещениях с разными требованиями по защищенности за счет применения метода статистических испытаний.

3. Разработан алгоритм управления безопасностью МАУ, отличающийся от известных определением 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.

4. 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.

Практическая новизна диссертационной работы заключается:

– в разработке научно-технических предложений по практической реализации системы управления безопасностью МАУ в корпоративных сетях, позволяющих повысить вероятность обеспечения безопасности информации при удаленном доступе к инфокоммуникационным услугам и ресурсам в сетях с разными требованиями по защищенности при использовании единого МАУ;

– в разработке рекомендаций по формированию оптимальных параметров системы определения местоположения МАУ в корпоративной сети, позволяющих повысить достоверность вычисления его местонахождения в специальных помещениях.

Теоретическая значимость выполненных в диссертации исследований состоит в разработке формального аппарата моделирования безопасности МАУ в корпоративных сетях с учетом его местоположения в специальных помещениях, а также разработке алгоритма оптимизации программно-аппаратной конфигурации (безопасности) МАУ, позволяющего повысить вероятность обеспечения безопасности информации при доступе к инфокоммуникационным услугам и информации корпоративных сетей с разными требованиями по защищенности при использовании единого МАУ за счет учета требований по информационной безопасности (ИБ) и качеству предоставляемых услуг в корпоративной сети.

Практическая значимость работы заключается:

1) в исследовании эффективности известных способов и систем определения местоположения МАУ при их использовании внутри здания в заданных помещениях и обосновании оптимальных параметров алгоритмов определения ме-

стоположения МАУ в корпоративной сети, позволяющих повысить достоверность определения местонахождения МАУ в специальных помещениях;

2) в реализации предложенных алгоритмов в виде комплекса программ для ЭВМ и проверке возможности их применения в корпоративной сети;

3) в разработке научно-технических предложений по практической реализации системы управления безопасностью МАУ, повысить вероятность обеспечения безопасности информации при доступе к инфокоммуникационным услугам и информации корпоративных сетей с разными требованиями по защищенности при использовании единого МАУ.

Методология и методы исследования. В работе использовался аппарат и методы теории машинного обучения, теории вероятности и математической статистики, аппарата скрытых марковских моделей, теории алгоритмов, теории управления, теории множеств, теории оптимизации, численных методов и методов математического и имитационного моделирования.

Апробация работы. Основные результаты, полученные в ходе работы, были представлены на следующих конференциях: 6-я, 7-я и 8-я Межрегиональные научно-практические конференции "Информационная безопасность и защита персональных данных: проблемы и пути их решения" (г. Брянск, БГТУ, 2014, 2015 и 2016 гг.); 12-е Всероссийское совещание по проблемам управления ВСПУ-2014 (г. Москва, ИПУ им. В. А. Трапезникова РАН, 16–19 июня 2014 г.); Международная научно-техническая конференция "Перспективные информационные технологии" (г. Самара, Самарский научный центр РАН, 2015, 2016 гг.).

Публикации. По теме диссертационной работы опубликовано 6 статей в рецензируемых журналах, входящих в перечень ВАК Минобнауки России, 7 тезисов докладов, 6 свидетельств об официальной регистрации программ для ЭВМ, 3 патента на изобретения.

Акты внедрения научных результатов диссертационного исследования получены в Спецсвязи ФСО России и ФГУП "Государственный научно-исследовательский институт прикладных проблем" ФСТЭК России.

Структура и объем диссертационной работы. Диссертационная работа состоит из введения, четырех разделов, заключения, библиографического списка, содержащего 150 источников, 3 приложения. Текст диссертации изложен на 233 страницах, включая 52 рисунка и 31 таблицу.

СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснованы актуальность работы для пользователей, ее научная новизна, теоретическая и практическая значимость. Определены объект, предмет и цель исследования, сформулирована научная задача. Перечислены основные положения, выносимые на защиту, дано краткое содержание работы.

В первом разделе проведен анализ научных исследований, методов и технических решений по защите информации при использовании МАУ для удаленного доступа к услугам корпоративных сетей с разными требованиями по защищенности. В качестве современных МАУ в работе рассматриваются защищенные мобильные смартфоны, технические мобильные средства защищенного терминального доступа, защищенные планшетные к мобильные компьютерные средства. Приведены результаты анализа технологий доступа к услугам сетей с разными требованиями по защищенности. Проведен анализ угроз информационной безопасности (ИБ) при использовании МАУ, предложены модели угроз и нарушителя

для мобильных пользователей в корпоративных сетях с разными требованиями по защищенности. Установлено, что потребность пользователей в получении удаленного доступа к информации с разными требованиями по защищенности обуславливает наличие у них нескольких мобильных терминалов. Однако в связи с запретом использования определенных МАУ в специальных помещениях пользователи вынуждены отказываться от получения информации и услуг в определенные интервалы времени.

Для обеспечения безопасного доступа МАУ к услугам корпоративных сетей с разными требованиями по защищенности возникает объективная потребность учитывать местоположение МАУ. Установлено, что существующие формальные модели безопасности компьютерных систем, учитывающих местоположение МАУ как дополнительный фактор, не содержат доказательств отсутствия запрещенных информационных потоков от объектов с высоким уровнем конфиденциальности к объектам с низким уровнем конфиденциальности. Кроме того, в известных формальных моделях безопасности не затрагиваются вопросы автоматического управления программно-аппаратной конфигурацией МАУ в целях выполнения требований политики безопасности, заключающейся в согласовании состояния МАУ с условиями доступа и его местоположением и другими требованиями, а также вопросы оценивания точности определения местоположения МАУ в помещениях внутри зданий.

Формальная постановка задачи диссертационного исследования: на основе теории машинного обучения, математический статистики и численных методов разработать модель безопасности МАУ и алгоритм управления безопасностью МАУ, учитывающий атрибуты доступа, включая местоположение устройства, требования по безопасности информации и качеству предоставляемых услуг.

Исходными данными для решения диссертационной задачи являются: MD – МАУ и его технические характеристики; $CONF$ – множество конфигураций МАУ; $Rooms$ – расположение и требования по защищенности помещений; AP – точки доступа БСПД, их расположение и характеристики; множество пороговых значений частных показателей эффективности $H = \left\{ P_{\beta}\left(\tilde{L}_{Room} > L_{Room} \right) \le P_{\beta}^{\text{треб}}, T_{RECONF} \le T_{\text{RECONF}}^{\text{доп}} \right\}$; A – атрибуты доступа.

