УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ МОБИЛЬНЫХ АБОНЕНТСКИХ УСТРОЙСТВ В КОРПОРАТИВНЫХ СЕТЯХ

Соискатель: Маркин Дмитрий Олегович

Научный руководитель: кандидат технических наук, доцент
Комашинский Владимир Владимирович

Орел 2017

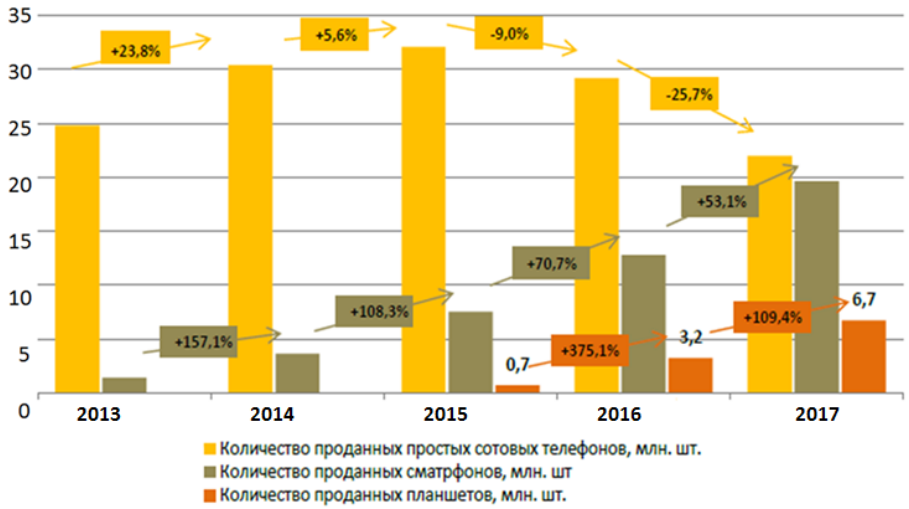


Рис. 1 Динамика увеличения количества мобильных абонентских устройств (МАУ)

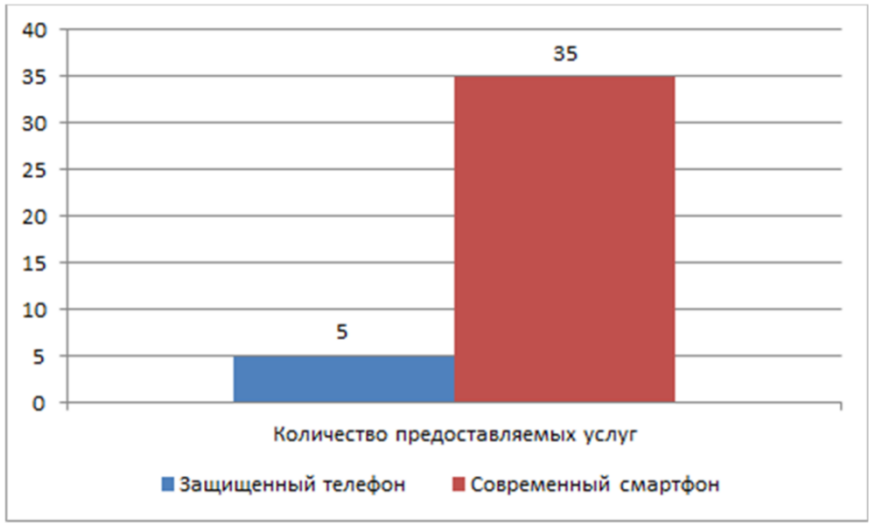


Рис. 3 Сравнительный анализ количества услуг, предоставляемых МАУ

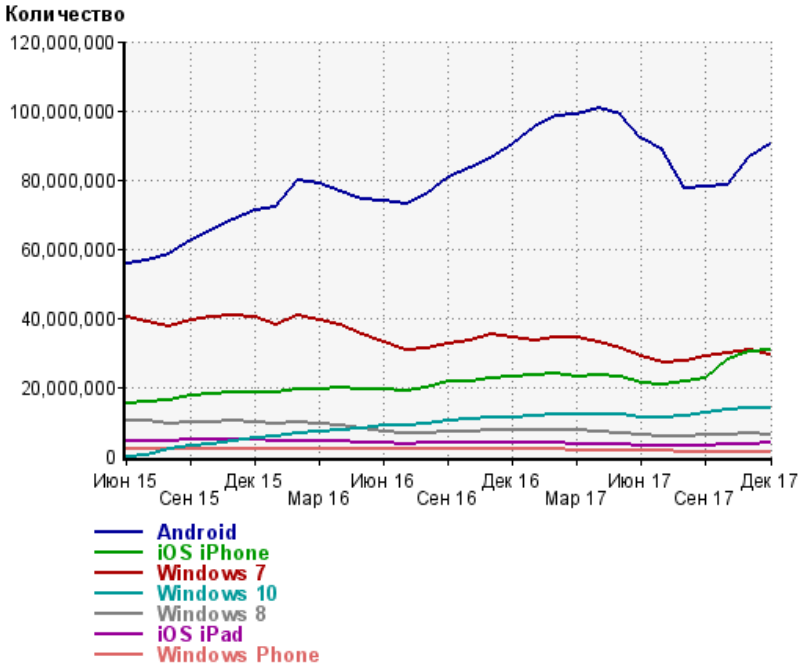


Рис. 2 Популярность операционных систем, используемых для выхода в Интернет по данным LiveInternet с 2015 по 2017

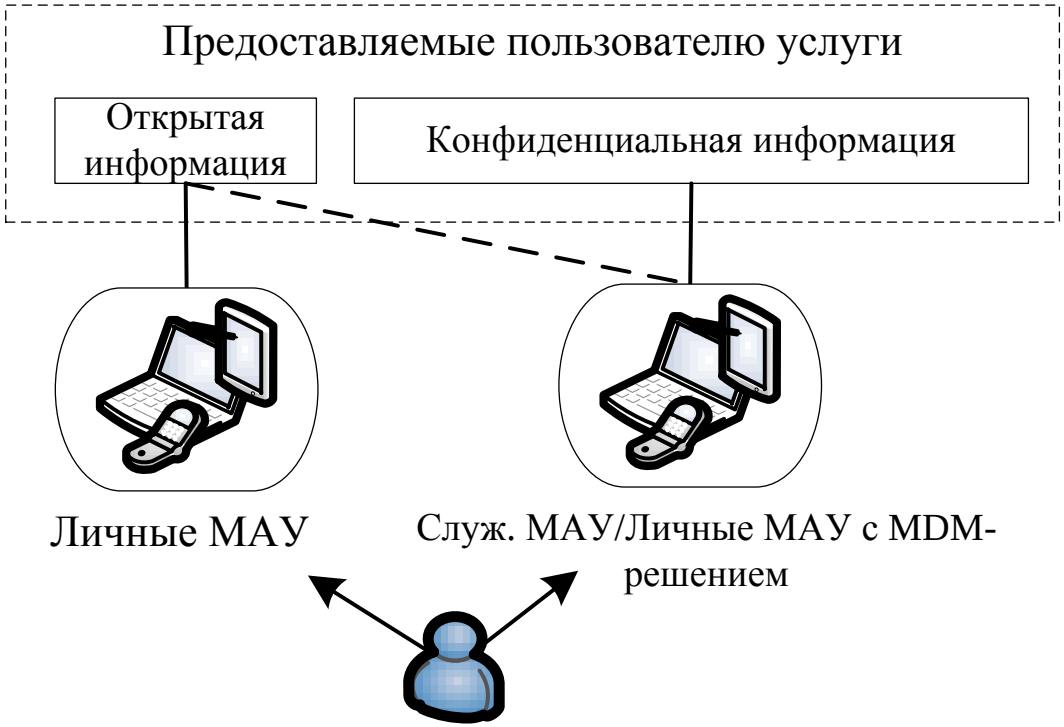


Схема доступа к информации с использованием МАУ и за его пределами в настоящее время

Образцы защищенных мобильных технических решений

Существующие технические средства (решения) и программное обеспечение для защиты информации при эксплуатации МАУ

№ п/п	Программное обеспечение (MDM-решения)
1	Cisco Unified Access/Cisco Identity Services Engine/Cisco Secure ACS
2	MobileIron
3	Kaspersky Security 10 для мобильных устройств
4	McAfee Enterprise Mobility Management (McAfee EMM)
5	Пакет Afaria компании SAP
6	SOTI Mobicontrol
7	AirWatch MDM
8	Samsung Enterprise Access Layer (SEAL)
9	Juniper Junos Pulse MSS

№ п/п	Техническое решение
Защищенные планшетные компьютеры	
1	Континент Т-10 ("Код безопасности)
2	Моб. ПАК "Рысь" (ЦНИИ ЭИСУ)
Защищенные мобильные вычислительные комплексы	
1	Изделие МВК-2 (ЗАО "Инфопро")
2	Комплекс "Модуль-HSM" (НТЦ "Атлас")
3	ПАК Туннель WiFi
Защищенные сотовые телефоны и программное обеспечение для них	
1	ПО ViPNet Client iOS/ViPNet Client Android
2	Спец. микросотовый телефон М-549М (НТЦ "Атлас")
3	Спец. сотовый телефон SMP-Атлас/2
4	ОС РоМОС (Защищ. мобильная ОС)

Противоречие

между требованиями, предъявляемыми к безопасности информации при доступе к защищенным услугам и информации с использованием МАУ,

и

техническими возможностями СЗИ, позволяющих обеспечить безопасность информации при осуществлении такого доступа в корпоративных сетях с разными требованиями по защищенности

Гипотеза исследования

для повышения вероятности обеспечения безопасности информации при эксплуатации МАУ в корпоративных сетях и обеспечении безопасного доступа к услугам сетей с разными требованиями по защищенности необходимо разработать **модель безопасности МАУ и алгоритм, позволяющий управлять безопасностью** (программно-аппаратной конфигурацией) МАУ, согласовывая его с требованиями по ИБ и качеству предоставляемых услуг, в зависимости от условий предоставления доступа к услугам и ресурсам, в которых находится МАУ, а также научно-технические предложения по реализации системы управления безопасностью МАУ в корпоративных сетях с разными требованиями по защищенности

Постановка задачи диссертационного исследования

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

Научная задача:
на основе аналитического описания модели безопасности МАУ разработать алгоритм управления состоянием МАУ, учитывающий атрибуты доступа пользователей и МАУ, включая его местоположение, требования по качеству предоставляемых услуг, а также научно-технические предложения по реализации системы управления безопасностью МАУ, позволяющие повысить вероятность обеспечения безопасности информации при доступе к инфокоммуникационным услугам и информации корпоративных сетей с разными требованиями по защищенности при использовании единого МАУ

Научные положения, выносимые на защиту

1. Модель безопасности мобильного абонентского устройства, отличающаяся от известных учетом его местонахождения в корпоративных сетях с разными требованиями по защищенности
(3 статьи, 2 программы для ЭВМ)

2. Алгоритм управления безопасностью мобильного абонентского устройства, учитывающий атрибуты доступа мобильных пользователей
(2 статьи, 1 программа для ЭВМ)

3. Научно-технические предложения по практической реализации системы управления безопасностью мобильных абонентских устройств в корпоративных сетях
(1 статья, 3 программы для ЭВМ, 3 патента на изобретения)

Формальная постановка задачи

Исходные данные:

1) мобильное абонентское устройство ***MD*** и его технические характеристики

2) параметры помещений ***Rooms*** (расположение, требования по защищенности)

3) точки доступа ***AP*** беспроводной сети, их расположение и технические характеристики

4) совокупность атрибутов доступа ***A***

5) множество конфигураций МАУ ***CONF***

Ограничения и допущения:

1. В состав корпоративной сети входит доверенная беспроводная сеть передачи данных (БСПД)

2. Канал управления между доверенными точками доступа и МАУ защищен криптографическими средствами защиты информации

3. МАУ имеет возможность функционирования в различных программно-аппаратных конфигурациях

4. В составе МАУ функционирует аппаратно-программный модуль доверенной загрузки (АПМДЗ), являющийся агентом, управляющим программно-аппаратной конфигурацией МАУ

5. На МАУ функционирует доверенная операционная система (ДОС)

6. В ДОС МАУ создана изолированная программная среда (ИПС)

7. Пользователь МАУ в корпоративной сети аутентифицирован

Формальная постановка задачи

Требуется

1) разработать модель безопасности МАУ ***Z***, учитывающую вероятность нахождения МАУ в специальных помещениях

