МЕТОДИКА ОЦЕНКИ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ЭКСПЛУАТАЦИИ МОБИЛЬНЫХ АБОНЕНТСКИХ УСТРОЙСТВ В КОРПОРАТИВНЫХ СЕТЯХ С РАЗНЫМИ ТРЕБОВАНИЯМИ ПО ЗАЩИЩЕННОСТИ

Маркин Д.О.[1], Комашинский В.В.[2], Сенотрусов И.А.[3]

В работе предложена методика расчета оценки эффективности защиты информации при эксплуатации мобильных абонентских устройств в корпоративных сетях с разными требованиями по защищенности. Осуществлена формальная постановка задачи на разработку методики оценки эффективности защиты информации. Описаны ограничения и допущения, в рамках которых предлагаемая методика может быть применима. Представлены примеры расчета оценок таких параметров как вероятности нарушения конфиденциальности информации, вероятности сохранения конфиденциальности информации, коэффициента доступности услуг, вероятности обеспечения доступности услуг и ресурсоемкости процесса защиты информации. В расчетах использованы исходные данные из нормативно–правовой базы, известных опубликованных работ автора и других источников. Представлены результаты оценки результативности защиты информации и получаемого эффекта от внедрения оцениваемой системы защиты информации. Предложенная методика может быть использована для оценивания результативности функционирования перспективных СЗИ, разрабатываемых для обеспечения безопасности информации в защищенных корпоративных сетях, в которых предусмотрена эксплуатация мобильных абонентских устройств для доступа к защищаемой информации и услугам с разными требованиями по защищенности. Ключевые слова: оценка эффективности защиты информации, мобильное устройство, конфиденциальность информации, средство защиты информации

DOI: 10.21581/2311-3456-2017-4-21-31

Введение

При эксплуатации мобильных абонентских устройств (МАУ) существует ряд важных особенностей, оказывающих существенное влияние на состояние защищенности информационного взаимодействия в рамках работы в ИВС [1]. К таким особенностям относятся: миниатюрность МАУ; мобильность; ограниченность вычислительных ресурсов МАУ; мультифункциональность МАУ; доступ к услугам защищенной корпоративной сети (ЗКС) на основе использования принципа однократного входа SSO («Single Sign-On»); доступ к информационным ресурсам сетей с разными требованиями по защищенности.

Указанные особенности увеличивают вероятность осуществления угроз информационной безопасности (ИБ) при работе с МАУ, поэтому необходимо учитывать факторы, влияющие на безопасность информации [1]. Для учета данных факторов, влияющих на ИБ, а также осуществления аудита безопасности эксплуатации МАУ в корпоративных сетях с разными требованиями по защищенности необходима методика расчета оценки эффективности защиты информации при эксплуатации МАУ, позволяющую учитывать совокупность факторов, оказывающий влияние на безопасности информации. Одним из принципиально важных факторов при расчете оценки защищенности ЗКС с МАУ является его местоположение и другие атрибуты доступа.

1. Постановка задачи

Для разработки методики оценки эффективности защиты информации при эксплуатации МАУ в корпоративных сетях с разными требованиями по защищенности предлагается использовать следующие **исходные данные**:

1) универсальное мобильное абонентское устройство (МАУ) MD, его технические характеристики;

2) множество возможных конфигураций МАУ – $CONF$;

3) расположение, требования по защищенности и параметры помещений:

1 Маркин Дмитрий Олегович, независимый эксперт, г. Орёл, admin@nikitka.net.

2 Комашинский Владимир Владимирович, кандидат технических наук, доцент, независимый эксперт, г. Орёл, vladkom-orel@mail.ru.

3 Сенотрусов Игорь Альбертович, кандидат технических наук, доцент, независимый эксперт, г. Орёл, wsilvez@mail.ru.

$$Rooms = \left\{ room_i = \left((x_{i1}, y_{i1}), (x_{i2}, y_{i2}), ..., (x_{in}, y_{in}), L_{Room_i} \right) \right\},$$
$$i = \overline{1, N_{Rooms}}, \quad (1)$$

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;

4) расположение точек доступа беспроводной сети $AP = \left\{ AP_j = \left(x_j, y_j \right) \right\}$, $j = \overline{1, N_{AP}}$, где (x_j, y_j) – координаты точек доступа, N_{AP} – количество точек доступа;

5) множество пороговых значений частных показателей эффективности $H = \left\{ P_\beta \left(\tilde{L}_{Room} > L_{Room} \right) \le P_\beta^{\text{треб}}, T_{RECONF} \le T_{\text{RECONF}}^{\text{доп}}, \right.$
$\left., T_{\text{ДИ}} \le T_{\text{RECONF}}^{\text{доп}} \right\}$; ;

6) совокупность атрибутов доступа $A = \{a_i\}$ пользователя МАУ, включающая:

– идентификационные данные о пользователе, МАУ, операционной системе (ОС) и приложениях МАУ;

– сетевая адресная информация;

– уровень конфиденциальности и идентификатор запрашиваемой услуги (ресурса).

Требуется разработать методику оценки эффективности защиты 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.

2. Разработка системы показателей качества для методики оценки защищенности защиты информации при эксплуатации МАУ

Для расчета оценки эффективности предложенной системы управления безопасностью МАУ, а также оценки степени защищенности ЗКС целесообразно пользоваться критерием превосходства [2], исходя из специфики предъявляемых к системе требований.