В рамках решения **частных задач** исследования требуется:

1) разработать модель безопасности МАУ Z, учитывающую вероятность нахождения МАУ в специальных помещениях и обосновать ее корректность;

2) разработать алгоритм управления безопасностью МАУ путем реализации решающего правила F отнесения совокупности атрибутов доступа, включающих в себя, в том числе, вероятность нахождения МАУ в специальном помещении к разрешенной конфигурации (состоянию) МАУ, обеспечивающей безопасность информации при доступе к услугам корпоративных сетей с разными требованиями по защищенности и заданное качество предоставление услуг, оценить свойства алгоритма:

$$\begin{cases} Z \xrightarrow{F(MD,Rooms,AP,A)} \{CONF_i\}_{t+1}, \\ P_{\text{БИ}}(T) > P_{\text{БИ}}^{\text{треб}}(T), \end{cases}$$

где $P_{\text{БИ}}(T)$ – вероятность обеспечения безопасности информации;

3) разработать научно-технические предложения по практической реализации системы управления безопасностью МАУ, позволяющей повысить безопасность информации при эксплуатации МАУ в корпоративных сетях с разными требованиями по защищенности при следующих **ограничениях и допущениях:**

– в состав корпоративной сети входит доверенная беспроводная сеть передачи данных (БСПД);

– канал управления между доверенными точками доступа и МАУ защищен криптографическими средствами защиты информации;

– МАУ имеет возможность функционировать в различных программно-аппаратных конфигурациях;

– в составе МАУ функционирует аппаратно-программный модуль доверенной загрузки (АПМДЗ), являющийся программно-аппаратным агентом, управляющим конфигурацией (состоянием) МАУ;

– на МАУ функционирует доверенная операционная система (ДОС);

– в ДОС МАУ функционирует изолированная программная среда (ИПС);

– пользователь МАУ в корпоративной сети аутентифицирован.

Для оценивания эффективности разработанного алгоритма и системы управления безопасностью МАУ предложена следующая система показателей. Вероятность обеспечения защиты информации (безопасности доступа) при эксплуатации МАУ оценивается как $P_{\text{ЗИМАУ}} = P\left(REZ \geq REZ^{\text{треб}}\right) \cdot P\left(RES \leq RES^{\text{доп}}\right) \cdot P\left(OPR \leq OPR^{\text{доп}}\right)$, где REZ и $REZ^{\text{треб}}$ – текущая и требуемая результативность процесса обеспечения безопасности доступа; RES и $RES^{\text{доп}}$ – текущий и допустимый расход операционных ресурсов для обеспечения требуемой безопасности доступа; OPR и $OPR^{\text{доп}}$ – текущий и допустимый расход операционного времени.

Согласно ГОСТ Р 50922–2006 результативность обеспечения безопасности доступа к конфиденциальной информации оценивается по значению вероятности обеспечения безопасности информации: $P_{\text{БИ}}(t) = P_{\text{КИ}}(t) \cdot P_{\text{ЦИ}}(t) \cdot P_{\text{ДИ}}(t)$, где $P_{\text{КИ}}(t)$, $P_{\text{ЦИ}}(t)$, $P_{\text{ДИ}}(t)$ – вероятности обеспечения конфиденциальности, целостности и доступности информации за оцениваемый период времени t.

Оценка вероятности обеспечения конфиденциальности информации согласно ГОСТ РВ 51987–2002 вычисляется с помощью выражения $P_{\text{КИ}}(t) = \left(1 - P_{\text{НСД}}(t)\right) \times P_{\text{СК}}(t)$, где $P_{\text{НСД}}(t)$ – вероятность несанкционированного доступа к защищаемой информации; $P_{\text{СК}}(t)$ – вероятность сохранения конфиденциальности информации.

Значение показателя $P_{\text{НСД}}(t)$ определяется эффективностью имеющихся СЗИ, которые согласно принятым ограничениям и допущениям гарантируют защиту от НСД, а также эффективностью предложенной системы управления МАУ: $P_{\text{НСД}} = P\left(CONF \subset CONF^{\text{доп}}\right) = P\left[P_{\beta}\left(\tilde{L}_{Room} > L_{Room}\right) \leq P_{\beta}^{\text{доп}}\right]$, где $CONF$ – сформированная конфигурация МАУ; $CONF^{\text{доп}}$ – множество допустимых (разрешенных конфигураций) МАУ при текущих атрибутах доступа; $P_{\beta}\left(\tilde{L}_{Room} > L_{Room}\right)$ – вероятность ошибки 2-го рода, характеризующая правильность принятия решения об уровне защищенности помещения, в котором находится МАУ; $P_{\beta}^{\text{доп}}$ – предельно допустимая величина ошибки 2-го рода, определяемая требованиями по ИБ (заказчиком) к системе управления безопасностью МАУ.

Величина вероятности сохранения конфиденциальности информации оценивается как вероятность своевременной переконфигурации МАУ при условии соответствия сформированной конфигурации МАУ множеству допустимых и заданных атрибутов доступа: $P_{\text{СК}} = P\left[\left(T_{RECONF} \le T_{RECONF}^{\text{доп}}\right) / \left(CONF \subset CONF^{\text{доп}}\right)\right]$.

Показатель вероятности доступности информации оценивается как $P_{\text{ДИ}}(T_{\text{ДИ}}) = \frac{N_{\text{ДУ}}}{N_{\text{У}}} \cdot P_{\text{св}}\left(T_{\text{ДИ}} \le T_{\text{ДИ}}^{\text{зад}}\right) \middle| T_{\text{ДИ}}^{\text{зад}} = T_{RECONF}^{\text{доп}}$, где $N_{\text{ДУ}}$ – количество доступных защищенных услуг; $N_{\text{У}}$ – общее количество предоставляемых МАУ услуг; $P_{\text{св}}\left(T_{\text{ДИ}} \le T_{\text{ДИ}}^{\text{зад}}\right)$ – вероятность своевременной переконфигурации МАУ; $T_{\text{ДИ}}$ и $T_{\text{ДИ}}^{\text{зад}}$ – время, необходимое для обработки запроса на доступ к услуге и заданное заказчиком нормативное время доступа к услугам.

Постановка задачи диссертационного исследования сформулирована как задача автоматического управления с элементами машинного обучения. Для ее решения предлагается использовать теорию машинного обучения, теории вероятности и математической статистики, аппарат скрытых марковских моделей, теорию алгоритмов, теорию управления, теорию оптимизации, теорию множеств, численные методы и методы математического и имитационного моделирования.

Во втором разделе предложена формальная модель безопасности МАУ в корпоративных сетях с разными требованиями по защищенности, учитывающая атрибуты доступа МАУ, включая вероятность его нахождения в специальном помещении. Обоснована ее корректность. Предложено технологическое решение по расчету оценки вероятности местонахождения МАУ в специальном помещении на территории организации с заданной точностью. Разработанная формальная модель безопасности базируется на классической модели Белла-ЛаПадулы, элементах ролевой и атрибутной моделях управления доступом, а также и моделях безопасности, учитывающих местоположение субъектов.