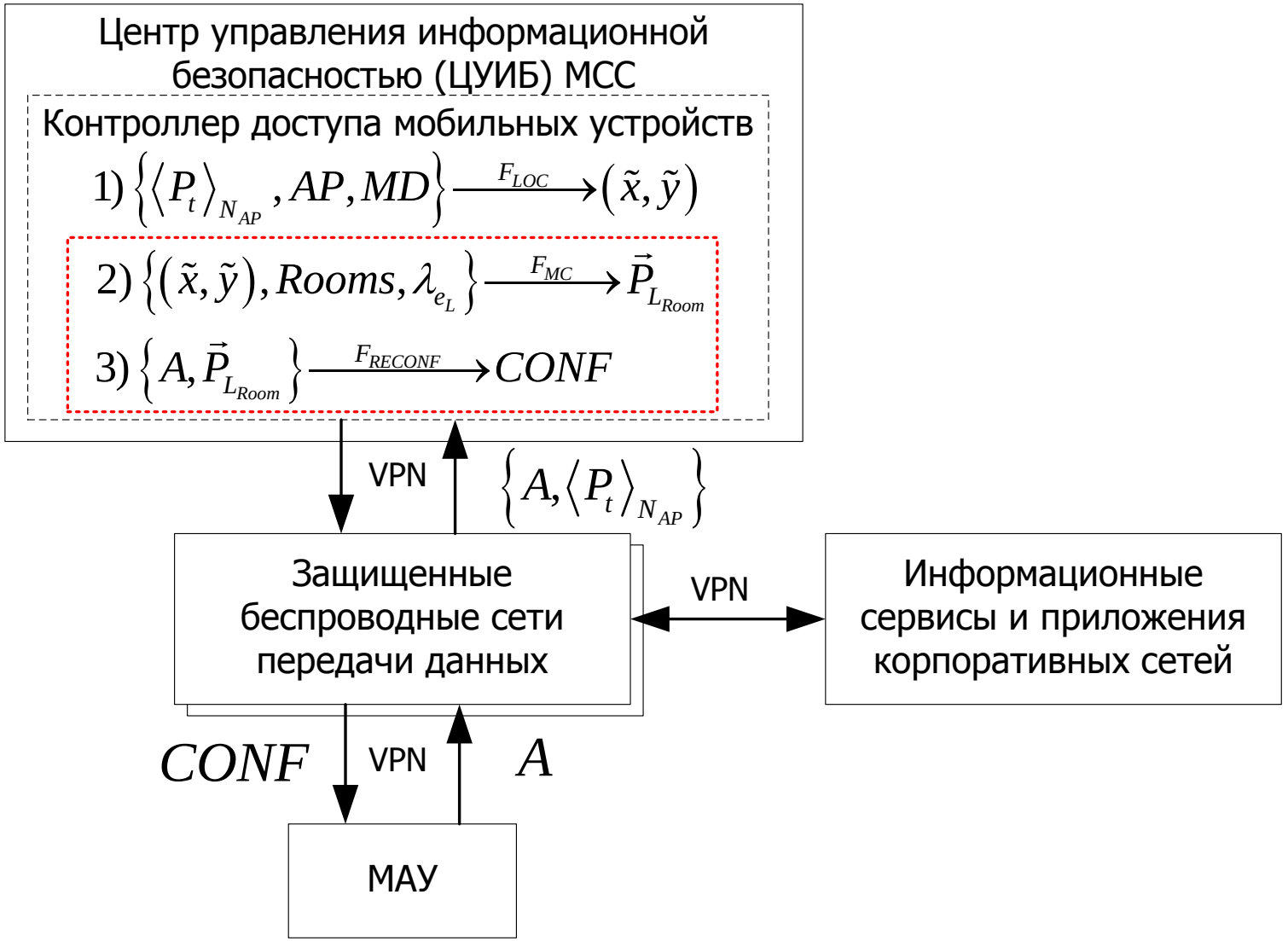
2) разработать алгоритм управления безопасностью МАУ путем реализации решающего правила ***F*** отнесения совокупности атрибутов доступа, включающих в себя, в том числе, вероятность нахождения МАУ в специальном помещении к разрешенной конфигурации (состоянию) МАУ, обеспечивающей безопасность информации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

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

$$\begin{cases} Z \xrightarrow{F(MD,Rooms,AP,A)} \{CONF_i\}_{t+1} & (1) \\ P_\beta\left(\tilde{L}_{Room} > L_{Room}\right) \le P_\beta^{\text{треб}} & (2) \\ T_{RECONF} \le T_{\text{RECONF}}^{\text{доп}} & (3) \end{cases}$$

Схема доступа к информации с использованием различных конфигураций МАУ в корпоративных сетях с разными требованиями по защищенности

Обобщенная схема доступа к информационным ресурсам с использованием управляемого МАУ



Показатели эффективности защиты информации при эксплуатации МАУ в корпоративных сетях с разными требованиями по защищенности

Вероятность обеспечения ЗИ при эксплуатации МАУ

$$P_{\text{ЗИМАУ}} = P\left(REZ \geq REZ^{\text{тр}}\right) \cap P\left(RES \leq RES^{\text{доп}}\right) \cap P\left(OPR \leq OPR^{\text{доп}}\right) \quad (1)$$

Результативность процесса защиты информации при эксплуатации МАУ (ГОСТ Р 50922-2006)

$$REZ = P_{\text{БИ}}(T) = P_{\text{КИ}}(T) \cdot P_{\text{ДИ}}(T) \cdot P_{\text{ЦИ}} \Big| P_{\text{ЦИ}} = 1 \quad (2)$$

Вероятность обеспечения конфиденциальности доступа (ГОСТ РВ 51987-2002)

$$P_{\text{КИ}}(T) = \left(1 - P_{\text{НСД}}\right) \cdot P_{\text{СК}}(T) \quad (3)$$

$$P_{\text{НСД}} = 1 - P\left(CONF \subset CONF^{\text{доп}}\right) = 1 - P\left[\beta\left(\tilde{L}_{Room} > L_{Room}\right) \leq \beta^{\text{доп}}\right] \quad (4)$$

$$P_{\text{СК}}\left(T_{RECONF}\right) = P\left[\left(T_{RECONF} \leq T_{RECONF}^{\text{доп}}\right) / \left(CONF \subset CONF^{\text{доп}}\right)\right] \cdot \left(1 - P_{\text{Пр3}}\right) \quad (5)$$

Вероятность обеспечения доступности информации (услуг) (ГОСТ РВ 51987-2002)

$$P_{\text{ДИ}}(T_{\text{ДИ}}) = \frac{N_{\text{ДУ}}}{N_{\text{У}}} \cdot P_{\text{св}}\left(T_{\text{ДИ}} \leq T_{\text{ДИ}}^{\text{зад}}\right) \Big| T_{\text{ДИ}}^{\text{зад}} = T_{RECONF}^{\text{доп}} \quad (6)$$

Ресурсоемкость процесса ЗИ при эксплуатации МАУ

$$RES = K_{\text{ИВР}} \cdot C_{\text{ВР}} + K_{\text{ИТР}} \cdot C_{\text{ТР}} + K_{\text{ИСУ}} \cdot C_{\text{СУМАУ}} + K_{\text{ИСОМ}} \cdot C_{\text{СОМ}} + \left(\sum_{i=1}^{N_{\text{МАУ}}} C_{\text{МАУ}_i}\right) \cdot N_{\text{Польз}} \quad (7)$$

1. Модель безопасности мобильного абонентского устройства, отличающаяся от известных учетом его местонахождения в корпоративных сетях с разными требованиями по защищенности

(3 статьи, 2 программы для ЭВМ)

Постановка задачи на разработку модели безопасности мобильного абонентского устройства

Недостатки существующих моделей безопасности применительно к МАУ:

- не учитывается вероятностный характер процесса определения местоположения как координат пользователей и устройств либо помещений, в которых находятся пользователи МАУ

- в качестве СЗИ в КС не используются возможности управления программно-аппаратной конфигурацией МАУ, позволяющие ограничивать доступы, представляющие в определенных условиях угрозы ИБ

Требуется:

разработать модель безопасности МАУ, отличающуюся от известных учетом его местонахождения в корпоративных сетях с разными требованиями по защищенности, при этом

а) обосновать безопасность системы, использующей предложенную модель

б) повысить достоверность оценивания местоположения МАУ до уровня, позволяющего определить помещение с заданными параметрами защищенности, не ниже требуемого

Элементы базовой модели Белла-ЛаПадулы в формальной модели безопасности МАУ

S множество субъектов системы

MD **множество МАУ, при этом** $MD \subseteq S$

O множество объектов системы

$P = \{read, write, append, execute\}$ множество видов доступа

$B = \{b \subseteq S \times O \times R\}$ множество возможных множеств текущих доступов в системе

$M = \{m_{|S|\times|O|}\}$ множество возможных матриц доступов

$(L, \leq)$ решетка уровней конфиденциальности

$L = \{"ОИ", "КИ"\}$ $"ОИ" < "КИ"$

$(f_s, f_o, f_c, f_{loc}) \in F = L^S \times L^O \times L^S$ четверка функций, задающих уровни конфиденциальности субъектов, объектов, **местоположения**, текущий уровень конфиденциальности субъектов

$f_s : S \to L$ $f_c : S \to L$

$f_o : O \to L$ $f_{loc} : LOC \to L$

$V = B \times M \times F$ множество состояний системы

Q множество запросов к системе

D множество решений по запросам $\{yes, no, error\}$

$W \subseteq Q \times D \times V \times V$ множество действий системы

$\mathbb{N}_0 = \{0, 1, 2, ...\}$ множество значений времени

X множество функций $x : \mathbb{N}_0 \to Q$

Y множество функций $y : \mathbb{N}_0 \to D$

Z множество функций $z : \mathbb{N}_0 \to V$

Система

$$\Sigma(Q, D, W, z_0) \subseteq X \times Y \times Z$$

безопасна, когда обладает

***ss* - свойством**

запрет чтения вверх

запрет записи для $f_s(s) < f_o(o)$

*** - свойством**

запрет информационного потока "сверху вниз"

***ds* - свойством**

свойства дискреционной безопасности

Элементы мандатно-ролевого управления доступом в 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

$SA: S \to 2^R$ функция, задающая для каждого субъекта множество ролей, на которые он может быть авторизован

$user: SS \to S$ 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**

$roles: SS \to 2^R$ функция, задающая для субъекта (пользователя) множество ролей, на которые он авторизован в данной сессии

$confs: SS \to 2^R$ **функция, задающая для субъекта (МАУ) множество конфигураций, на которые он авторизован в данной сессии**

Элементы атрибутной политики безопасности, учитывающей особенности программно-аппаратных конфигураций МАУ и его местоположение в формальной модели безопасности МАУ

$A = \{a_i\}$ **атрибуты доступа пользователя МАУ**

- идентификационные данные о пользователе, мобильном абонентском устройстве, операционной системе (ОС) и приложениях МАУ
- сетевая адресная информация
- уровень конфиденциальности и услуги (ресурса, приложения)
- время запроса на доступ

LOC **множество возможных местоположений**

$\mathrm{MA} = \{ma_{|CONF|\times|A|}\}$ множество возможных матриц атрибутов доступа

$ma_{|CONF|\times|A|}$ матрица требуемых атрибутов доступа

$ma[conf, a] \subseteq A$ множество требуемых значений атрибутов доступа для конфигурации *conf*

$Rooms = \{room_i = ((x_{i1}, y_{i1}), (x_{i2}, y_{i2}), ..., (x_{in}, y_{in}), L_{Room_i})\}$ расположение и другие параметры помещений

$AP = \{AP_j = (x_j, y_j)\}$ расположение точек доступа БСПД

Особенности модели безопасности МАУ

Субъекты доступа - **МАУ**

Таблица 1 Примерный состав функциональных модулей (**объектов доступа**) управляемой конфигурации МАУ

Функциональные модули МАУ		
АПМДЗ	Модуль Bluetooth	Модуль дисплея
ПЗУ(о)	Модуль Wi-Fi	Модуль клавиатуры
ПЗУ(к)	Модуль GSM	Виброзвонок
ОЗУ(о)	Модуль USB	Модуль тачскрина
ОЗУ(к)	Модуль шифратора	Модуль фото- и видеокамеры
ЦП(о)	Модуль аудиокодека	Модуль акселероментра
ЦП(к)	Микрофон	Модуль ГЛОНАСС
SIM-карта	Динамик	