Система показателей качества построена из следующих соображений. Поскольку цель разрабатываемой системы – обеспечение безопасности информации при эксплуатации МАУ в корпоративных сетях с разными требованиями по защищенности, то степень достижения данной цели согласно теории эффективности целенаправленных процессов [2] может быть представлена в виде выражения

$$Э_{\text{ЗИМАУ}} = P\left[\left(REZ \ge REZ^{\text{тр}} \right) \wedge \left(RES \le RES^{\text{доп}} \right) \wedge \right.$$
$$\left. \wedge \left(OPR \le OPR^{\text{доп}} \right) \right], \quad (2)$$

где REZ – результативность процесса защиты информации; $REZ^{\text{треб}}$ – требуемое значение результативности процесса защиты информации; RES – ресурсоемкость процесса защиты информации; $RES^{\text{доп}}$ – максимально допустимый расход ресурсов для процесса защиты информации; OPR – затраты операционного времени для достижения цели функционирования системы; $OPR^{\text{доп}}$ – максимально допустимое время для достижения цели функционирования системы.

В соответствие с ГОСТ Р 50922–2006, ГОСТ Р 53114–2008, а также [3, 4] безопасность информации является комплексным свойством и обеспечивается за счет выполнения требований по обеспечению конфиденциальности, целостности и доступности информации. Исходя из этого, результативность процесса защиты информации при эксплуатации МАУ может быть представлена в виде выражения

$$P_{\text{БИ}}(T) = P_{\text{КИ}}(T) \cdot P_{\text{ЦИ}}(T) \cdot P_{\text{ДИ}}(T), \quad (3)$$

где $P_{\text{КИ}}(T)$ – вероятность обеспечения конфиденциальности информации в течение времени T; $P_{\text{ЦИ}}(T)$ – вероятность обеспечения целостности информации; $P_{\text{ДИ}}(T)$ – вероятность обеспечения доступности информации.

Вопросы обеспечения целостности информации в работе не рассматриваются, поэтому показатель при расчетах принят равным единице: $P_{\text{ЦИ}}(T) = 1$.

Вероятность обеспечения доступности информации предлагается оценивать по своевременности обработки запросов на доступ к услугам в соответствии с ГОСТ РВ 51987–2002 с учетом количества доступным услуг $N_{\text{ДУ}}$ относительно их

общего числа $N_{\text{у}}$. Тогда вероятность предоставления информации или услуг $P_{\text{ДИ}}(T_{\text{ДИ}})$ за заданное время $T_{\text{ДИ}}^{\text{зад}}$ будет определяться с помощью табулированной неполной гамма-функции:

$$P_{\text{ДИ}}(T_{\text{ДИ}}) = \frac{N_{\text{ДУ}}}{N_{\text{у}}} \cdot P_{\text{ДИ}}^{y}(T_{\text{ДИ}}) = \frac{N_{\text{ДУ}}}{N_{\text{у}}} \cdot \int_0^{\theta} exp(-\tau) \cdot \tau^{\gamma}\, d\tau / \Gamma(\gamma), \quad (4)$$

где

$\Gamma(\gamma) = \int_0^{\theta} exp(-\tau) \cdot \tau^{\gamma}\, d\tau / \Gamma(\gamma)$ - гамма функция,

$$\gamma = \frac{T_{\text{полн}}}{\sqrt{T_2 - T_{\text{полн}}^2}}, \theta = T_{\text{ДИ}}^{\text{зад}} \cdot \frac{\gamma^2}{T_{\text{полн}}}, \quad (5)$$

где $T_{\text{полн}}$ и T_2 – рассчитываемые соответственно среднее время и 2-й момент времени реакции системы при обработке запросов системе (полного времени пребывания на обработке с учетом ожидания в очереди), $T_{\text{ДИ}}^{\text{зад}}$ – заданное время (предельно допустимое) для обработки запроса на доступ к информации (услугам).

Целью диссертационного исследования является повышение вероятности обеспечения безопасности информации при эксплуатации МАУ для доступа к инфокоммуникационным услугам и ресурсам корпоративных сетей с разными требованиями по защищенности, соответственно, необходимо доказать, что показатель вероятности обеспечения конфиденциальности информации будет не хуже, чем в действующих прототипах. Для обеспечения конфиденциальности информации необходимо обеспечить защиту от несанкционированного доступа (НСД), а также обеспечить сохранение конфиденциальности на заданном периоде времени [3], а также в соответствии с ГОСТ РВ 51987–2002. Исходя из этих соображений, показатель вероятности обеспечения конфиденциальности может быть представлен в виде выражения

$$P_{\text{КИ}}(T) = \left(1 - P_{\text{НСД}}\right) \cdot P_{\text{СК}}\left(T\right), \quad (6)$$

где $P_{\text{НСД}}$ – вероятность НСД к информации; $P_{\text{СК}}\left(T\right)$ – вероятность сохранения конфиденциальности информации на заданном периоде времени.

Вероятность НСД при условии корректно заданной политики безопасности, будет определяться величиной вероятности ошибки 2-го рода при определении местоположения МАУ, которая будет оказывать непосредственное влияние на выбор конфигурации МАУ в системе управления безопасностью МАУ. Тогда показатель вероятности НСД можно представить в виде выражения

$$P_{\text{НСД}} = 1 - P\left(CONF \subset CONF^{\text{доп}}\right) = 1 - P\left[\beta\left(\tilde{L}_{Room} > L_{Room}\right) \le \beta^{\text{доп}}\right], \quad (7)$$

$$P\left(CONF \subset CONF^{\text{доп}}\right) = P\left[P_{\beta}\left(\tilde{L}_{Room} > L_{Room}\right) \le P_{\beta}^{\text{доп}}\right], \quad (8)$$

где $CONF$ – конфигурация МАУ, сформированная системой управления безопасностью МАУ; $CONF^{\text{доп}}$ – множество допустимых конфигураций МАУ при текущих условиях доступа.