Исходными данными формальной модели являются:

1) элементы классической модели Белла-ЛаПадулы с дополнениями формальной модели безопасности МАУ: S – множество субъектов системы; MD – множество МАУ, при этом $MD \subseteq S$; O – множество объектов системы, включая функциональные блоки МАУ; $P = \{read, write, append, execute\}$ – множество видов доступа и видов прав доступа; $B = \{b \subseteq S \times O \times P\}$ – множество возможных множеств текущих доступов в системе; $(L, \le)$ – решетка конфиденциальности, например, $L = \{\text{"ОИ"}, \text{"КИ"}\}$, где "ОИ" < "КИ"; $\text{М} = \left\{m_{|S|\times|O|}\right\}$ – множество возможных матриц доступов, где $m_{|S|\times|O|}$ – матрица доступов, $m[s,o] \subseteq P$ – права доступа субъекта s к объекту o; $(f_s, f_o, f_c, f_{loc}) \in F = L^S \times L^O \times L^S$ – четверка функций (f_s, f_o, f_c, f_{loc}), задающих соответственно: $f_s : S \to L$ – уровень доступа субъектов; $f_o : O \to L$ – уровень конфиденциальности объектов; $f_c : S \to L$ – текущий уровень доступа субъектов, при этом для любого $s \in S$, выполняется неравенство $f_c(s) \le f_s(s)$; $f_{LOC} : LOC \to L$ – функция, определяющая уровень конфиденциальности местоположения; $V = B \times M \times F$ – множество состояний системы; Q – мно-

жество запросов к системе; D – множество ответов по запросам, например, $\{yes, no, error\}$; $W \subseteq Q \times D \times V \times V$ – множество действий системы, где четверка $(q, d, v^*, v) \in W$ означает, что система по запросу q с ответом d перешла из состояния v в состояние v^*; $\mathbb{N}_0 = \{0,1,2,...\}$ – множество значений времени; X – множества функций $x: \mathbb{N}_0 \to Q$, задающих все возможные последовательности запросов к системе; Y – множество функций $y: \mathbb{N}_0 \to D$, задающих все возможные последовательности ответов системы по запросам; Z – множество функций $z: \mathbb{N}_0 \to V$, задающих все возможные последовательности состояний системы;

2) элементы мандатно-ролевого управления доступом с дополнениями формальной модели безопасности МАУ: R – множество ролей; $CONF$ – множество возможных конфигураций МАУ, при этом $CONF \subseteq R$; SS – множество сессий пользователей (субъектов); $PA: R \to 2^P$ – функция, задающая для каждой роли множество прав доступа; при этом для каждого права доступа $p \in P$ существует роль $r \in R$ такая, что $p \in PA(r)$; $SA: S \to 2^R$ – функция, задающая для каждого субъекта множество ролей, на которые он может быть авторизован, при этом для $MD \subseteq S$ $SA: MD \to 2^{CONF}$; $user: SS \to S$ –функция, задающая для каждой сессии субъекта (пользователя), от имени которого она активизирована; $device: SS \to S$ – функция, задающая для каждой сессии субъекта (МАУ), от имени которого она активизирована, при этом MD – множество МАУ и $MD \subseteq S$; $roles: SS \to 2^R$ – функция, задающая для субъекта (пользователя) множество ролей, на которые он авторизован в данной сессии, при этом в каждый момент времени для каждой сессии $ss \in SS$ выполняется условие $roles(ss) \subseteq SA(user(ss))$; $confs: SS \to 2^R$ – функция, задающая для субъекта (МАУ) множество конфигураций, на которые он авторизован в данной сессии, при этом в каждый момент времени для каждой сессии $ss \in SS$ выполняется условие $confs(ss) \subseteq SA(device(ss))$;

3) элементы атрибутной политики безопасности, учитывающей особенности программно-аппаратных конфигураций МАУ и его местоположение: A – множество оцениваемых атрибутов доступа, таких как, например, идентификационные данные о пользователе, МАУ, операционной системе (ОС) и приложениях МАУ, сетевая адресная информация, уровень конфиденциальности и идентификатор запрашиваемой услуги, время запроса на доступ; LOC – множество возможных местоположений; $\text{MA} = \left\{ ma_{|CONF| \times |A|} \right\}$ – множество возможных матриц атрибутов доступа, где $ma_{|CONF| \times |A|}$ – матрица требуемых атрибутов доступа, $ma[conf, a] \subseteq A$ – множество требуемых значений атрибутов доступа для конфигурации $conf$; расположение и другие параметры помещений: $Rooms = \left\{ room_i = \left((x_{i1}, y_{i1}), (x_{i2}, y_{i2}), ..., (x_{in}, y_{in}), L_{Room_i} \right) \right\}$, $i = \overline{1, N}_{Rooms}$, где L_{Room_i} – уровень требований по защищенности помещения; $(x_{i1}, y_{i1}), (x_{i2}, y_{i2}), ..., (x_{in}, y_{in})$ – координаты n углов помещений; N_{Rooms} – количество помещений; расположение

точек доступа БСПД $AP = \left\{ AP_j = \left(x_j, y_j \right) \right\}$, $j = \overline{1, N}_{AP}$, где (x_j, y_j) – координаты точек доступа, N_{AP} – количество точек доступа.

В разработанной формальной модели безопасности МАУ предложены следующие дополнения к известным моделям:

– множество объектов доступа O дополнено множеством функциональных блоков МАУ: ПЗУ, ОЗУ, ЦП, АПМДЗ, модули Bluetooth, дисплея, Wi-Fi, клавиатуры, GSM, USB, тачскрина, фото- и видеокамеры и другие;

– множество субъектов доступа S дополнено множеством МАУ $MD \subseteq S$;

– множество ролей R дополнено множеством возможных конфигураций МАУ $CONF \subseteq R$, при этом каждая конфигурация (роль) определяется набор тех или иных прав и видов прав доступа на объекты доступа;

– определен порядок оценивания местоположения с учетом известных технологий определения местоположения и их точности, позволяющий обеспечить требуемую достоверность;

– определены свойства системы защиты, учитывающие уровни конфиденциальности местоположения и особенности программно-аппаратных конфигураций МАУ с учетом мандатного разграничения доступа и особенностей функционирования системы определения местоположения МАУ.

Свойства классической модели Белла-ЛаПадулы дополнены *as*-свойством атрибутной, в результате чего установлены следующие свойства безопасности:

ss – свойство простой безопасности (simple security);

* –свойства "звезда";

ds – свойство дискреционной безопасности (discretionary security).

as – свойства атрибутной безопасности (attribute security).