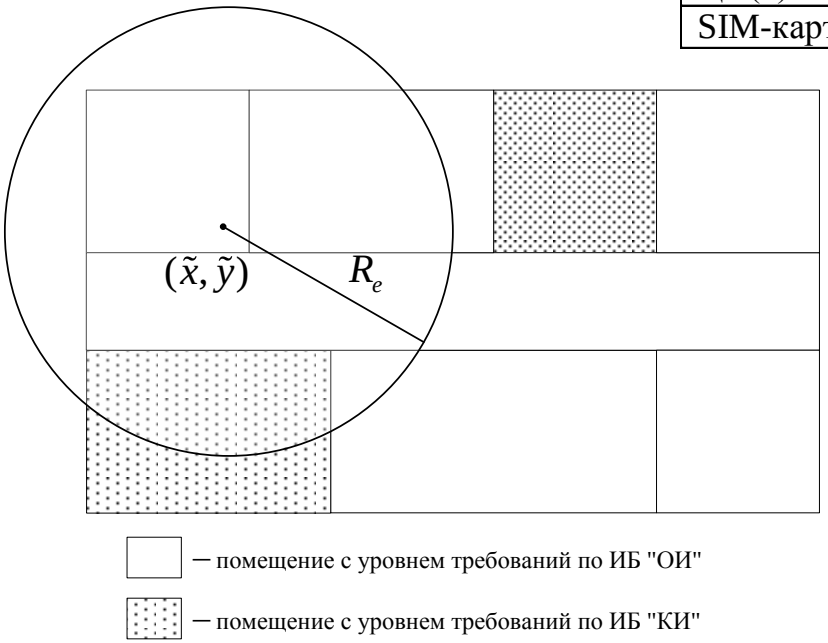


Рис 1 Погрешность определения местоположения МАУ в помещениях внутри здания

Оценивание местоположения МАУ в здании с развернутыми корпоративными сетями с разными требованиями по защищенности

Свойства модели безопасности МАУ

Свойство простой безопасности (выполняется одно из условий):

$p \in \{execute, append\}$

$p \in \{read, write\}$

*** - свойство** (выполняется одно из условий):

$p \in execute$

$p \in append$ и $f_o(o) \geq f_s(s)$

$p \in read$ и $f_c(s) \geq f_o(o)$

$p \in write$ и $f_c(s) = f_o(o)$

as-свойство атрибутной безопасности (одновременно выполняются условия):

$f_{LOC}(loc) = f_s(confs(ss))$

$f_{LOC}(loc) = f_s(user(ss))$

$\left(\forall a \in A \exists a^{\text{треб}} \in A^{\text{треб}} : a = a^{\text{треб}} \text{ и } a^{\text{треб}} \in ma[conf, a]\right)$

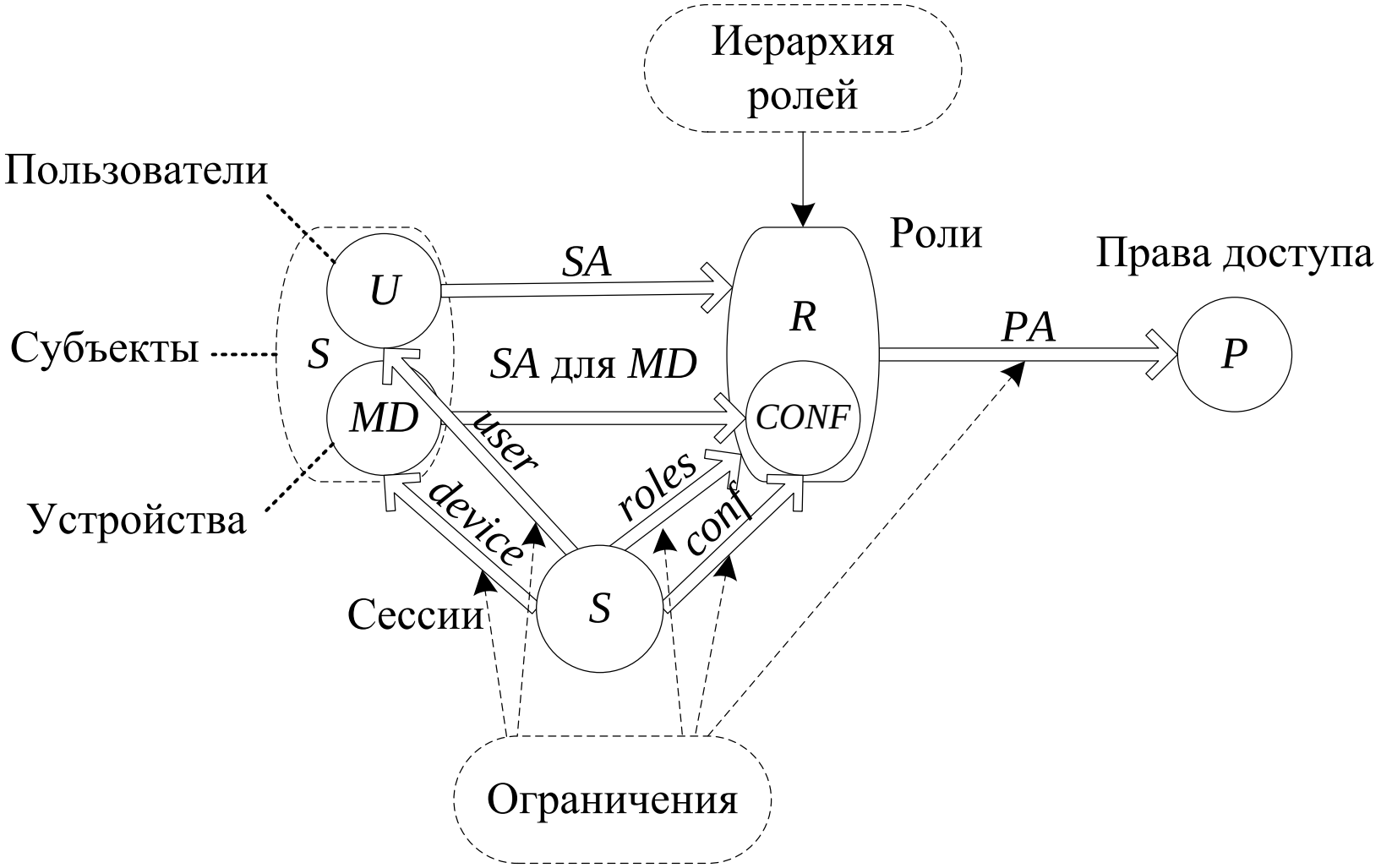
Проверка безопасности системы для описанных свойств

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 $(s,o,p)\in b^*\setminus b$ обладает *as*-свойством относительно f^*.

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

Дополнения к мандатной ролевой модели управления доступом в формальной модели безопасности МАУ



Обоснование невозможности возникновения запрещенных информационных потоков от объектов с высоким уровнем конфиденциальности к объектам с низким уровнем конфиденциальности

Определение 19. 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 $r, r' \in confs(ss)$.

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'.

Определение требований по защищенности (уровень конфиденциальности) местоположения

Исходные данные:

1) МАУ и его технические характеристики MD

2) расположение и параметры помещений

$$Rooms = \left\{ room_i = \left((x_{i1}, y_{i1}), (x_{i2}, y_{i2}), ..., (x_{in}, y_{in}), L_{Room_i} \right) \right\}$$

$$i = \overline{1, N}_{Rooms}$$

3) расположение точек доступа беспроводной сети

$$AP = \left\{ AP_j = \left(x_j, y_j \right) \right\} \qquad j = \overline{1, N}_{AP}$$

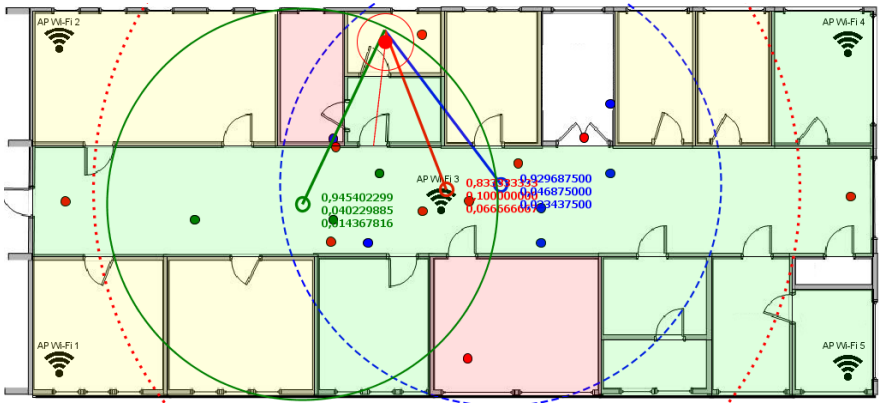


Рис. 1 Схема помещений с разными требованиями по защищенности

Входные данные: $\langle P_t \rangle_{N_{AP}}$ – измерения уровня сигнала МАУ точками доступа БСПД с известными координатами и техническими характеристиками

$Rooms$ – параметры и расположение помещений

AP – точки доступа БСПД с известными координатами и техническими характеристиками

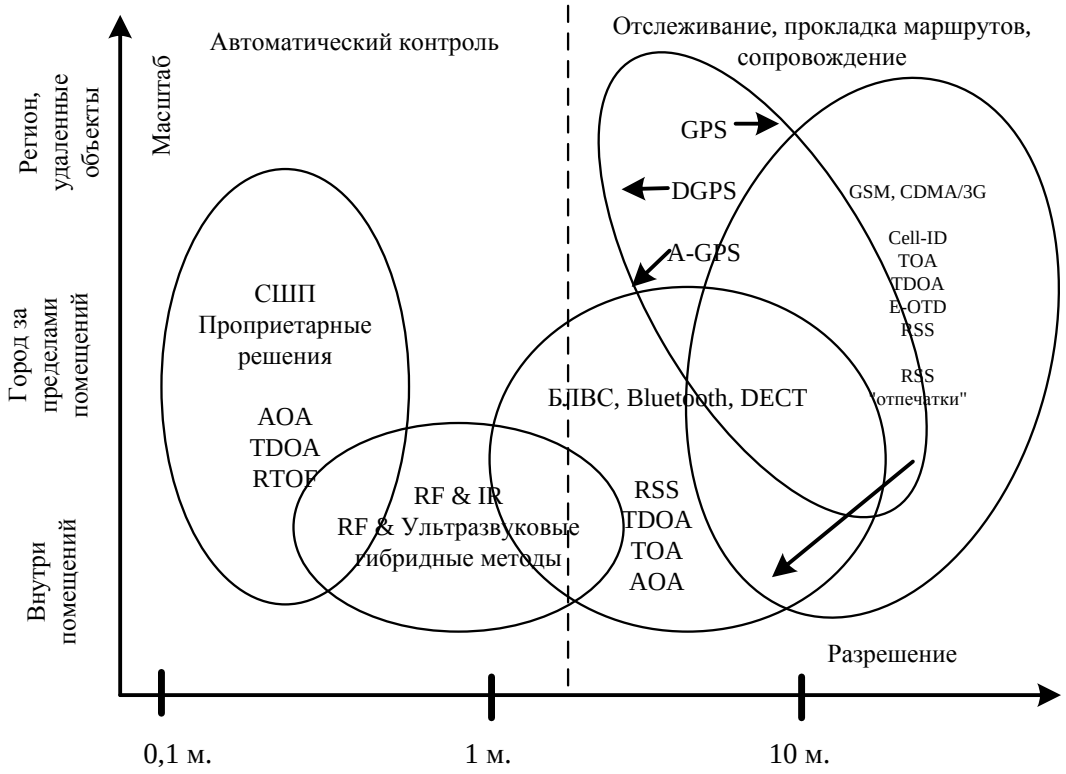
MD – МАУ и их технические характеристики

Выходные данные: $\vec{P}_{L_{Room}}$ – вероятность нахождения МАУ в помещениях с теми или иными требованиями по защищенности

Технологии определения местоположения

1. GSM/CDMA/3G/LTE
2. **RFID/Bluetooth/Wi-Fi**
3. УКВ/СШП
4. IP-адрес
5. Лазеры (лазерные дальномеры)
6. ВОЛС
7. Встроенные датчики ориентации в пространстве (гироскоп, альтиметр, 3Д-акселерометр)
8. GPS/ГЛОНАСС/Galileo/Beidou