Показатель вероятности сохранения конфиденциальности информации на заданном периоде времени определяется своевременностью переконфигурации МАУ при изменении атрибутов доступа и при условии назначения конфигурации из допустимого множества $P\left[\left(T_{RECONF} \le T_{RECONF}^{\text{доп}}\right) / \left(CONF \subset CONF^{\text{доп}}\right)\right]$, а также вероятностью преодоления СЗИ за данный период времени $P_{\text{Пр3}}$ [3], а также по ГОСТ РВ 51987–2002. Данный показатель может быть представлен в виде выражения:

$$P_{\text{СК}}\left(T_{RECONF}\right) = P\left[\left(T_{RECONF} \le T_{RECONF}^{\text{доп}}\right) / \left(CONF \subset CONF^{\text{доп}}\right)\right] \cdot \left(1 - P_{\text{Пр3}}\right). \quad (9)$$

В соответствие с ГОСТ РВ 51987–2002 показатель $P_{\text{Пр3}}$ может быть рассчитан как

$$P_{\text{Пр3}} = 1 - \prod_{m=1}^{k} P_{\text{НСД}_m}, \quad (10)$$

где k – количество преград, которое необходимо преодолеть нарушителю, чтобы получить доступ к информационным и программным ресурсам, $P_{\text{НСД}_m}$ – вероятность преодоления нарушителем m-той преграды (средства защиты).

Для экспоненциальной аппроксимации распределений исходных характеристик при их независимости:

$$P_{НСД_m} = \frac{f_m}{f_m + u_m}, \quad (11)$$

где f_m – среднее время между соседними изменениями параметров m-й преграды системы защиты (время между сменой конфигураций); u_m – среднее время расшифровки (вскрытия) значений параметров m-й преграды системы защиты. Показатель $P_{\text{Пр3}}$ в рамках работы вынесен в ограничения и принят равным нулю.

Ресурсоемкость процесса защиты информации [3] при эксплуатации МАУ может быть определена, исходя из выражения:

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

где $K_{ИВР}$ – коэффициент использования вычислительных ресурсов; $C_{ВР}$ – стоимость вычислительных ресурсов; $K_{ИТР}$ – коэффициент использования телекоммуникационных ресурсов; $C_{ТР}$ – стоимость телекоммуникационных ресурсов; $K_{ИСУ}$ – коэффициент использования системы управления безопасностью МАУ; $C_{СУМАУ}$ – стоимость системы управления безопасностью МАУ; $K_{ИСОМ}$ – коэффициент использования системы определения местоположения МАУ; $C_{СОМ}$ – стоимость системы определения местоположения МАУ; $C_{МАУ_i}$ – стоимость i-го МАУ, необходимого для доступа к услугам; $□_{МАУ}$ – количеством МАУ, необходимых для доступа ко всему перечню услуг; $□_{Польз}$ – количество пользователей МАУ.

3. Пример расчета по методике оценки эффективности защиты информации при эксплуатации МАУ в корпоративных сетях с разными требованиями по защищенности

Целью разработки перспективных систем защиты информации (СЗИ), эксплуатируемых в корпоративных сетях с разными требованиями по защищенности для доступа к услугам с единого МАУ, как правило, является повышение вероятности обеспечения безопасности информации. Результативность процесса оценивается с помощью вероятности обеспечения безопасности информации при доступе к услугам с использованием МАУ согласно выражению (3). Используя выражения (3), (4), (6)-(10) и следующие ограничения и допущения ($□_{ЦИ} \to 1$, $□_{П□□□} \to 0$), получим итоговое выражение для оценивания результативности процесса защиты информации при эксплуатации МАУ:

$$P_{БИ}(T) = \left(1 - P\left[\beta\left(\tilde{L}_{Room} > L_{Room}\right) \le \beta^{доп}\right]\right) \cdot$$

$$\cdot P_{СК}\left(T_{RECONF}\right) \cdot \frac{N_{ДУ}}{N_{У}} \cdot P^{У}_{ДИ}(T_{ДИ}). \qquad (13)$$

Анализ нормативно-правовой базы и требований по обеспечению ИБ [5], ГОСТ РВ 51987–2002 показал, что:

– существуют особые требования системы ИБ в отношении эксплуатации МАУ в защищенных корпоративных сетях;

– использование личных МАУ в ЗКС запрещено либо существенно ограничено в рамках принципа BYOD с учетом выполнения требований системы ИБ;

– абонентские устройства (сотовые телефоны, смартфоны, планшетные компьютеры и т.п.) стандарта IEEE 802.11 должны отвечать требованиями корпортивной политике ИБ в ЗКС;

– оборудование сети Wi-Fi также должно отвечать требованиями корпортивной политике ИБ в ЗКС.

Расчет вероятности нарушения конфиденциальности информации

Результаты оценивания параметра $P\left[\beta\left(\tilde{L}_{Room} > L_{Room}\right) \le \beta^{доп}\right]$ приведены в работах [1, 8]. Данный параметр характеризуют вероятность возникновения ошибки 2-го рода, являющейся критичной для нарушения конфиденциальности информации в защищенной корпоративной сети, при определении местоположения МАУ. Результаты исследования эффективности определения уровня защищенности помещения численным методом Монте-Карло при использовании различных технологий определения местоположения представлены в таблице 1. В таблице: П – прототип, С – перспективная система.