Доказательство корректности дополнений к классической модели Белла-ЛаПадуллы основывается на определении системы и условий безопасности, заданных на множестве действий данной системы.

Определение 1. $\sum(Q, D, W, z_0) \subseteq X \times Y \times Z$ называется системой, когда для каждого $(x, y, z) \in \sum(Q, D, W, z_0)$ выполняется условие: для $t \in \mathbb{N}_0$, $(x_t, y_t, z_{t+1}, z_t) \in W$, где z_0 – начальное состояние системы. При этом каждый набор $(x, y, z) \in \sum(Q, D, W, z_0)$ называется реализацией системы, а $(x_t, y_t, z_{t+1}, z_t) \in W$ – действием системы в момент времени $t \in \mathbb{N}_0$.

Для учета особенностей эксплуатации МАУ в корпоративных сетях с разными требованиями по защищенности дано определение *as*-свойства.

Определение 2. Состояние системы $(b, m, f) \in V$ обладает *as*-свойством, когда каждого доступа $(s, o, p) \in b$ выполняются одновременно условия $f_{LOC}(loc) = f_s(confs(ss))$, $f_{LOC}(loc) = f_s(user(ss))$ и $\left(\forall a \in A \, \exists a^{\text{треб}} \in A^{\text{треб}} : a = a^{\text{треб}} \, и \, a^{\text{треб}} \in ma[conf, a]\right)$.

На основе данных и других вспомогательных введена и доказана теорема безопасности системы.

Теорема 1. Система $\sum(Q, D, W, z_0)$ обладает *as*-свойством атрибутной безопасности для любого начального состояния z_0, обладающего *as*-свойством,

тогда и только тогда, когда для каждого действия $\left(q,d,\left(b^*,m^*,f^*\right),\left(b,m,f\right)\right)\in W$ выполняются условия 1, 2.

Условие 1. Каждый доступ $\left(s,o,p\right)\in b^*\setminus b$ обладает *as*-свойством относительно f^*.

Условие 2. Если $\left(s,o,p\right)\in b$ и не обладает *as*-свойством относительно f^*, то $\left(s,o,p\right)\notin b^*$.

Доказано, что для описанной модели отсутствует логическая увязка условий выполнения системой свойств безопасности, данных в их определениях, с заложенными в модель условиями их проверки. В связи с этим большое значение имеет корректное определение свойств безопасности, непротиворечащее здравому смыслу и логике обеспечения безопасности информации. Поскольку вновь введенное *as*-свойство атрибутной безопасности определяет совокупность дополнительных ограничений на доступы в системе, то такое описание свойства безопасности, как минимум, не ухудшает уровня безопасности, установленного в классической модели Белла-ЛаПадуллы, а выполнение данного условия позволяет ограничить потенциально опасные доступы в системе, тем самым обеспечив выполнение заложенных в политику безопасности требований, и повысить адекватность формальной модели безопасности МАУ условиям ее эксплуатации.

В рамках теоретико-множественного подхода указанные условия сформулированы таким образом, что они расширяют множество субъектов, объектов и ролей, установленное в системе, не нарушая их целостности, но вводя дополнительные ограничения. В связи с этим ограничения, установленные для классических ролей, распространяются и на универсум ролей, включающих в свой состав конфигурации МАУ. Структура элементов ролевой модели управления доступом с конфигурациями МАУ представлены на рисунке 1.

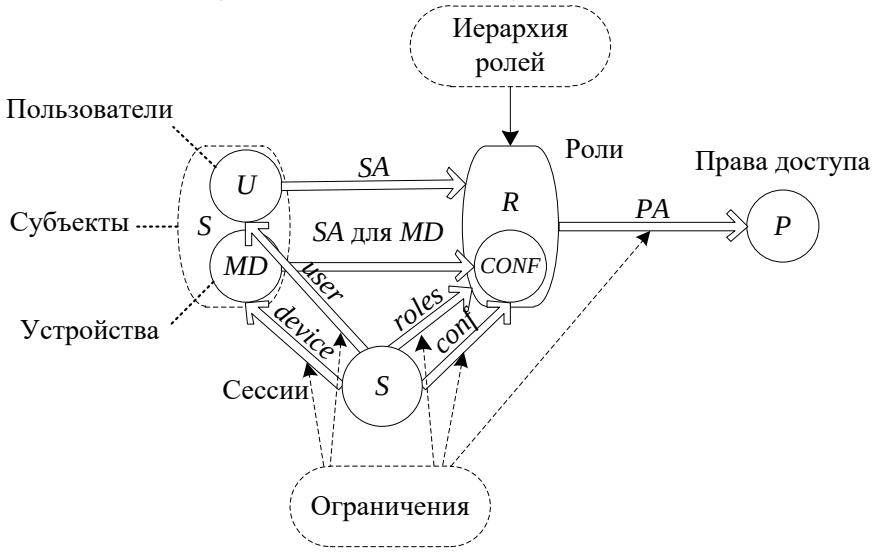

Рисунок 1 — Структура элементов ролевой модели управления доступом с конфигурациями МАУ

Мандатное управление доступом реализуется на базе ролевого управления доступом с доказательством невозможности реализации запрещенных информационных потоков от объектов с высоким уровнем конфиденциальности к объектам с низким уровнем конфиденциальности. В работе показано, что при введении понятия конфигурация МАУ, множество которых представляют собой аналог роли пользователя $CONF\subseteq R$, невозможна реализация запрещенных информационных потоков от объектов с высоким уровнем конфиденциальности к объектам с низким уровнем конфиденциальности.

Определение 3. Будем считать, что существует информационный поток от объекта $o \in O$ к объекту $o' \in O$ (функционального модуля МАУ) тогда и только тогда, когда существуют конфигурации $conf, conf' \in CONF$, сессия $ss \in SS$ такие, что $(o, read) \in PA(conf)$, $(o', write) \in PA(r')$ и $r, r' \in confs(ss)$.

Введены определения либерального и строгого мандатного управления доступов для конфигураций $CONF \subseteq R$. Обосновано, что в модели ролевого управления доступом, соответствующей требованиям либерального и строгого мандатного управления доступом, невозможна реализация запрещенных информационных потоков от объектов с высоким уровнем конфиденциальности к объектам с низким уровнем конфиденциальности. Представлено доказательство теоремы.

Теорема 2. Если модель ролевого управления доступом с конфигурациями МАУ соответствует требованиям либерального или строгого мандатного управления доступом, то в ней для любых объектов $o' \in O$ таких, что $f_o(o) > f_o(o')$, невозможно возникновение информационного потока от o к o'.