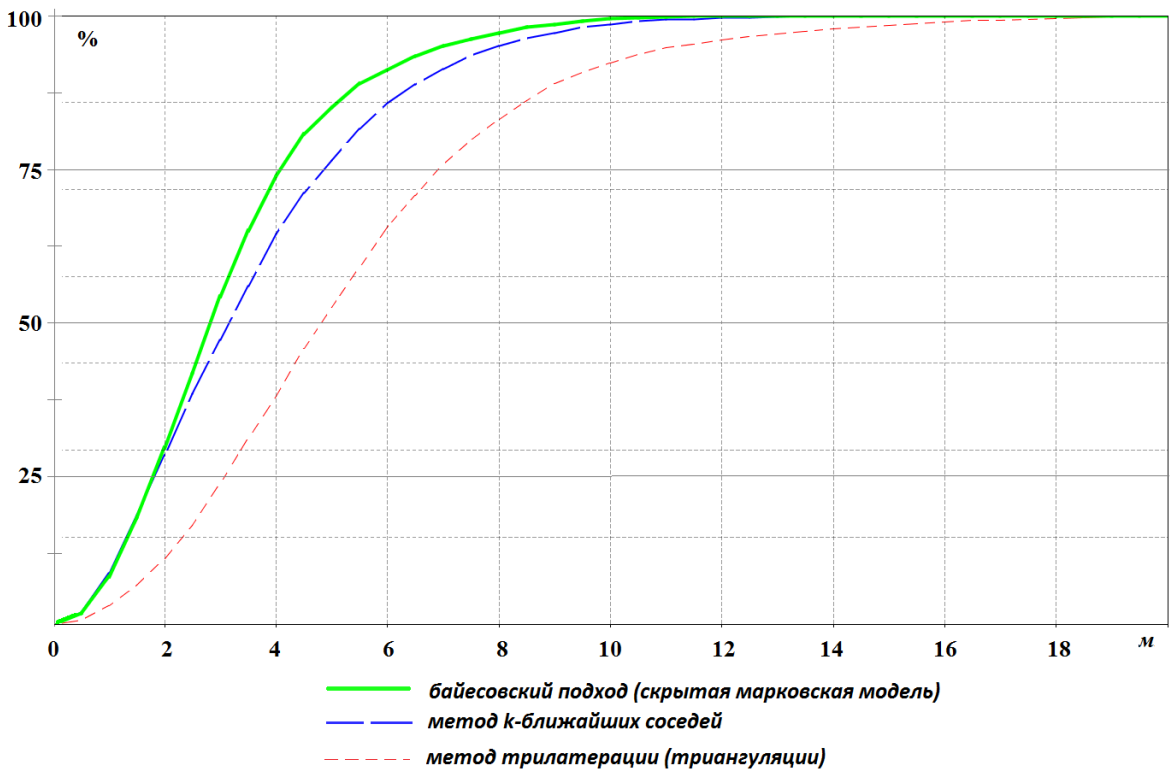
Обзор современных беспроводных технологий определения местоположения



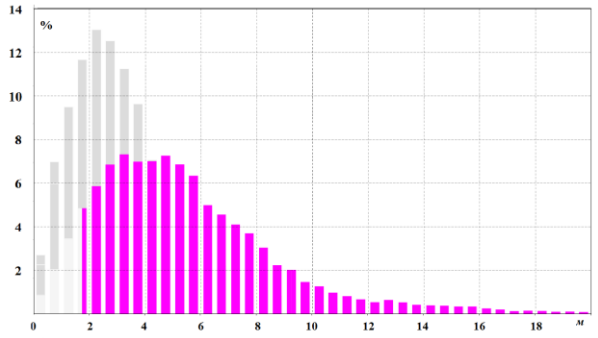
Системы и технические решения по определению местоположения МАУ внутри помещений на основе беспроводных технологий

№ п/п	Система / Тех. решение	Беспроводная технология	Алгоритм определения местоположения	Точность	Погрешность	Масшт-ть / Разреш.	Стоим.
1	**Microsoft RADAR**	**WLAN, RSS**	**K NN, алгоритм Витерби**	**3-5 м.**	**50 % при 2,5 м, 90 % при 5,9 м**	**Хор. / 2D, 3D**	**Низ.**
2	Horus	WLAN, RSS	Вероятностный метод	2 м.	90 % при 2.1 м.	Хор. / 2D	Низ.
3	DIT	WLAN, RSS	Нейр.сети/МОВ/стат. метод	3 м.	90 % при 5,12 м. для МОВ, 90 % при 5,4 м. при МСП	Хор. / 2D, 3D	Низ.
4	Ekahau	WLAN, RSS	Вероятностный метод	1 м.	50 % при 2 м.	Хор. / 2D	Низ.
5	SnapTrack	GPS, TDOA		5 м. – 50 м.	50 % при 25 м.	Хор. / 2D, 3D	Ср.
8	LANDMARC	Активный RFID, RSS	K NN	< 2 м.	50 % при 1 м.	Узлы разм. плотно	Низ.
9	**Robot-based**	**WLAN, RSS**	**Байесовский подход**	**1,5 м.**	**Более 50 % при 1,5 м.**	**Хор. / 2D**	**Ср.**
10	MultiLoc	WLAN, RSS	SMP (Symmetric Multiprocessing)	2,7 м.	50 % при 2,7 м.	Хор. / 2D	Ср.
11	**TIX**	**WLAN, RSS**	**TIX**	**5,4 м.**	**50 % при 5,4 м.**	**Хор. / 2D**	**Ср.**
12	PinPoint 3D-1D	УКВ (40МГц), RTOF	Байессовский подход	1 м.	50 % при 1 м.	Хор. / 2D	Низ.
13	GSM-"почерк"	GSM, RSS	Взвешенный K NN	5 м.	80 % при 10 м.	Отл. / 2D, 3D	Ср.

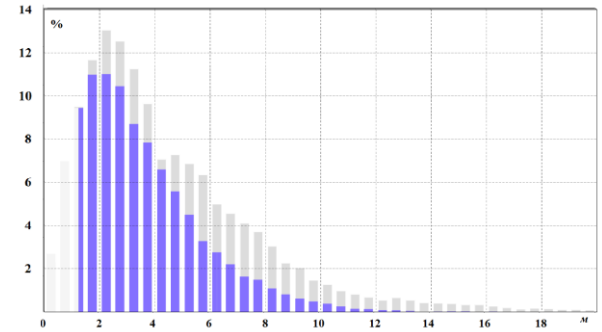
Сравнительный анализ точности исследуемых технологий



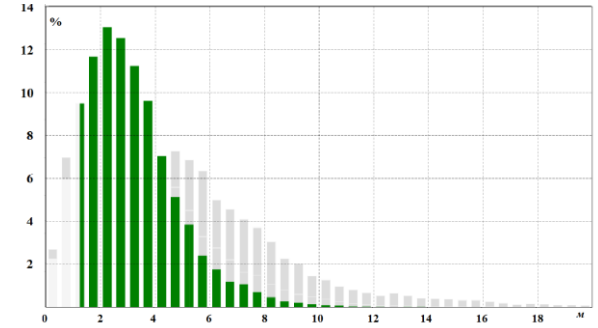
а)



б)



в)



а) трилатерация
б) метод *k*-ближайших соседей
в) байесовский подход

Оценивание вероятности местонахождения МАУ в специальном помещении за счет использования численного метода статистических испытаний (метода Монте-Карло)

$$e_L = \sqrt{(x-\tilde{x})^2 + (y-\tilde{y})^2} \quad (1) \qquad R_e = \max[e_L] \quad (2)$$

$$Rooms = \left\{ Room_i = \left(\langle (x_{i1}, y_{i1}), \ldots, (x_{iN}, y_{iN}) \rangle, L_{Room_i,} \right) \right\} \quad (3)$$

$$\lambda_{e_L} = \left\{ R_e, P\{a \le e_L < b\} = \sum_{a \le e_L < b} p(e_L) \,\middle|\, \sum_{0 \le e_L \le R_e} p(e_L) = 1 \right\} \quad (4)$$

$$P(\tilde{L}_{Room} = L_{Room}) = \frac{F_{Sq}\left(L_{Room}, (\tilde{x}, \tilde{y}), R_e\right)}{\pi \cdot R_e^2} \quad (5)$$

$$\vec{P}_{L_{Room}} = \left\{ P\left(\tilde{L}_{Room} = \text{"ОИ"}\right), P\left(\tilde{L}_{Room} = \text{"КИ"}\right) \right\} \quad (6)$$

Реализация метода статистических испытаний

$$(x_i', y_i') \,|\, \lambda_{e_L}, i = \overline{1, N_{MC}} \quad (7)$$

$$\tilde{L}_{Room} = F_{L_{Room}}\left((x_i', y_i'), Rooms\right) \quad (8)$$

$$N\left(L_{Room_i}\right) := N\left(L_{Room_i}\right) + 1 \quad (9)$$

$$F_{Sq}\left(L_{Room}, (\tilde{x}, \tilde{y}), R_e\right) = \frac{N\left(L_{Room}\right)}{N_{MC}} \quad (10)$$

$$\vec{P}_{L_{Room}} = \left\{ \frac{N(\tilde{L}_{Room} = \text{"ОИ"})}{N_{MC}}, \frac{N(\tilde{L}_{Room} = \text{"КИ"})}{N_{MC}} \right\} \quad (11)$$

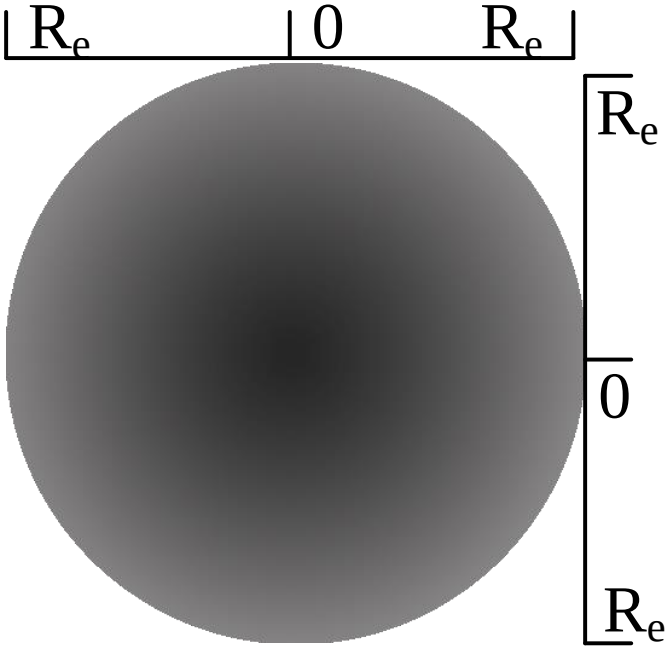


Рис. 1 Плотность распределения ошибок определения местоположения относительно координат найденной точки (центра окружности)

Принятие решения о местонахождения МАУ в специальном помещении за счет использования численного метода статистических испытаний (метода Монте-Карло)

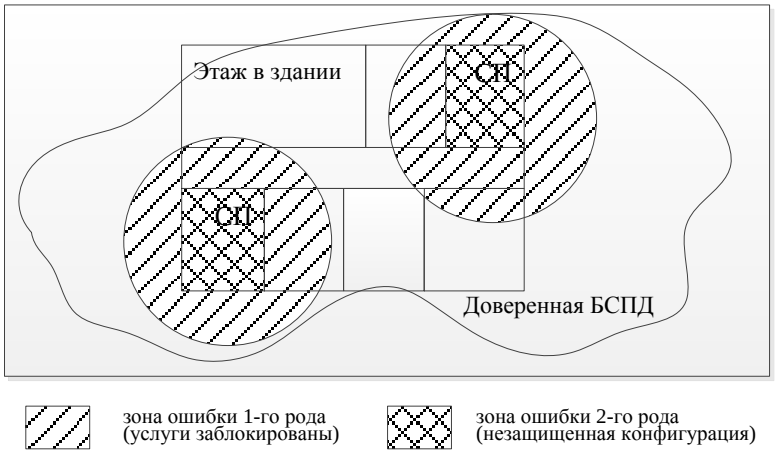
Принятие решения о **блокировании запрещенного режима работы** МАУ

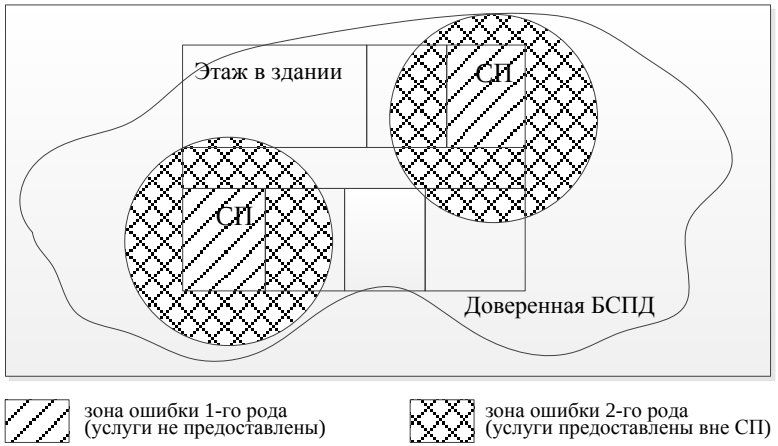
$$\tilde{L}_{Room} = \begin{cases} \text{"ОИ / КИ"}, \text{ при } P\left[\left(\frac{N(\tilde{L}_{Room} = \text{"КИ"})}{N_{MC}}\right) \geq N^{\text{треб}}_{\text{блок}}\right] \\ \text{"ОИ"}, \text{ при } P\left[\left(\frac{N(\tilde{L}_{Room} = \text{"КИ"})}{N_{MC}}\right) < N^{\text{треб}}_{\text{блок}}\right] \end{cases}$$