Как видно из анализа таблицы, вне зависимости от технологии определения местоположения оценка эффективности определения уровня защищенности в виде ошибки 2-го рода не превышает 1 % при заданном критерии принятия решения. Однако, при данном критерии высокие значения

Таблица 1

Результаты исследования эффективности определения уровня защищенности численным методом Монте-Карло при использовании различных технологий определения местоположения и их комбинаций

№ п/п	Метод	Правильно		Ошибка 1-го рода		Ошибка 2-го рода	
		П	С	П	С	П	С
1.	Трилатерация	72,104	16,779	5,325	81,614	22,569	**0,906**
2.	k-ближайших соседей	76,881	14,333	9,247	84,447	13,871	**0,919**
3.	Байесовский подход	75,572	11,153	17,726	87,786	6,700	**0,906**
4.	методы 1 и 2	71,934	6,255	8,982	93,225	19,083	**0,519**
5.	методы 1 и 3	72,069	8,349	9,615	90,997	18,314	**0,653**
6.	методы 2 и 3	75,728	15,055	10,44	82,88	13,831	**2,064**
7.	методы 1, 2 и 3	76,327	8,727	7,938	90,235	15,786	**1,037**

имеет ошибка 1-го рода. Графическая иллюстрация результатов имитационного моделирования представлена на рисунке 1.

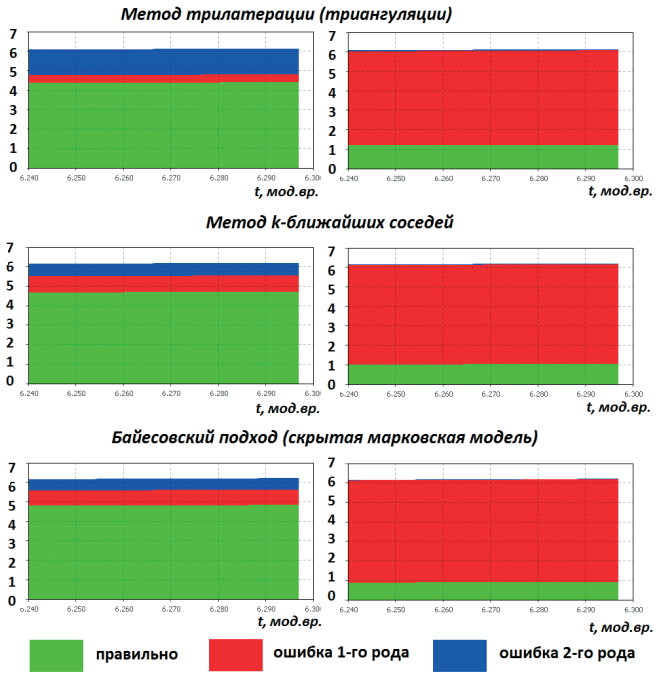

Рис.1. Результаты имитационного моделирования исследования эффективности определения уровня защищенности помещения численным методом Монте-Карло

На основе анализа таблицы и рисунка можно сделать вывод, что при условии задания критерия $\beta^{\text{доп}} = 0,01$ вероятность нарушения конфиденциальности информации находится в пределах допустимых значений $P\left[\beta\left(\tilde{L}_{Room} > L_{Room}\right) \le \beta^{\text{доп}}\right] \to 1$.

Расчет вероятности сохранения конфиденциальности информации

Для оценивания параметра $P_{\text{СК}}\left(T_{RECONF}\right)$ необходимо рассчитать оценочное значение времени, необходимого для смены конфигурации МАУ. В процессе движения пользователя с МАУ неизбежно возникают ситуации, когда меняются атрибуты доступа и в том числе уровень защищенности помещений, в которых находится мобильный пользователь. Атрибуты доступа и политика безопасности определяют требования к конфигурации МАУ при текущих условиях доступа. Для мобильных пользователей время смены конфигурации МАУ в некоторых ситуациях является важным показателем качества.

Процесс смены конфигурации МАУ осуществляется в несколько этапов:

1. Измерение уровня сигнала МАУ на точках доступа беспроводной сети передачи данных (T_{RSS}).
2. Определение местоположения МАУ (T_{LOC}).
3. Отправка атрибутов доступа (запроса на доступ к услугам) с МАУ (T_{REQ}).
4. Обработка запроса с учетом параметров политики безопасности (T_{POLICY}).
5. Формирование и отправка управляющей команды на смену конфигурации МАУ (T_{RESP}).
6. Прием и обработка управляющей команды на стороне МАУ, применение новой конфигурации (T_{CONF}).

Таким образом, оценка общего времени, необходимого для смены конфигурации МАУ, может быть представлена в виде

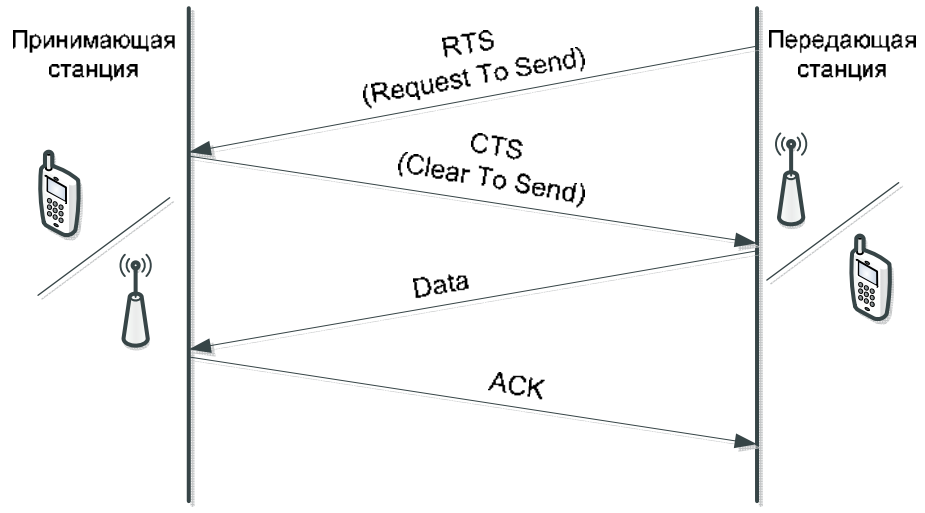

***Рис. 2**. Четырехэтапн ый протокол передачи данных, реализующий метод коллективного доступа к среде с минимизацией вероятности возникновения столкновений*