Предложено технологическое решение, позволяющее повысить достоверность определения местонахождения МАУ в специальном помещении. Основным параметром, вносящим неопределенность для формирования управляющей команды, является местоположение МАУ. В результате проведенного анализа технологий, систем и алгоритмов определения местоположения МАУ, обоснована целесообразность использования БСПД стандарта 802.11 по сравнению с системами на базе технологий сотовой связи GSM (2G), UMTC(3G), LTE (4G), датчиков RFID, Bluetooth, радиолокационных технологий и технологий на основе применения волоконно-оптических линий связи и инерциальной навигации.

Реальное местоположение МАУ находится в пределах условной окружности с центром с координатами $(\tilde{x}, \tilde{y})$ и радиусом, равным максимальному значению ошибки измерения местоположения: $R_e = \max[e_L]$. Учитывая, что величина R_e соизмерима с габаритами помещений и даже может превышать их, то реальное местоположение пользователя МАУ может значительно отличаться от вычисленного. Зная координаты центра окружности $(\tilde{x}, \tilde{y})$, ее радиус R_e и карту расположения помещений $Rooms$, решение задачи вычисления вероятности того, что пользователь находится в помещении с заданным уровнем защищенности, может быть представлено как вычисление доли площади помещений заданного уровня защищенности относительно площади окружности с центром в точке $(\tilde{x}, \tilde{y})$ и радиусом R_e. Таким образом, для помещений с уровнями защищенности $L_{Room} = \{\text{"ОИ","КИ"}\}$ получено выражение для оценки вероятности того, что пользователь находится в помещении с заданным уровнем защищенности: $P(\tilde{L}_{Room} = L_{Room}) = \dfrac{F_{Sq}(L_{Room}, (\tilde{x}, \tilde{y}), R_e)}{\pi \cdot R_e^2}$, где L_{Room} – уровень защищенности помещения; R_e – радиус окружности, характеризуемый максимальной ошибкой измерения местоположения; $(\tilde{x}, \tilde{y})$ – координаты вычисленного местоположения; $F_{Sq}(L_{Room}, (\tilde{x}, \tilde{y}), R_e)$ – функция, вычисляющая площадь помещений с уровнем защищенности L_{Room}, находящихся внутри окружности с центром в точке $(\tilde{x}, \tilde{y})$, радиусом R_e и площадью $\pi \cdot R_e^2$. Результат вычислений представляется в виде

вектора вероятностей: $\vec{P}_{L_{Room}} = \left\{ P\left(\tilde{L}_{Room} = \text{"ОИ"}\right), P\left(\tilde{L}_{Room} = \text{"КИ"}\right) \right\}$. Вычисление функции $F_{Sq}\left(L_{Room}, (\tilde{x}, \tilde{y}), R_e\right)$ для произвольной конфигурации расположения помещений реализовано на основе метода статистических испытаний (Монте-Карло), для которого формируется обучающая выборка: $\lambda_{e_L} = \left\{ R_e, P\{a \le e_L < b\} = \sum_{a \le e_L < b} p(e_L) \middle| \sum_{0 \le e_L \le R_e} p(e_L) = 1 \right\}$. В результате реализации метода Монте-Карло значение функции $F_{Sq}\left(L_{Room}, (\tilde{x}, \tilde{y}), R_e\right)$ вычисляется как $\frac{N\left(L_{Room}\right)}{N_{MC}}$, а оценка вектора вероятностей того, что пользователь находится в помещении с тем или иным уровнем защищенности: $\vec{P}_{L_{Room}} = \left\{ \frac{N(\tilde{L}_{Room} = \text{"ОИ"})}{N_{MC}}, \frac{N(\tilde{L}_{Room} = \text{"КИ"})}{N_{MC}} \right\}$. Точность данного метода существенно зависит от числа испытаний – N_{MC} и параметров генератора случайных чисел, используемого для формирования координат случайной точки $(x_i', y_i'), i = \overline{1, N}_{MC}$.

Для принятия решения о том, в помещении с каким уровнем защищенности находится в данный момент МАУ, используется критерий: $\tilde{L}_{Room} = \begin{cases} \text{"КИ"}, \text{при } P\left[\left(\frac{N(\tilde{L}_{Room} = \text{"КИ"})}{N_{MC}} \right) \ge N_{\text{КИ}}^{\text{треб}} \right] \\ \text{"ОИ"}, \text{при } P\left[\left(\frac{N(\tilde{L}_{Room} = \text{"КИ"})}{N_{MC}} \right) < N_{\text{КИ}}^{\text{треб}} \right] \end{cases}$, где пороговое значение $N_{\text{КИ}}^{\text{треб}}$ определяется руководящими документами регуляторов в сфере информационной безопасности (ИБ) и, как правило, задается для наихудшего случая. Предложенный способ определения местоположения МАУ инвариантен к методу вычисления координат МАУ внутри здания и может использоваться с любой из известных технологий определения местоположения МАУ внутри здания, основанной на измерении уровня сигнала БСПД.

В третьем разделе представлено описание разработанного алгоритма управления безопасностью МАУ, учитывающего атрибуты доступа к услугам корпоративных сетей с разными требованиями по защищенности. Данный алгоритм решает следующую оптимизационную задачу:

$$\begin{cases} f\left(S^*\right) \longrightarrow \max, \\ \sum_{i=1}^{|S^*|} V_{lm}^{S_i^*} \le \hat{V}_{lm}, \\ S^* = F_S\left(CONF^*\right) \middle| CONF^* \in CONF^{\text{доп}}, S^* \subseteq S, \end{cases}$$

где S – множество, представляемых с помощью МАУ услуг; $f\left(S^*\right)$ – целевая функция, максимизирующая количество предоставляемых пользователю МАУ услуг при заданных условиях; $V_{lm}^{S_i^*}$ – норматив информационной скорости для i-й услуги S_i^* в беспроводном радиоканале между l-м МАУ и m-й точкой доступа; $\hat{V}_{lm}$ – оценочная максимально возможная информационная скорость в беспроводном радиоканале между l-м МАУ и m-й точ-

кой доступа; $CONF^{*}$ – новая конфигурация МАУ; $CONF^{\text{доп}}$ – множество допустимых конфигураций МАУ при текущих атрибутах доступа и местоположении МАУ; F_S – функция отображения конфигурации МАУ на множество услуг, которые могут быть предоставлены пользователю при данной конфигурации с учетом выполнения требований по ИБ. Блок-схема алгоритма представлена на рисунке 2.