Принятие решения о **предоставлении защищенных услуг** пользователю МАУ

$$\tilde{L}_{Room} = \begin{cases} \text{"КИ"}, \text{ при } P\left[\left(\frac{N(\tilde{L}_{Room} = \text{"КИ"})}{N_{MC}}\right) \geq N^{\text{треб}}_{\text{дост}}\right] \\ \text{"ОИ"}, \text{ при } P\left[\left(\frac{N(\tilde{L}_{Room} = \text{"КИ"})}{N_{MC}}\right) < N^{\text{треб}}_{\text{дост}}\right] \end{cases}$$

$$N^{\text{треб}}_{\text{блок}} < N^{\text{треб}}_{\text{дост}}$$





Эффективность определения местоположения МАУ

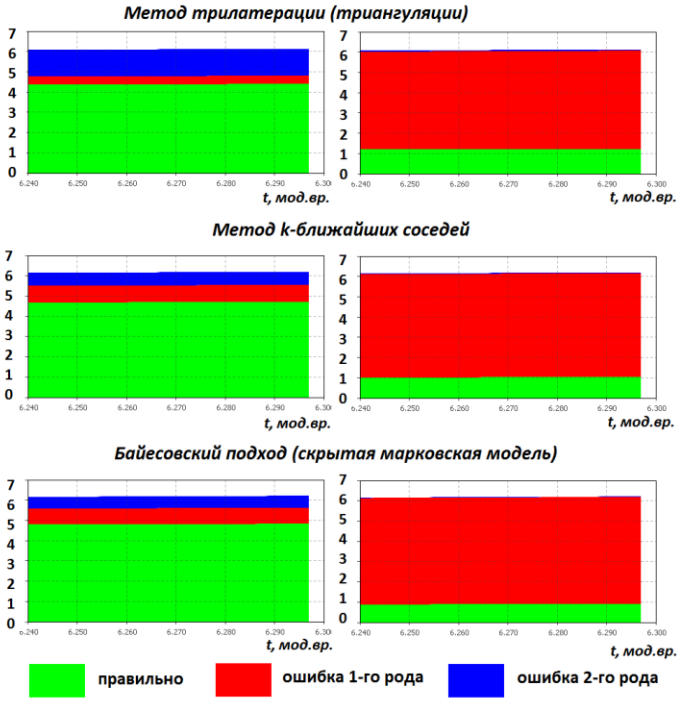


Рис.1 Статистика ошибок 1-го и 2-го рода

№ п/п	Метод (комбинация методов)	Правильно		Ошибка 1-го рода		Ошибка 2-го рода	
		Пр-п	**Сист.**	**Пр-п**	**Сист.**	**Пр-п**	**Сист.**
1.	Трилатерация (триангуляция)	68,966	34,255	6,521	59,378	**24,511**	**6,366**
2.	K-ближайших соседей	71,66	16,528	14,516	79,83	**13,823**	**3,641**
3.	Байесовский подход	73,172	10,341	14,578	87,653	**12,249**	**2,004**
4.	1,2	71,934	6,255	8,982	93,225	**19,083**	**0,519**
5.	1,3	72,069	8,349	9,615	90,997	**18,314**	**0,653**
6.	2,3	75,728	15,055	10,44	82,88	**13,831**	**2,064**
7.	1,2,3	76,327	8,727	7,938	90,235	**15,786**	**1,037**

Статья. Вестник РГРТУ. 2015. № 54-1. С. 32-39

Свидетельства (ФИПС)
№№ 2013618388, 2015615631

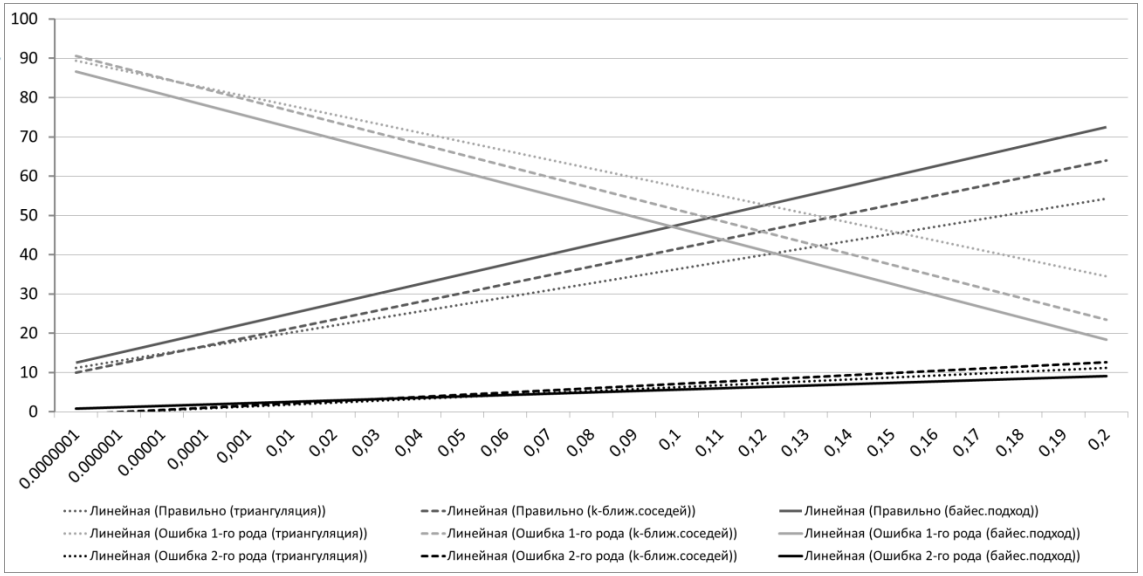


Рис.2 Зависимость ошибок 1-го и 2-го рода от значения порога принятия решения

2. Алгоритм управления безопасностью мобильного абонентского устройства, учитывающий атрибуты доступа мобильных пользователей

(2 статьи, 1 программа для ЭВМ)

Алгоритм управления безопасностью мобильного абонентского устройства

Постановка задачи на разработку алгоритма

$$f\left(S^*\right) \longrightarrow \max \quad (1)$$

$$\sum_{i=1}^{|S^*|} V_{lm}^{S_i^*} \le \hat{V}_{lm} \quad (2)$$

$$S^* = F_S\left(CONF^*\right) \Big| CONF^* \in CONF^{\text{доп}}, S^* \subseteq S \quad (3)$$

Исходные данные:

$$\{CONF_i\}, i = \overline{1,|CONF|}, CONF = \{M, f_t, P_t\} \quad (4)$$

$$A = \{a_i\}, i = \overline{1,N_A}, N_A = |A| \quad (5)$$

$$AP = \left\{AP_j = \left(x_j, y_j\right)\right\}, j = \overline{1,N_{AP}}, N_{AP} = |AP| \quad (6)$$

$$Rooms = \left\{Room_i = \left(\langle (x_{i1}, y_{i1}), \ldots, (x_{iN}, y_{iN}) \rangle, L_{Room_i,}\right)\right\} \quad (7)$$

$$MAP_{P_t} = \left\{\left(x_i, y_i\right), \lambda_{P_t}\right\}, i = \overline{1,N}_{MAP} \quad (8)$$

$$\lambda_{e_L} = \left\{ R_e, P\{a \le e_L < b\} = \sum_{a \le e_L < b} p(e_L) \Big| \sum_{0 \le e_L \le R_e} p(e_L) = 1 \right\} \quad (9)$$

Критерии защищенности и качества услуг:

Матрица нормативов информационной скорости предоставляемых пользователям услуг

$$\text{VS} = \left|vs_i\right|, i = \overline{1,|S|} \quad (10)$$

Матрица атрибутов доступа (политика безопасности МАУ)

$$\text{SEC} = \begin{vmatrix} CONF_0 & a_{00} & \ldots & a_{0N_A} & L_0 \\ CONF_1 & a_{10} & \ldots & a_{1N_A} & L_1 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ CONF_{N_{CONF}} & a_{N_{CONF}0} & \ldots & a_{N_{CONF}N_A} & L_{N_{CONF}} \end{vmatrix} \quad (11)$$

Решающее правило политики безопасности для определения допустимых конфигураций МАУ

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

$$: \left(\forall CONF_i \in CONF^{\text{доп}} \; \exists L_{Room}^{\text{треб}} = F_{L_{Room}}\left(CONF_i\right)\right) \wedge \quad (12)$$

$$\wedge \left(\forall a_i \in A_i \; \exists a_i^{\text{треб}} \in A_i^{\text{треб}} = F_A\left(CONF_i\right) : a_i = a_i^{\text{треб}}\right)$$

Управление безопасностью МАУ

Уравнение наблюдения (1)

$$Y^*(t) = g\left[t, x(t), Z^*(t)\right]$$

$$Y^*(t) = \left\langle A(t), \vec{P}_{L_{Room}}(t), h(conf^*, t)\right\rangle$$

$$Z^*(t) = conf^* \in CONF$$

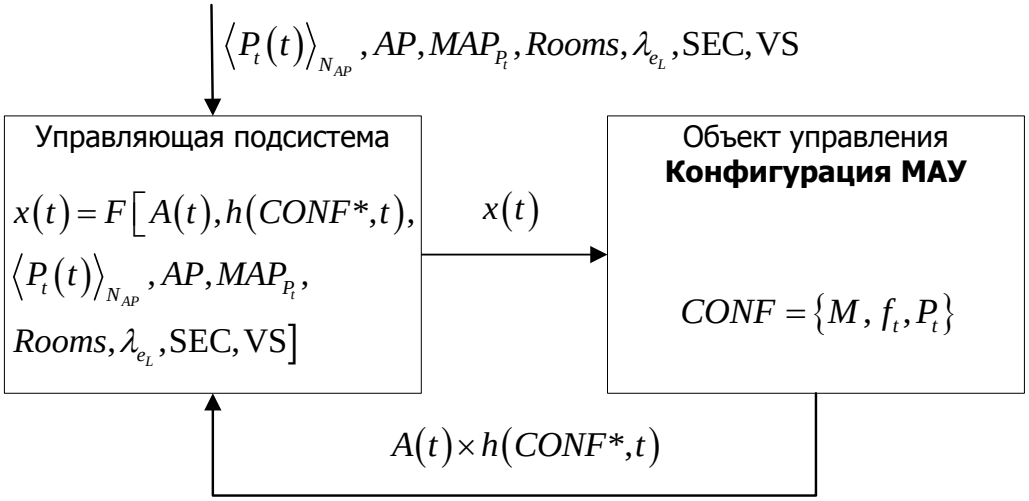


Рис 1 Цикл управления безопасностью МАУ

Уравнение состояния (2)

$$Z(t) = f\left[Z(t_0), x(\tau)\right], \tau \in [t_0, t]$$

$$Z(t) = conf \in CONF$$

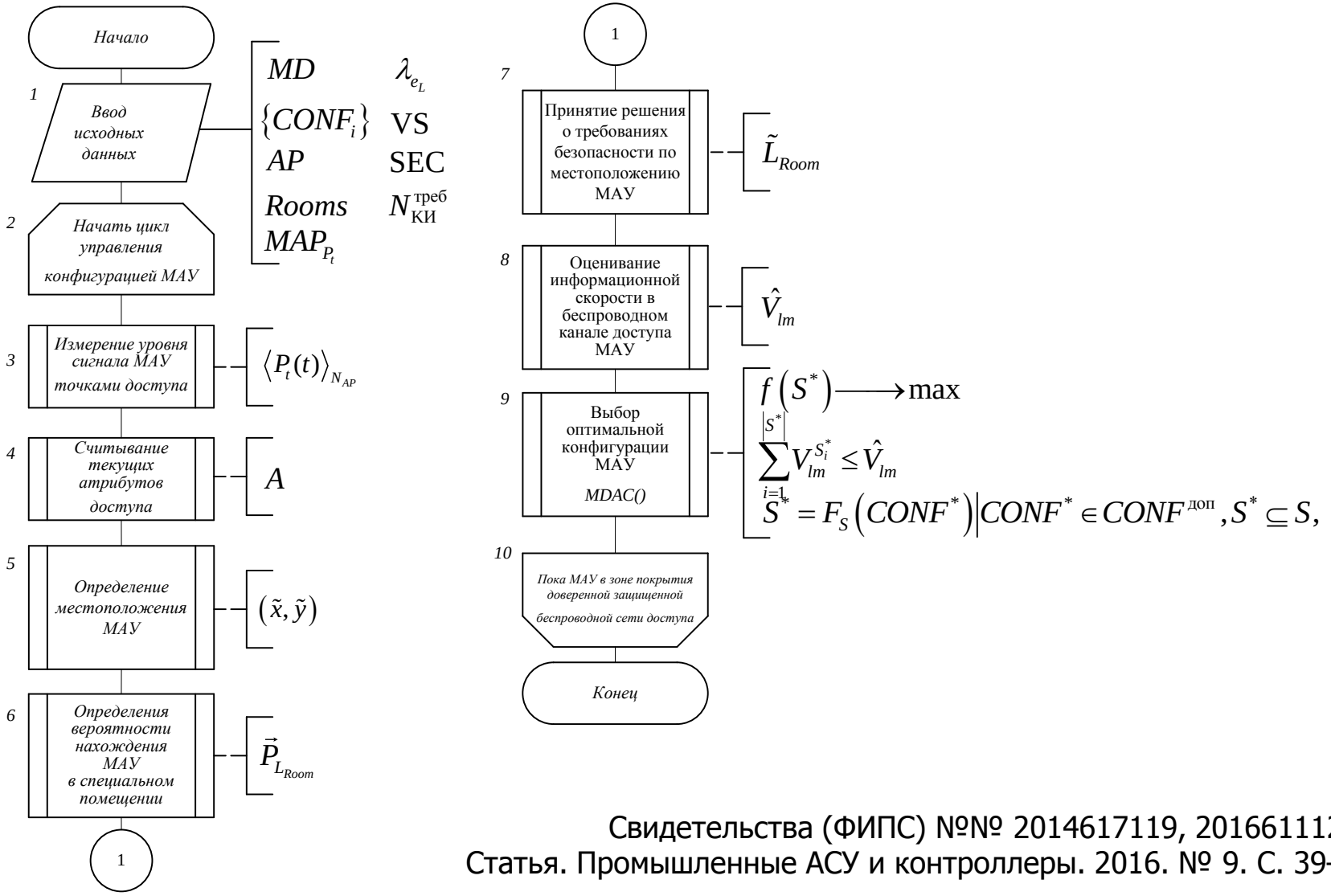
Цель управления (3)

$$\max\left[P_{\text{БИ}}(T)\right] = P_{\text{КИ}}(T) \cdot P_{\text{ДИ}}(T) \cdot P_{\text{ЦИ}} \left| P_{\text{ЦИ}} = 1 \right.$$