$$T_{RECONF} = T_{RSS} + T_{LOC} + T_{REQ} + T_{POLICY} + T_{RESP} + T_{CONF} . \quad (14)$$

Расчет времени, необходимого на каждом этапе, осуществим для наиболее распространенного стандарта беспроводной передачи данных – IEEE 802.11 при следующих ограничениях и допущениях:

– доступ к беспроводной сети передачи данных установлен, мобильное устройство прошло аутентификацию и находится в зоне действия доверенной беспроводной сети передачи данных;

– расчет временных параметров производится на наихудший случай.

В соответствие со стандартом IEEE 802.11 передача пакета данных на канальном уровне, обладающем идентификационной информацией о передатчике осуществляется в 4 этапа. Данные этапы представлены на рисунке 2.

В стандарте IEEE 802.11 используется метод коллективного доступа с обнаружением несущей и избеганием коллизий (Carrier Sense Multiple Access / Collision Avoidance, CSMA/CA). Перед началом передачи данных осуществляется выбор свободного канала на основе алгоритма оценки чистоты канала (Channel Clearance Algorithm, CCA). В основе данного алгоритма лежит измерение энергии сигнала на антенне и мощности принятого сигнала (Received Signal Strength Indicator, RSSI). Если мощность принятого сигнала ниже заданного порога, то канал объявляется свободным и MAC-уровень получает статус CTS (Clear To Send).

Перед началом передачи данных, МАУ отправляет сообщение RTS (Ready To Send), содержащее информацию о готовности отправки данных, адресате и продолжительности передачи. Если приемная станция (точка доступа) отвечает посылкой сигнала CTS, то МАУ начинает передачу данных. По завершение передачи данных точка доступа возвращает кадр ACK, подтверждающий безошибочный прием.

Максимальная дальность действия беспроводной сети определяется множеством параметров и в первую очередь мощностью передатчика, чувствительностью приемника и наличием препятствий. Расчет времени передачи сигнала от передатчика к источнику в условиях здания произведем для дальности в $l = 100$ м. Тогда четырехэтапная передача данных будет осуществляться за время, равное

$$t_{data} \approx \frac{4 \cdot l}{c} = \frac{4 \cdot 100}{299\,792\,458} = 1{,}334256 \cdot 10^{-6} \text{ с}. \quad (15)$$

Соответственно, передача пакета данных с идентифицирующей МАУ информацией будет осуществляться за время $T_{RSS} = t_{data}$.

Исходя из тех же соображений, осуществляется расчет значений T_{REQ} и T_{RESP} . При этом необходимо учесть, что максимальный размер блока данных, предусмотренный спецификацией пакетирования данных, предусматривает блок данных до 2048 байт, рекомендуя при этом использовать пакеты длиной 1500 и 2048 байт. Поскольку в запросе на доступ содержатся сведения об атрибутах доступа и запрашиваемой услуге, а в ответе на запрос – информация о назначаемой конфигурации, то размер передаваемых данных может превышать максимальный размер пакета, поэтому для значений T_{REQ} и T_{RESP} предусмотрим 10-кратное превышение максимального размера пакета. Тогда с учетом (15) получим:

$$T_{LOC} \approx 2{,}92 \cdot 10^{-3} \text{ с}, \; T_{POLICY} \approx 0{,}71 \cdot 10^{-3} \text{ с}.$$

Значение T_{LOC} определяется временем, необходимым для получения данных об уровне сигнала МАУ точками доступа, в зоне действия которых, находится данное устройство, а также временем работы алгоритма определения местоположения МАУ и уровня защищенности помещения, в котором оно находится.

Значения T_{LOC}, T_{POLICY}, T_{CONF} определяются быстродействием программно-аппаратной составляющей системы управления МАУ.

В процессе имитационного моделирования и функционирования разработанных прог рамм для ЭВМ [9, 10, 11] были получены следующие результаты: $T_{LOC} \approx 2{,}92 \cdot 10^{-3}$ с, $T_{POLICY} \approx 0{,}71 \cdot 10^{-3}$ с, $T_{CONF} \approx 1{,}12 \cdot 10^{-3}$ с.

Исходя из полученных оценок времени выполнения процедур и выражения (14) получим оценку значения времени, необходимого для смены конфигурации мобильного устройства:

$$T_{RECONF} = T_{RSS} + T_{LOC} + T_{REQ} + T_{POLICY} + T_{RESP} + T_{CONF} \approx$$
$$\approx 0{,}001334256 \cdot 10^{-3} + 2{,}92 \cdot 10^{-3} + 0{,}01334256 \cdot 10^{-3} + 0{,}71 \cdot 10^{-3} +$$
$$+ 0{,}01334256 \cdot 10^{-3} + 1{,}12 \cdot 10^{-3} = 4{,}778019376 \cdot 10^{-3} \text{ с} \approx 4{,}778 \text{ мс}$$

Полученная оценка времени, необходимого для смены конфигурации МАУ в позволяет сделать вывод, что при данных ограничениях и допущениях время переконфигурации МАУ не превышает заданный порог и не снижает уровень защищенности при движении мобильного пользователя.