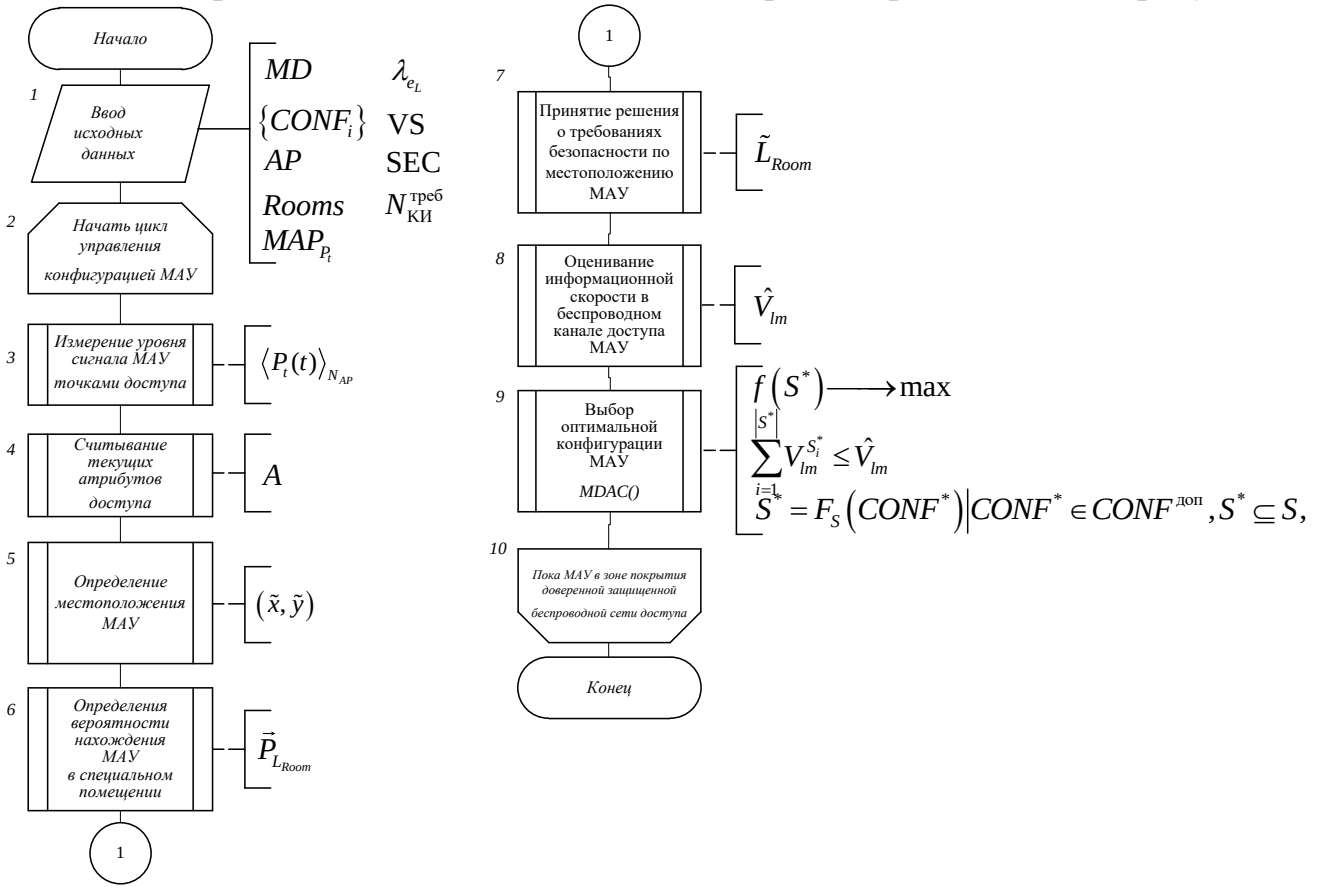

Рисунок 2 – Обобщенная блок-схема алгоритма управления безопасностью МАУ

Защищенность и качество услуг оцениваются на основе матрицы $\text{VS}=\left|vs_i\right|, i=\overline{1,\left|S\right|}$, представляющей собой нормы информационной скорости для i-й услуги, и матрицы SEC, представляющей собой требования правил политики безопасности МАУ для конфигураций МАУ, включающие набор требуемых атрибутов доступа $a_{i0},..,a_{iN_A}$ для i-й конфигурации и местоположение L_i.

Для выбора множества допустимых конфигураций МАУ при заданных атрибутах доступа и местоположении сформулировано решающее правило:

$$CONF^{\text{доп}}=F_{RECONF}\left(\tilde{L}_{Room},A_i\right)\Big|\tilde{L}_{Room}=L_{Room}^{\text{треб}}:\Big(\forall CONF_i\in CONF^{\text{доп}}\ \exists L_{Room}^{\text{треб}}=$$

$$=F_{L_{Room}}\left(CONF_i\right)\Big)\wedge\left(\forall a_i\in A_i\ \exists a_i^{\text{треб}}\in A_i^{\text{треб}}=F_A\left(CONF_i\right):a_i=a_i^{\text{треб}}\right),$$

где $\tilde{L}_{Room}$ – характеристика текущего местоположения МАУ; A_i – множество текущих атрибутов доступа МАУ; $F_{L_{Room}}\left(CONF_i\right)$ – правило выбора из матрицы SEC местоположения $L_{Room}^{\text{треб}}$, для которого определена конфигурация $CONF_i$; $F_A\left(CONF_i\right)$ – правило выбора из матрицы SEC атрибутов доступа $A_i^{\text{треб}}$, для которых определена конфигурация $CONF_i$.

Объект управления – программно-аппаратная конфигурация МАУ. Управляющая подсистема формирует команду $x(t)$ на основе значений следующих параметров: атрибутов доступа $A(t)$, информации о текущей конфигурации МАУ $h(CONF^*,t)$, поступающих по защищенному беспроводному каналу управления, координат местоположения МАУ, вычисляемых на основе данных об уровнях сигнала МАУ $\langle P_t(t)\rangle_{N_{AP}}$, поступающих от точек доступа БСПД, сведений о точках доступа AP, карт сигнального пространства MAP_{P_t}, параметров помещений $Rooms$, статистики ошибок определения местоположения МАУ λ_{e_L}, правил политики безопасности SEC.