Конфигурация	Кат. пом.	Атрибуты доступа			
		Время	ID МАУ	User	...
$CONF_0$	∞	∞	∞	∞	...
$CONF_1$	L_O	∞	5,29,53,...	3,7,12,...	...
$CONF_2$	L_O	8^{00}-17^{30}	7,11,52,...	9,17,23,..	...
$CONF_3$	L_O	∞	13,17,...	5,11,...	...
$CONF_4$	L_K	16^{00}-17^{00}	17	5	...
$CONF_5$	L_K	∞	13	1	...
$CONF_6$	L_K	11^{00}-13^{00}	17,21	11,27	...

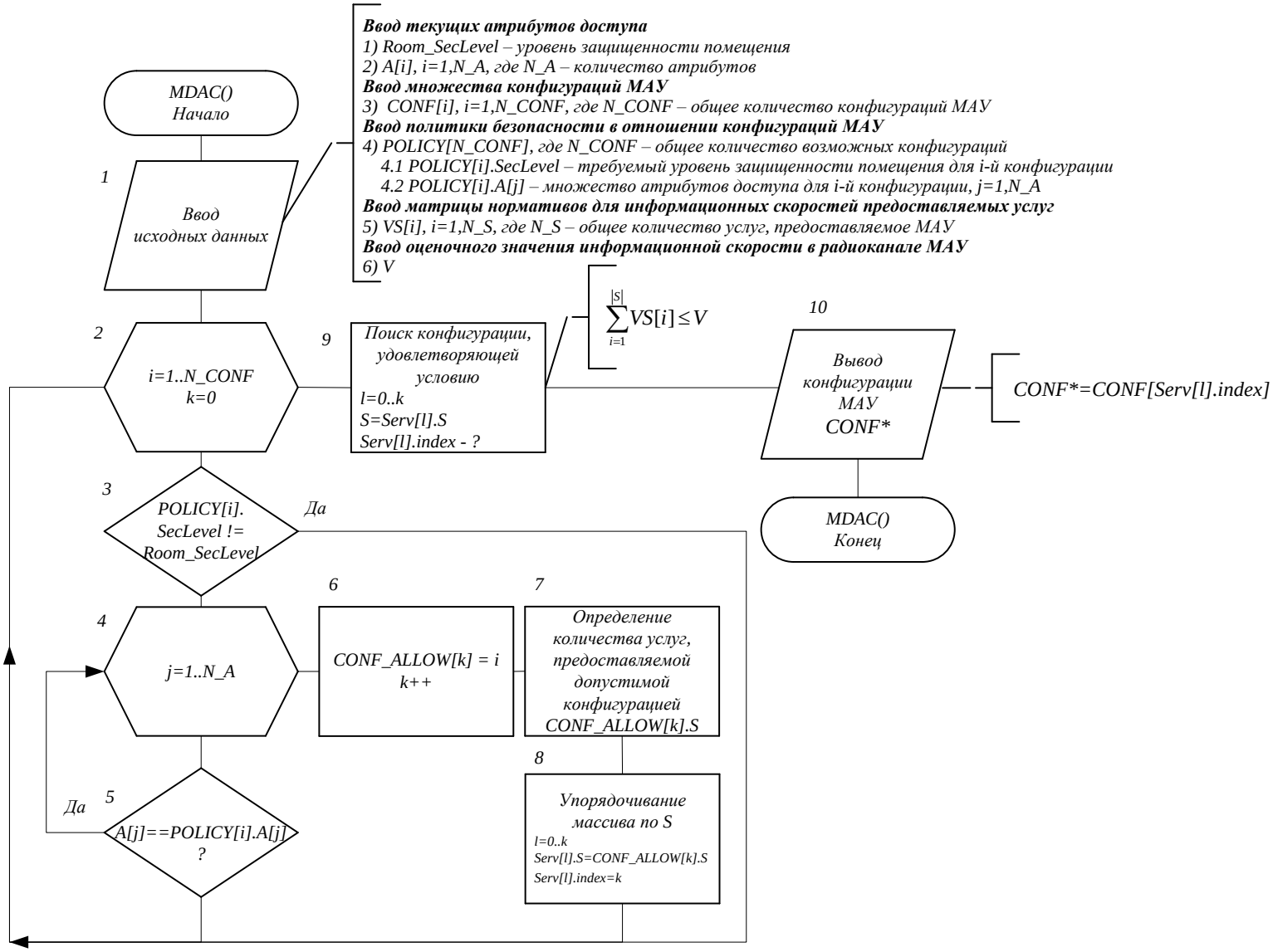
Таблица 1 Пример таблицы политики безопасности мобильных абонентских устройств (МАУ)

Алгоритм управления конфигурацией мобильного абонентского устройства



Свидетельства (ФИПС) №№ 2014617119, 20166111210
Статья. Промышленные АСУ и контроллеры. 2016. № 9. С. 39–50

Выбор оптимальной конфигурации МАУ



Оценка свойств алгоритма управления конфигурацией мобильного абонентского устройства

Временная сложность

$$S_t = t_{\text{иниц}} + t_{\text{обучен}} + t_{\text{местопол}} + t_{SR} + t_{\text{ПЗМУ}} \quad (1)$$

$$S_t = C_1\left(N_{AP} \cdot N_{Int} + k \cdot N_{HMM}\right) + C_2 \cdot N_{MC} \cdot N_{Int} \cdot N_{Rooms} \quad (2)$$

$$T_{RECONF} = T_{RSS} + T_{LOC} + T_{REQ} + T_{POLICY} + T_{RESP} + T_{CONF} \quad (3)$$

Сложность по памяти

$$S_v = N_{AP} \cdot N_{Int} \cdot N_{HMM} + N_{Rooms} \quad (4)$$

Точность

$$\delta \approx 10^{-4} \quad (5)$$

Алгоритм (процедура)	Параметр	Временная сложность, мс
Инициализация исходных данных	$T_{\text{иниц}}$	0,01
Алгоритм определения местоположения – на основе метода трилатерации – на основе метода *k*-ближайших соседей – на основе байесовского подхода	T_{LOC}	 0,98 1,01 2,92
Алгоритм определения вероятности местонахождения МАУ в специальном помещении	T_{POLICY}	710
Алгоритм оценивания информационной скорости в беспроводном канале доступа	T_V	0,3
Алгоритм формирования оптимальной конфигурации МАУ	T_{CONF}	1,12
Итого:	S_t	714,35

Рис. 1 Оценки временной сложности процедур алгоритма управления безопасностью МАУ

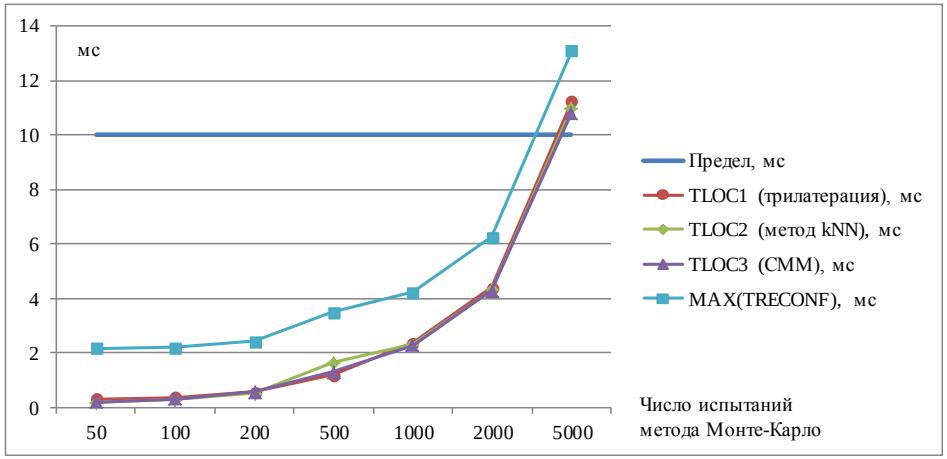


Рис. 2 График зависимости времени переконфигурации МАУ от вычислительной сложности

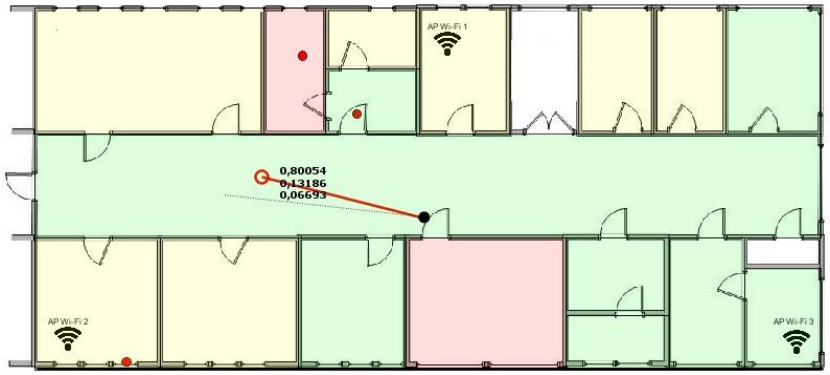
Статья. Промышленные АСУ и контроллеры. 2016. № 9. С. 39–50
Статья. Информационные технологии. 2015. № 9 (21). С. 611–618

3. Научно-технические предложения по практической реализации системы управления безопасностью мобильных абонентских устройств в корпоративных сетях

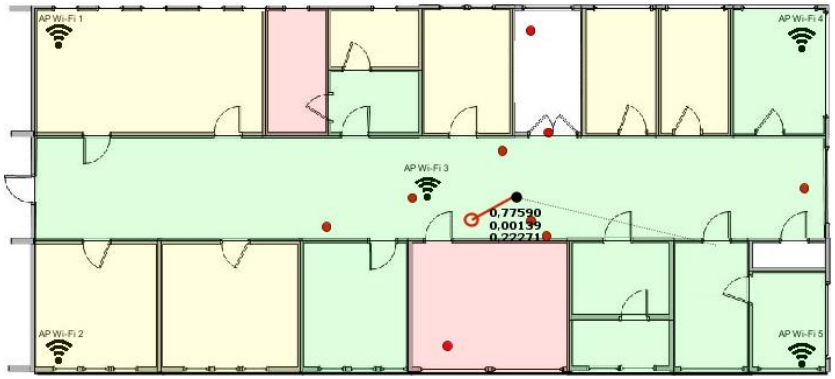
(1 статья, 3 программы для ЭВМ,
3 патента на изобретения)

Рекомендации по формированию оптимальных параметров системы определения местоположения

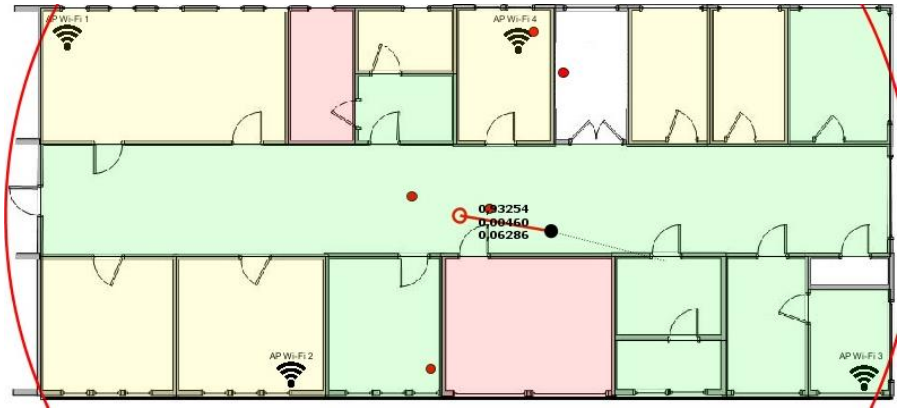
Оптимальное расположение ***N*** точек доступа для заданной карты расположения помещений