На основании полученных значений может быть получена оценка вероятности сохранения

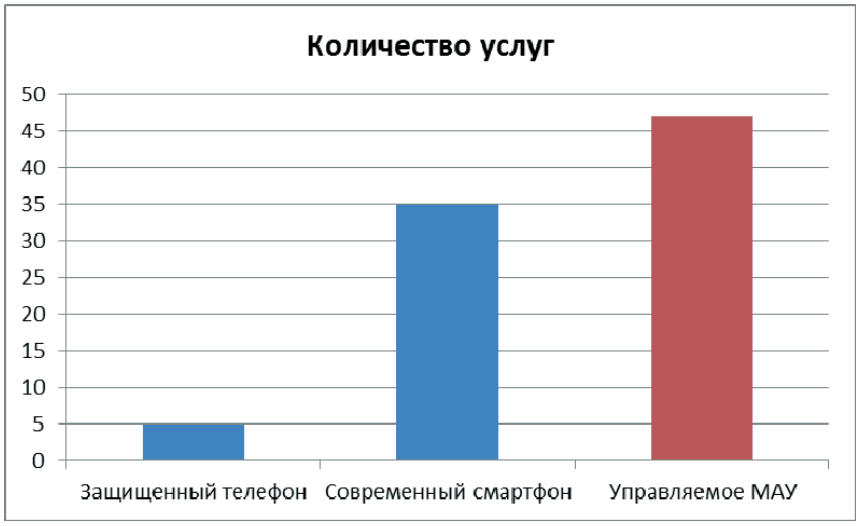

***Рис. 3**. – Сравнительный анализ количества услуг, предоставляемых МАУ*

конфиденциальности информации при доступе к услугам сетей с разными требованиями по защищенности согласно принятой системе показателей эффективности. Вероятность сохранения конфиденциальности информации предложено оценивать с помощью выражения (9), при этом принято, что вероятность преодоления системы защиты $P_{\text{Пр3}} \to 0$. Таким образом, при условии $CONF \subset CONF^{\square\square\square}$, принятых ограничениях и допущениях ($P_{\text{Пр3}} \to 0$), а также полученной оценки времени переконфигурации $T_{RECONF} = 4{,}778 \cdot 10^{-3}$ с, находящейся в пределах заданных заказчиком значений $T_{RECONF}^{\text{доп}} = 10^{-2}$ с, можно сделать вывод о том, что $P_{\text{СК}}\left(T_{RECONF}\right) \to$.

Расчет коэффициента доступности услуг

Для оценивания коэффициента $\frac{N_{\text{ДУ}}}{N_{\text{У}}}$ был проведен анализ доступности услуг для обычных (личных), защищенных и перспективных (с управляемой программно-аппаратной конфигурацией) МАУ. Очевидно, что доступность защищенных инфокоммуникационных услуг связи при использовании личных МАУ в ЗКС существенно ограничена. Открытые услуги, предоставляемые с использованием личных МАУ могут быть и вовсе недоступны. Вместе с тем современные МАУ позволяют получать доступ к широкому перечню услуг. Сравнительный анализ количества представляемых различными МАУ [1, 6, 7] услуг представлен на рисунке 3.

Таким образом, из анализа представленного рисунка и введенных ограничений и допущений коэффициент $\frac{N_{\text{ДУ}}}{N_{\text{У}}} \approx \frac{5}{47}$ для защищенных МАУ и $\frac{N_{\text{ДУ}}}{N_{\text{У}}} \to 1$.

Расчет вероятности обеспечения доступности услуг

Своевременность обработки запросов на доступ к услугам оценивалась в соответствии со стандартом ГОСТ РВ 51987–2002. Вероятность предоставления информации или услуг $P_{\text{ДИ}}(T_{\text{ДИ}})$ за заданное время $T_{\text{ДИ}}^{\text{зад}}$ будет определяться с помощью табулированной неполной гамма-функции:

$$P_{\text{ДИ}}^{\text{У}}(T_{\text{ДИ}}) = \int_0^{\theta} exp(-\tau) \cdot \tau^{\gamma}\, d\tau \,/\, \Gamma(\gamma), \qquad (16)$$

где $\Gamma(\gamma) = \int_0^{\infty} exp(-\tau) \cdot \tau^{\gamma}\, d\tau$ – гамма функция; $\gamma = \frac{T_{\text{полн}}}{\sqrt{T_2 - T_{\text{полн}}}}$; $\theta = T_{\text{ДИ}}^{\text{зад}} \cdot \frac{\gamma^2}{T_{\text{полн}}}$; $T_{\text{полн}}$ и $\square_{\square}$ – рассчитываемые соответственно среднее время и 2-й момент времени реакции системы при обработке запросов системе (полного времени пребывания на обработке с учетом ожидания в очереди), $T_{\text{ДИ}}^{\text{зад}}$ – заданное время (предельно допустимое) для обработки запроса на доступ к информации (услугам).

В соответствие с выражением (14) рассчитанное временем, требующееся для переконфигурации МАУ в составляет $T_{RECONF} = \square\square\square\square\square\square\square\square\square\square\square\square\square\square$ Соответствующее ему значение вероятности своевременности обработки запроса, полученное с помощью табулированной неполной гамма-функции равно

$$P_{\text{ДИ}}^{\text{У}}(T_{\text{ДИ}}) = \Gamma(\gamma) = \Gamma\left(\frac{T_{RECONF}}{\sqrt{D\left[T_{RECONF}\right] + T_{RECONF}^2}}\right) =$$

$$= \Gamma(1{,}033804) = 0{,}9983$$

Таким образом, при одинаковых условиях получения доступа к услугам для разрабатываемой системы и ее прототипа в условиях, МАУ в разрабатываемой системе необходимо осуществить реконфигурацию, дополнительно затратив на это время, равное $T_{RECONF} = 4{,}778019376 \cdot 10^{-3}$ с.