Задано уравнение наблюдения для системы управления, связывающее состояние объекта управления, управляющую команду и выходное состояния:

$$y^*(t) = g\left[t, x(t), z^*(t)\right] \Big| z^*(t) = \left\langle A(t), \vec{P}_{L_{Room}}(t), h(conf^*,t)\right\rangle,$$

где $\vec{P}_{L_{Room}}(t)$ – вектор вероятностей нахождения МАУ в помещениях с разными требованиями по защищенности; уравнение состояния $z(t) = f\left[z(t_0), x(\tau)\right]$, где $z(t) = conf \in CONF$, – текущее состояние (конфигурация) МАУ, $\tau \in [t_0, t]$ – момент формирования управляющей команды, $z(t_0) = conf_0$ – начальная (базовая) конфигурация МАУ. Целью управления является обеспечение максимальной безопасности информации при эксплуатации МАУ при условии предоставления услуг связи и информации: $\max\left[P_{\text{БИ}}(T)\right] = P_{\text{КИ}}(T) \times P_{\text{ДИ}}(T) \times P_{\text{ЦИ}} \big| P_{\text{ЦИ}} = 1.$

Описаны основные процедуры алгоритма, дана характеристика подпрограммам, решающим частные задачи в процессе его функционирования. Осуществлена проверка основных свойств алгоритма: результативности, точности, элементарности, корректности, вычислительной сложности и сложности алгоритма по памяти. Практическая ценность разработанного алгоритма заключается в возможности его применения для решения задач управления доверенными МАУ к услугам сетей с разными требованиями по защищенности.

В четвертом разделе описаны научно-технические предложения по практической реализации системы управления безопасностью МАУ в корпоративных сетях. Представлены результаты группы экспериментов по обоснованию оптимальных параметров алгоритмов определения местоположения МАУ с заданной картой помещений. Предложен состав и структура МАУ с управляемой программно-аппаратной конфигурацией. Предложенная структура управляемого МАУ предполагает наличие независимых трактов прохождения информации с разными требованиями по защищенности, обрабатываемой с помощью различных запоминающих устройств, вычислительных процессоров, элементов питания. Управление конфигурацией МАУ осуществляет АПМДЗ за счет воздействия на блок управляемых элементов-переключателей трактов прохождения информации. Таким образом, при выполнении условий $P_\beta\left(\tilde{L}_{Room} > L_{Room}\right) \le P_\beta^{\text{треб}}$ и $T_{RECONF}, T_{\text{ДИ}} \le T_{\text{RECONF}}^{\text{доп}}$ гарантируется выполнения требований ИБ. Оценка степени достижения цели исследования представлена на рисунках 3–6.

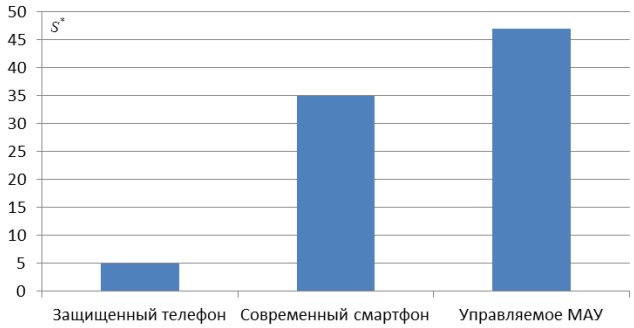

Рисунок 3 – Сравнительный анализ услуг, предоставляемых различными МАУ

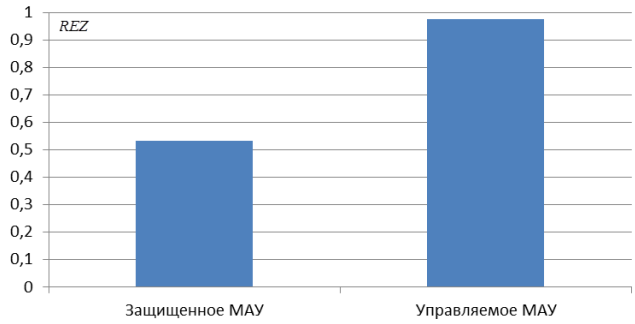

Рисунок 4 – Результативность защиты информации при использовании МАУ

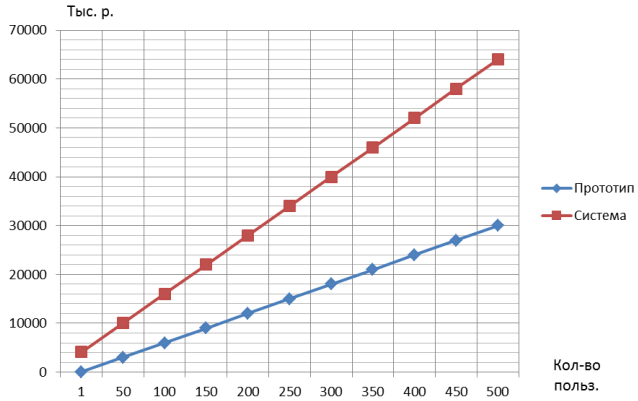

Рисунок 5 – Оценка затрат при использовании различных МАУ для доступа к услугам корпоративных сетей

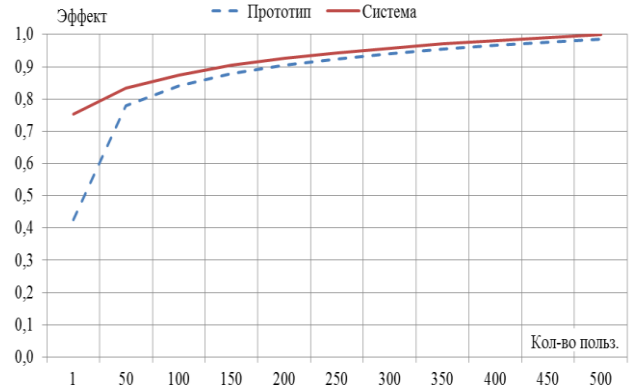

Рисунок 6 – Сравнительный анализ получаемого эффекта для прототипа и разработанной системы

Из анализа рисунков 8-11 видно, что цель исследования достигнута.

В заключении представлены основные выводы, сделанные на основе проведенного диссертационного исследования, перечислены полученные научные и практические результаты, обозначены проблемы, оставленные за пределами работы, а также направления дальнейших исследований.

ОСНОВНЫЕ ВЫВОДЫ И РЕЗУЛЬТАТЫ ДИССЕРТАЦИИ

В диссертационной работе получено решение актуальной задачи по разработке алгоритма и основанной на нем системы управления безопасностью МАУ, базирующиеся на предложенной формальной модели безопасности МАУ, в совокупности позволяющие повысить вероятность обеспечения безопасности информации при доступе к инфокоммуникационным услугам и информации корпоративных сетей с разными требованиями по защищенности при использовании единого МАУ за счет учета атрибутов доступа, включая местоположения МАУ, требований по качеству предоставляемых услуг, а также политик безопасности защищенных корпоративных сетей. В рамках проведения исследований были получены следующие основные результаты:

1. Разработана модель безопасности МАУ, отличающаяся от известных учетом его местонахождения в корпоративных сетях с разными требованиями по защищенности; обоснован выбор технологий, на основе которых целесообразно построение системы определения местоположения МАУ, а также предложен подход, позволяющий повысить достоверность определения местонахождения МАУ в специальных помещениях.