N=3



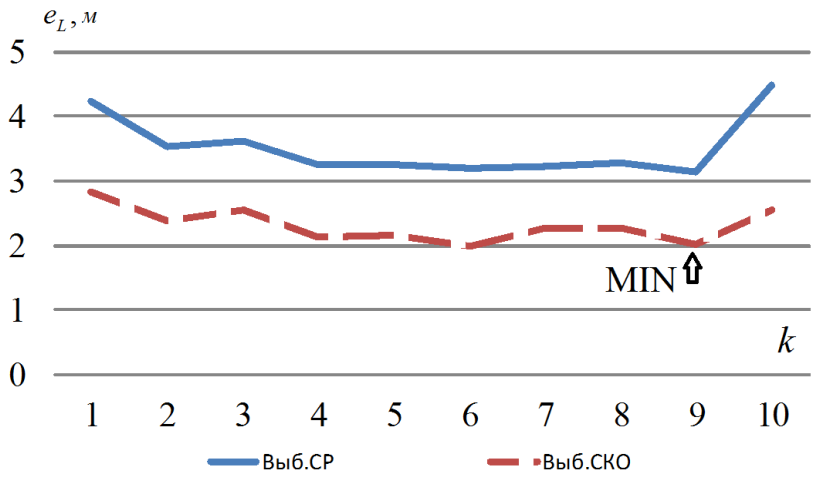
N=4



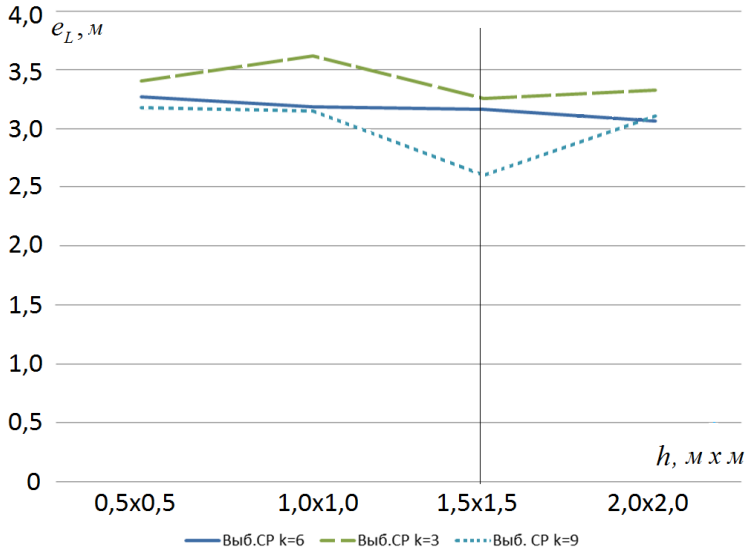
N=5

Рекомендации по формированию оптимальных параметров системы определения местоположения

Оптимальные параметры метода ***k***-ближайших соседей для заданной карты расположения помещений



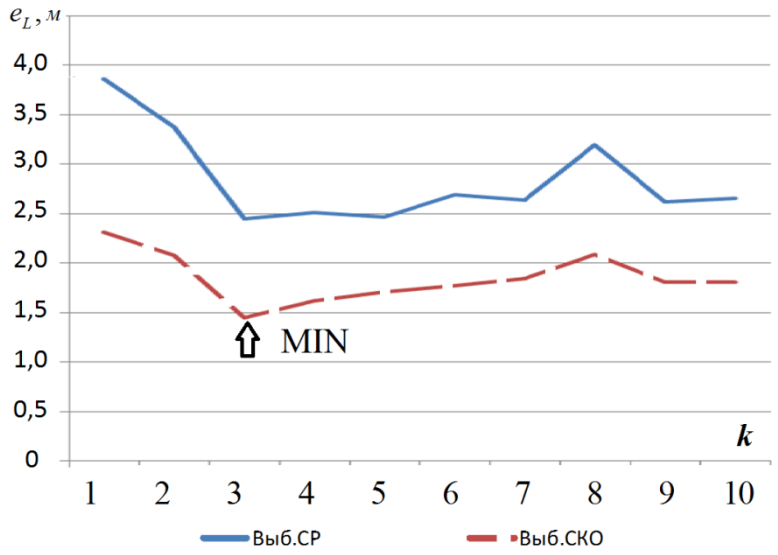
Оптимальное значение ***k***



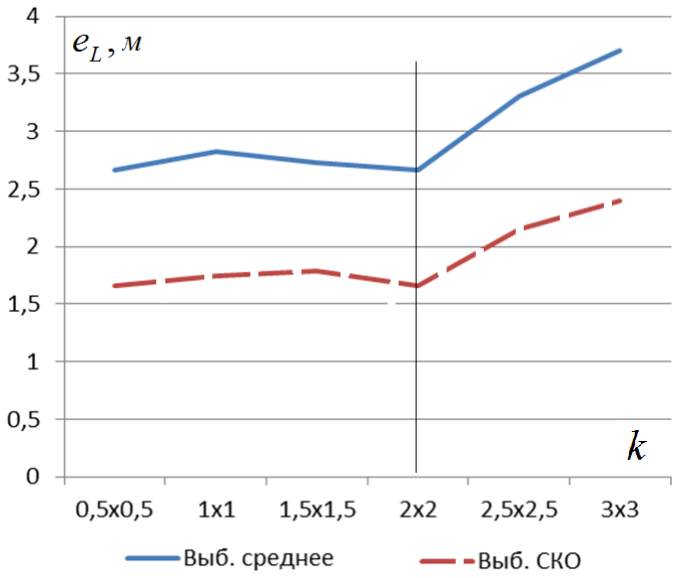
Оптимальное расположение точек измерения на карте сигнального пространства

Рекомендации по формированию оптимальных параметров системы определения местоположения

Оптимальные параметры метода на основе *модифицированного* ***байесовского классификатора*** для заданной карты расположения помещений



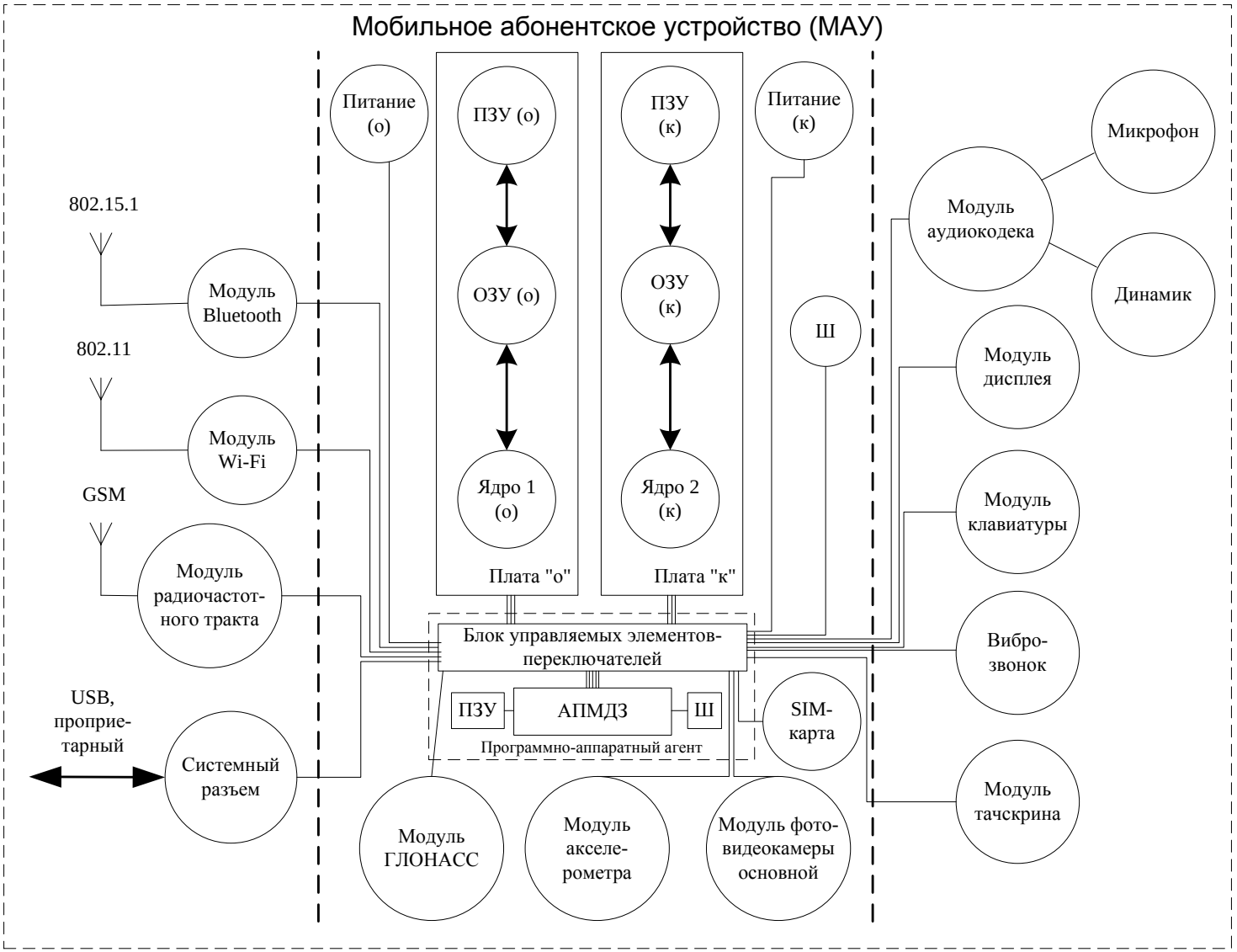
Оптимальное значение ***k*** (учитываемого числа наиболее вероятных состояний)



Оптимальное расположение точек измерения на карте сигнального пространства

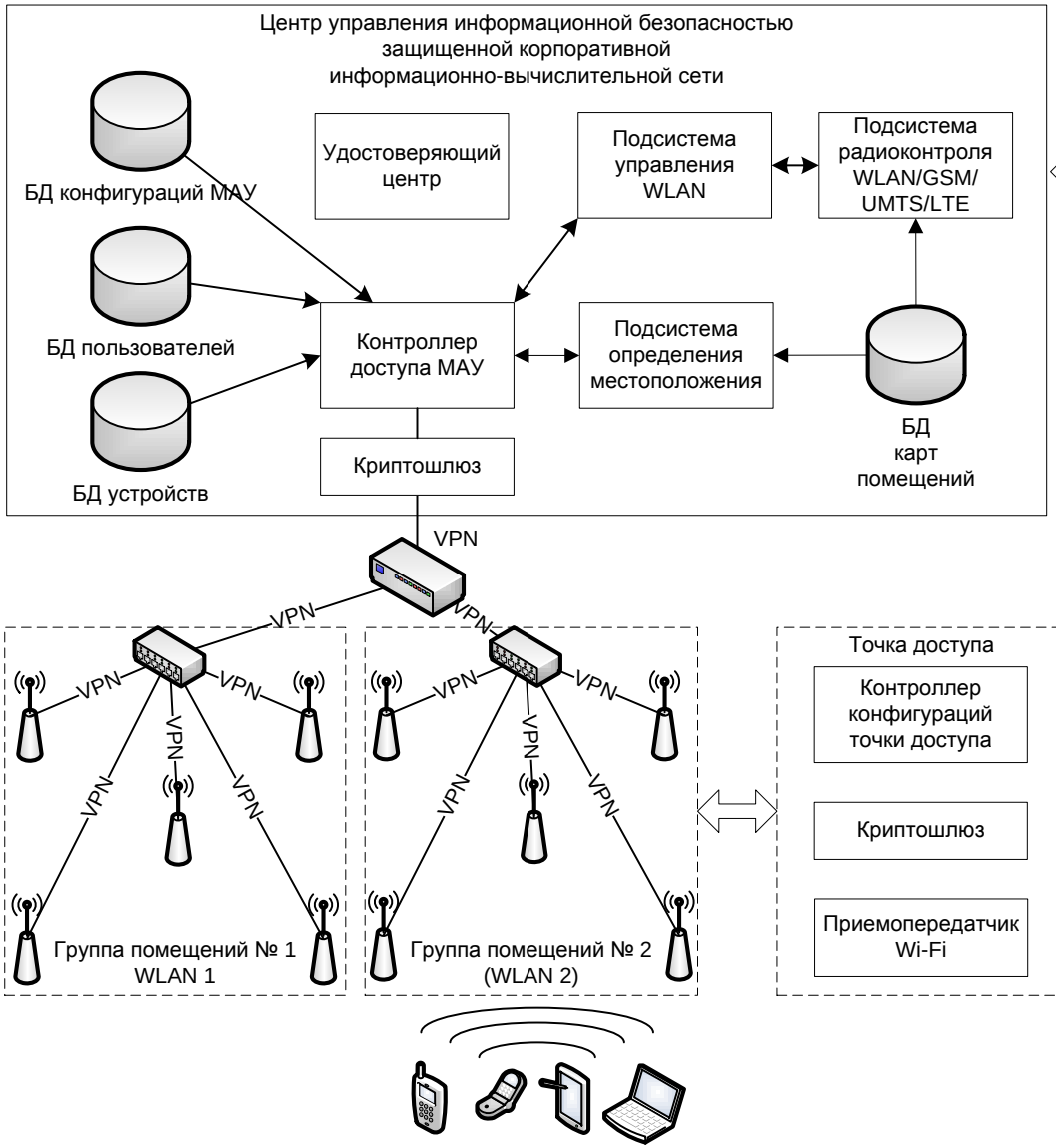
Структурная схема мобильного абонентского устройства