Расчет ресурсоемкости процесса защиты информации

Ресурсоемкость процесса защиты информации [3] при эксплуатации МАУ может быть определена, исходя из выражения (12). Анализа открытых источников информации и средней стоимости защищенных мобильных технических решений, а также средняя стоимость проектирования и развертывания защищенной беспроводной сети передачи данных и серверной составляющей, выполняющей функции центра управления информационной безопасностью, позволил выявить примерную зависимость между затратами и количеством пользователей МАУ для прототипа и разработанной системы управления безопасностью МАУ. График данной зависимости представлен на рисунке 4.

Анализа рисунка показывает, что изначально ресурсоемкость предлагаемого технического решения превышает аналогичный показатель для прототипа на величину затрат на систему управления и систему определения местоположения $K_{\text{ИСУ}} \cdot C_{\text{СУМАУ}} + K_{\text{ИСОМ}} \cdot C_{\text{СОМ}}$, при этом стоимость управляемого МАУ также не позволяет получить экономический эффект вне зависимости от количества пользователей МАУ.

Расчет результативности процесса защиты информации и получаемого эффекта от внедрения разработанного СЗИ

На основе полученных результатов оценивания параметров:

вероятности нарушения конфиденциальности информации;

вероятности сохранения конфиденциальности информации;

коэффициента доступности услуг;

вероятности обеспечения доступности услуг;

ресурсоемкости процесса защиты информации;

может быть рассчитана оценка результативности процесса защиты информации и получаемый эффект от внедрения разработанного СЗИ.

В качестве прототипа оценивалась система доступа к услугам, основанная на типовых защищенных МАУ с количеством предоставляемых услуг, равным 5, и системой из организационно-технических мер по защите информации, обеспечивающих требования по информационной безопасности. На основании представленных данных получена оценка результативности защиты информации (ЗИ), представленная на рисунке 5.

Получаемый эффект (нормированный на логарифмической шкале) при внедрении разработанной системы управления МАУ с учетом выражений (2), (12), (13) может быть оценен как

$$\text{Э} = \frac{\left|\lg\left(\frac{REZ}{RES}\right)\right|}{\max\left[\left|\lg\left(\frac{REZ}{RES}\right)\right|\right]}. \qquad (17)$$

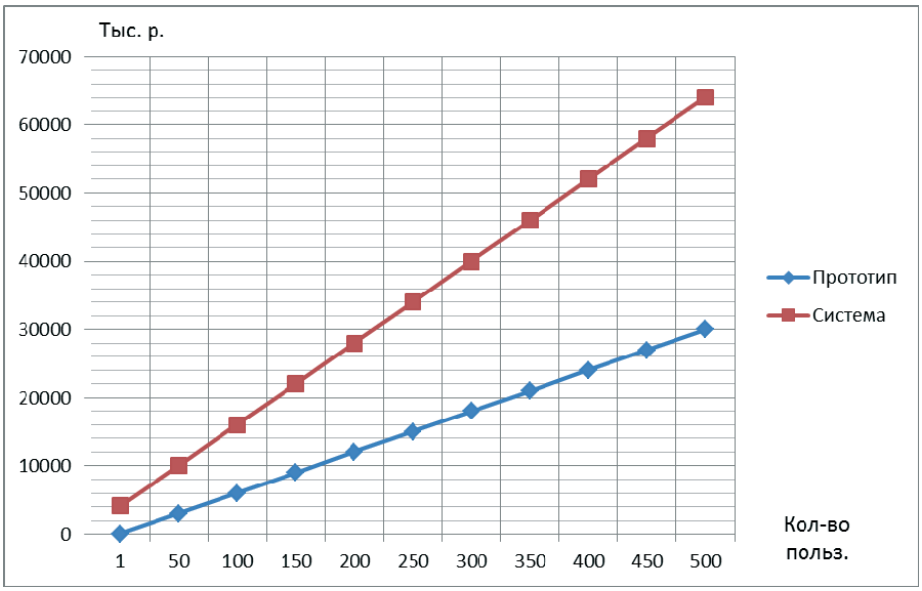

Рис. 4. *График зависимости ресурсоемкости технических решений по предоставлению услуг для прототипа и предложенной системы управления безопасностью МАУ от количества пользователей МАУ*