2. Разработан алгоритм управления безопасностью МАУ, учитывающий атрибуты доступа мобильных пользователей; описана оптимизационная задача, ре-

шаемая в алгоритме и охарактеризованная как задача многокритериальной оптимизации целочисленного динамического программирования.

3. Сформированы научно-технические предложения по практической реализации системы управления безопасностью МАУ в корпоративных сетях с разными требованиями по защищенности.

Перспективы развития заключаются в исследования технологий определения местоположение пользователей МАУ в помещениях внутри здания с целью снижения ошибок; исследовании технологий агентно-ориентированного подхода для оптимизации информационного взаимодействия контроллеров беспроводных сетей по передаче управляющей информации; совершенствовании подходов по управлению конфигурацией современных МАУ с целью создания возможности реализации разработанных подходов по управлению доступом применительно к услугам, использующим сведения, отнесенные к государственной тайне.

Выполненное исследование и полученные результаты соответствуют пп. 2, 8 и 13 пунктов паспорта научной специальности 05.13.19 (технические науки):

методы, аппаратно-программные и организационные средства защиты систем (объектов) формирования и предоставления пользователям информационных ресурсов различного вида;

модели противодействия угрозам нарушения информационной безопасности для любого вида информационных систем;

принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности.

СПИСОК РАБОТ, ОПУБЛИКОВАННЫХ АВТОРОМ ПО ТЕМЕ ДИССЕРТАЦИИ В ЖУРНАЛАХ, ВХОДЯЩИХ В ПЕРЕЧЕНЬ ВАК

1. Маркин, Д. О. Методика оценки эффективности защиты информации при эксплуатации мобильных абонентских устройств в корпоративных сетях с разными требованиями по защищенности / Д. О. Маркин, В. В. Комашинский, И. А. Сенотрусов // Вопросы кибербезопасности. – 2017. – № 4 (22). – С. 21–31.

2. Маркин, Д. О. Модель состояний мобильного абонентского устройства в помещениях с разными требованиями по защищенности / Д. О. Маркин, В. В. Комашинский, А. А. Двилянский // Промышленные АСУ и контроллеры. – 2016. – № 10. – С. 40–51.

3. Маркин, Д. О. Алгоритм управления программно-аппаратной конфигурацией защищенного мобильного абонентского устройства / Д. О. Маркин, В. В. Комашинский, А. А. Двилянский // Промышленные АСУ и контроллеры. – 2016. – № 9. – С. 39–50.

4. Маркин, Д. О. Модель доступа к информационным сервисам / Д. О. Маркин, М. А. Сазонов // Телекоммуникации. – 2013. – № 9. – С. 27–31.

5. Маркин, Д. О. Модель системы определения местоположения мобильного устройства на основе метода статистических испытаний / Д. О. Маркин, С. М. Макеев // Известия Тульского государственного университета. Технические науки. – 2016. – № 2. – С. 150–165.

6. Маркин, Д. О. Модель управления профилем защиты мобильного устройства при доступе к услугам с разным уровнем конфиденциальности / Д. О. Маркин, В. В. Комашинский, И. Ю. Баранов // Информационные технологии. – 2015. – № 9 (21). – С. 611–618.

7. Маркин, Д. О. Исследование эффективности алгоритмов определения местоположения мобильных устройств внутри помещений // Вестник РГРТУ. – 2015. – № 54-1. – С. 32–39.

ДРУГИЕ ПУБЛИКАЦИИ

8. Маркин, Д. О. Система удаленного управления функциональностью мобильного абонентского устройства / Д. О. Маркин, А. Н. Разумов // Перспективные информационные технологии (ПИТ 2016): труды Международной научно-технической конференции / под ред. С.А. Прохорова. – Самара: Издательство Самарского научного центра РАН, 2016. – С. 322–326. ISBN 978-5-93424-758-5.

9. Маркин, Д. О. Практические аспекты реализации управления функциональностью мобильных устройств на базе операционной системы Android // Д. О. Маркин, А. Н. Разумов // Информационная безопасность и защита персональных данных. Проблемы и пути их решения: Материалы VIII Всероссийской научно-практической конференции [Текст] + [Электронный ресурс] / под ред. О. М. Голембиовской, М. Ю. Рытова. – Брянск: БГТУ, 2016. – С. 111–116. ISBN 978-5-89838-886-10.

10. Патент 2503059 Российская Федерация : МПК G06F 15/173, H04L 29/12. Способ удаленного мониторинга и управления информационной безопасностью сетевого взаимодействия на основе использования системы доменных имен / Д. О. Маркин, М. С. Аксаментов ; заявитель и патентообладатель Академия ФСО России. – № 2012123556 ; заявл. 06.06.2012 ; опубл. 27.12.2013, Бюл. № 36. – 16 с. : ил.

11. Патент 2530691 Российская Федерация : МПК G06F11/00; H04L9/08. Способ защищенного удаленного доступа к информационным ресурсам / Д. О. Маркин, Д. Е. Шугуров, А. Н. Цибуля, Д. Д. Громей ; заявитель и патентообладатель Академия ФСО России. – № 2013113592; заявл. 26.03.2013; опубл. 10.10.2014, Бюл. № 28. – 13 с. : ил.

12. Патент 2546236 Российская Федерация : МПК G06F11/00; H04L9/08. Способ анализа информационного потока и определения состояния защищенности сети на основе адаптивного прогнозирования и устройство для его осуществления / Д. О. Маркин, С. В. Гребенев, В. Ю. Сергеенков, А. А. Кузькин ; заявитель и патентообладатель Академия ФСО России. – № 2013136682; заявл. 05.08.2013; опубл. 10.04.2015, Бюл. № 10. – 29 с. : ил.

13. Свидетельство о государственной регистрации программы для ЭВМ № 2013618388 Российская Федерация. Анализатор контекста доступа мобильного устройства / Д. О. Маркин, С. В. Шекшуев, В. В. Комашинский ; заявл. 19.07.2013; зарегистрировано в Реестре программ для ЭВМ 06.09.2013 г.

14. Свидетельство о государственной регистрации программы для ЭВМ № 2015615631 Российская Федерация. Автоматизированная система определения местоположения пользователей мобильных устройств внутри здания на основе сигналов беспроводной сети / Д. О. Маркин, Н. И. Биркун, А. О. Зозуля ; заявл. 24.03.2015; зарегистрировано в Реестре программ для ЭВМ 21.05.2015 г.

15. Свидетельство о государственной регистрации программы для ЭВМ № 20166111210 Российская Федерация. Программный агент удаленного управления функциональностью мобильного абонентского устройства / Маркин Д. О., Разумов А. Н., Сенотрусов И. А. ; заявл. 06.11.2015; зарегистрировано в Реестре программ для ЭВМ 27.01.2016 г.