Статья. Информационные технологии. 2015. № 9 (21). С. 611-618



ПрЭВМ 2013618388
ПрЭВМ 2016611210

Структурная схема системы управления безопасностью мобильных абонентских устройств в корпоративных сетях с разными требованиями по защищенности



ПрЭВМ 2013612870
ПрЭВМ 2013615947
ПрЭВМ 2014617119
ПрЭВМ 2014617940
ПрЭВМ 2015615631
Пат. 2503059
Пат. 2530691
Пат. 2546236

Прототип структуры базы данных, хранящей данные, необходимые для алгоритма управления безопасностью МАУ (политику безопасности МАУ организации)

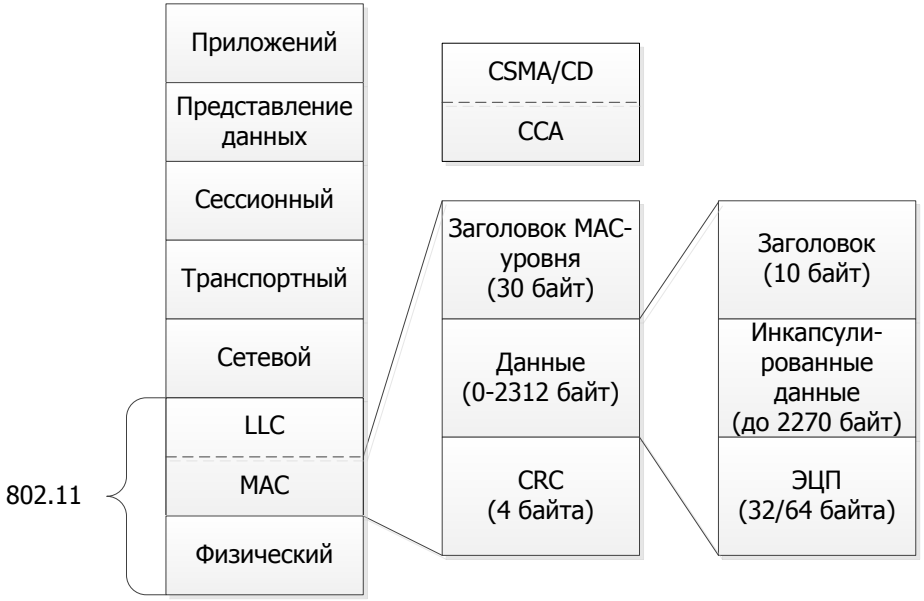


Рис. 1 Защищенный канал управления МАУ в составе инкапсулированных данных MAC-подуровня канального уровня 802.11

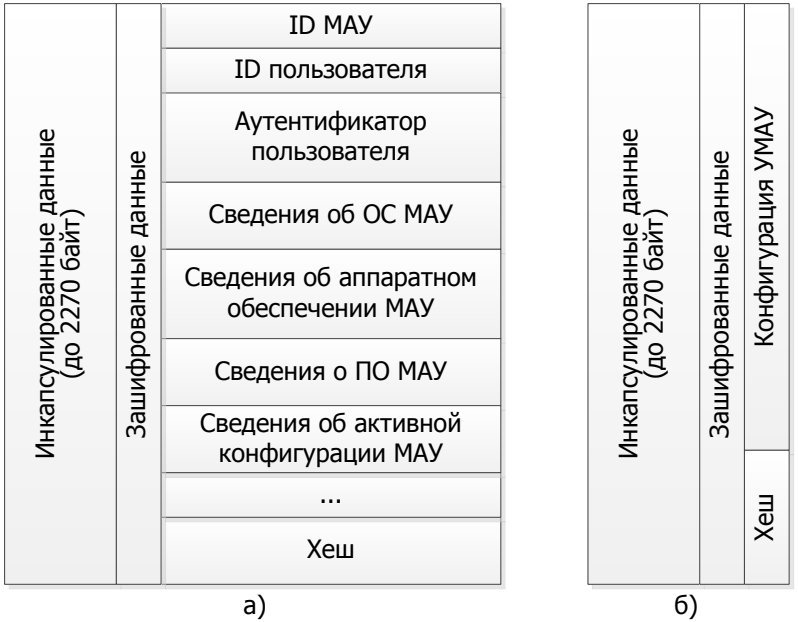


Рис. 2 Варианты реализации структуры данных:

а) при передаче атрибутов доступа контроллеру МАУ

б) при передаче МАУ управляющего воздействия в виде конфигурации

Эффективность предложенной системы управления безопасностью МАУ

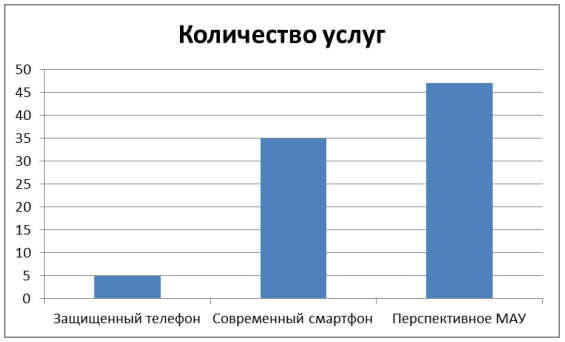


Рис. 1 Сравнительный анализ количества услуг, предоставляемых различными МАУ

$$REZ = P_{\text{БИ}}(T) = P_{\text{КИ}}(T) \cdot P_{\text{ДИ}}(T) \cdot P_{\text{ЦИ}} \Big| P_{\text{ЦИ}} = 1 \quad (1)$$

$$P_{\text{КИ}}(T) = \left(1 - P_{\text{НСД}}\right) \cdot P_{\text{СК}}(T) \quad (2)$$

$$P_{\text{НСД}} = 1 - P\left(CONF \subset CONF^{\text{доп}}\right) = 1 - P\left[\beta\left(\tilde{L}_{Room} > L_{Room}\right) \le \beta^{\text{доп}}\right] \quad (3)$$

$$P_{\text{СК}}\left(T_{RECONF}\right) = P\left[\left(T_{RECONF} \le T_{RECONF}^{\text{доп}}\right) / \left(CONF \subset CONF^{\text{доп}}\right)\right] \quad (4)$$

$$P_{\text{ДИ}}(T_{\text{ДИ}}) = \frac{N_{\text{ДУ}}}{N_{\text{У}}} \cdot P_{\text{св}}\left(T_{\text{ДИ}} \le T_{\text{ДИ}}^{\text{зад}}\right) \Big| T_{\text{ДИ}}^{\text{зад}} = T_{RECONF}^{\text{доп}} \quad (5)$$

$$RES = K_{\text{ИВР}} \cdot C_{\text{ВР}} + K_{\text{ИТР}} \cdot C_{\text{ТР}} + K_{\text{ИСУ}} \cdot C_{\text{СУМАУ}} + K_{\text{ИСОМ}} \cdot C_{\text{СОМ}} + \left(\sum_{i=1}^{N_{\text{МАУ}}} C_{\text{МАУ}_i}\right) \cdot N_{\text{Польз}} \quad (6)$$

$$Э = \frac{\left|\lg\left(\frac{REZ}{RES}\right)\right|}{\max\left[\left|\lg\left(\frac{REZ}{RES}\right)\right|\right]} \quad (7)$$

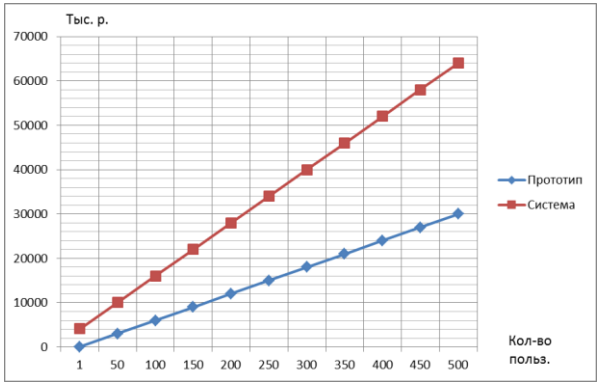


Рис. 2 График зависимости ресурсоемкости технических решений от количества пользователей

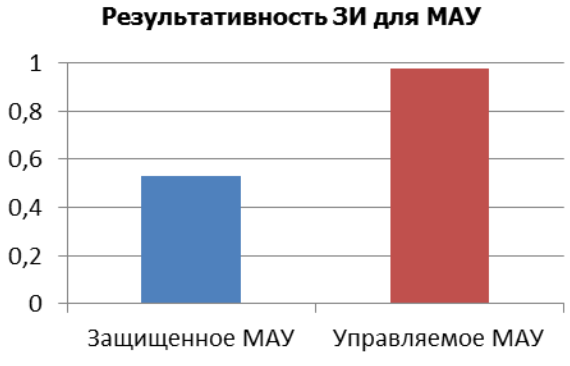


Рис. 3 Оценка степени достижения результатов диссертационного исследования

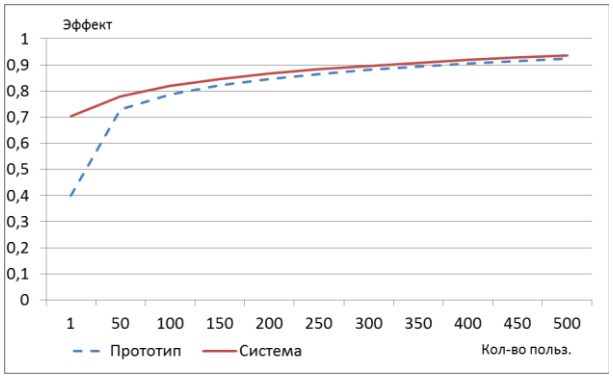


Рис. 4 Сравнительный анализ получаемого эффекта для прототипа и разработанной системы

СВЕДЕНИЯ О ПУБЛИКАЦИЯХ, АПРОБАЦИЯХ И РЕАЛИЗАЦИЯХ

Публикации – 7:

Научные статьи в изданиях, рекомендованных ВАК при Минобрнауки России:

- Вопросы кибербезопасности – 1
- Телекоммуникации – 1
- Информационные технологии – 1
- Вестник РГРТУ – 1
- Известия ТулГУ – 1
- Промышленные АСУ и контроллеры – 2

Апробации – 11:

7, 8, 9-я Научно-практические конференции, г. Орел, Академия ФСО России, 2011, 2013, 2015 гг.
10-я Межведомственная научная конференция, Москва, ИКСИ Академии ФСБ России, 29-31 января 2014 г.
6, 7-я Межрегиональной научно-практической конференции, г. Брянск, БГТУ, 2014, 2015 гг.
12-е Всероссийское совещание по проблемам управления ВСПУ-2014, Москва, ИПУ им. В. А. Трапезникова РАН, 16-19 июня 2014 г.
6, 7-я Межрегиональные научно-практические конференции, г. Брянск, БГТУ, 2014, 2015 гг.
VII Всероссийской научно-практической конференции, г. Калининград, Калининградский пограничный институт ФСБ России, 2014 г.
Всероссийская научно-техническая конференция, г. Королев, Моск. обл, 4 ЦНИИ МО РФ, 2015 г.
Международной научно-технической конференции "ПИТ-2015", г.Самара, Самарский научный центр РАН, 2015 г.

Реализации – 10:

Программы для ЭВМ – 6 (№№ 2013615947,2013618388,2014617119,2014617940,2015615631,20166111210)
Патенты на изобретения – 3: №№ 2503059, 2530691, 2546236

Акты внедрения – 2:

Спецсвязь ФСО России, ФГУП "ГосНИИПП" ФСТЭК России