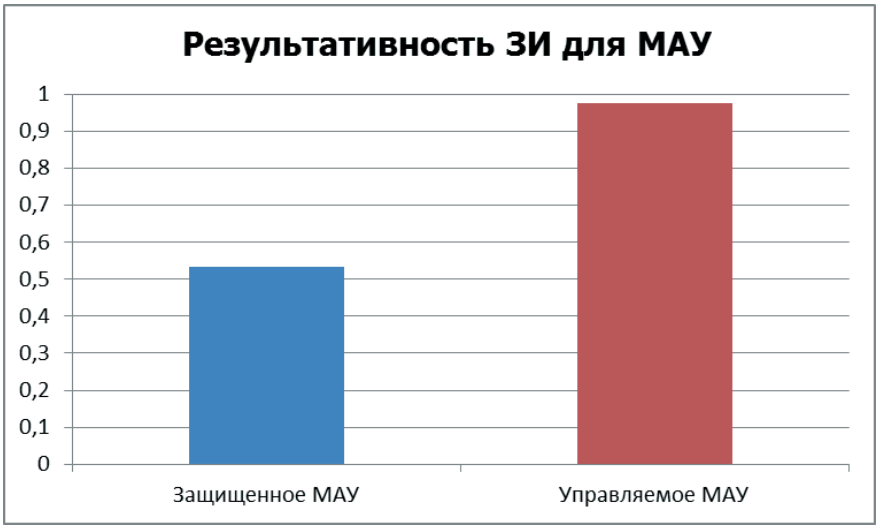

***Рис.5**. Оценка результативности защиты информации при эксплуатации МАУ*

Численные значения ресурсоемкости представлены на рисунке 4. С учетом выражения (17) и данных численных значений, а также в зависимости от количество пользователей МАУ были получены оценки получаемого эффекта от внедрения разработанной системы управления безопасностью МАУ и управляемых МАУ по сравнению с применяемым в настоящее время прототипом. Сравнительный анализ получаемых эффектов представлен на рисунке 6.

Анализ рисунка 6 показывает, что получаемый эффект для разработанной системы выше, чем для используемого в настоящее время прототипа. При этом необходимо отметить, что существенный вклад в получаемый эффект вносит повышение числа доступных пользователю МАУ услуг.

Заключение

В работе предложена методика расчета оценки эффективности защиты информации при эксплуатации МАУ в корпоративных сетях с разными требованиями по защищенности. Представлены примеры расчета оценок таких параметров как вероятности нарушения конфиденциальности информации, вероятности сохранения конфиденциальности информации, коэффициента доступности услуг, вероятности обеспечения доступности услуг и ресурсоемкости процесса защиты информации.

Предложенная методика может быть использована для оценивания результативности функционирования перспективных СЗИ, разрабатываемых для обеспечения безопасности информации в защищенных корпоративных сетях, в которых предусмотрена эксплуатация МАУ для доступа к защищаемой информации и услугам с разными требованиями по защищенности.

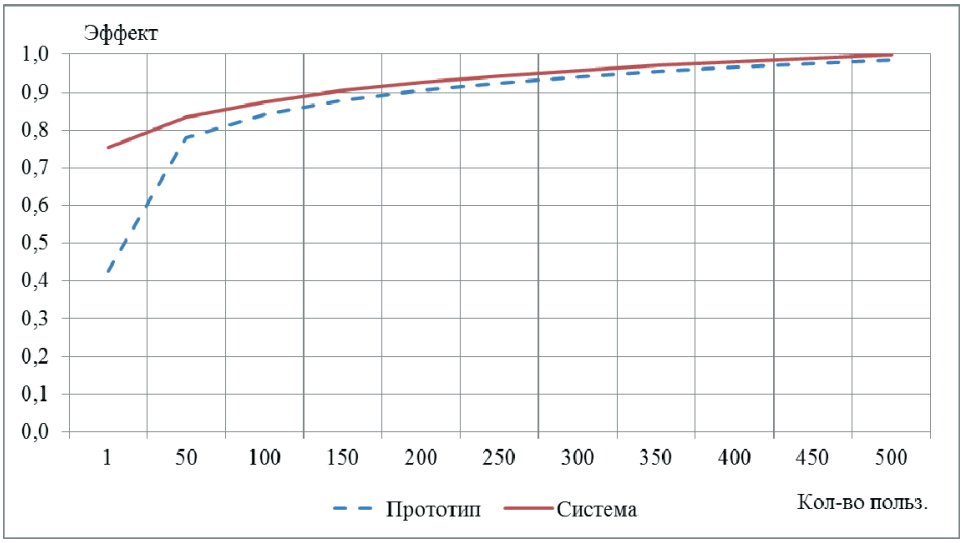

***Рис. 6**. Сравнительный анализ получаемого эффекта для прототипа и разработанной системы*

Рецензент: *Коськин А.В., доктор технических наук, профессор кафедры информационных систем ФГБОУ ВО «ОГУ имени И.С.Тургенева»*

Литература:

1. Маркин Д.О., Комашинский В.В., Баранов И.Ю. Модель управления профилем защиты мобильного устройства при доступе к услугам с разным уровнем конфиденциальности // Информационные технологии. 2015. Т. 21. № 8. С. 611-618.
2. Петухов Г.Б. Основы теории эффективности целенаправленных процессов. Часть 1. Методология, методы, модели. Учебное пособие. М.: Издательство МО СССР, 1989. 660 с.
3. Бочков М.В. Адаптивная защита информации от несанкционированного доступа в вычислительных сетях / М.В. Бочков, С.Н. Бушуев, В.А. Логинов, И.Б. Саенко. СПб.: ВАС, 2005. 172 с.
4. Девянин, П.Н. Теоретические основы компьютерной безопасности: Учеб. пособие для вузов / П.Н. Девянин, О.О., Михальский, Д.И. Правиков, А.Ю. Щербаков. М.: Радио и связь, 2000. 192 с.
5. Бельтов А.Г., Жуков И.Ю., Новицкий А.В., Михайлов Д.М., Стариковский А.В. Вопросы безопасности мобильных устройств // Безопасность информационных технологий. 2012. № 2s. С. 5-7.
6. Десницкий, В.А. Конфигурирование безопасных встроенных устройств с учетом показателей ресурсопотребления: автореферат дис. ... кандидата технических наук : 05.13.19 / Санкт-Петербургский институт информатики и автоматизации Российской академии наук. Санкт-Петербург, 2013.
7. Маркин Д.О., Комашинский В.В., Двилянский А.А. Алгоритм управления программно-аппаратной конфигурацией защищенного мобильного абонентского устройства // Промышленные АСУ и контроллеры. 2016. № 9. С. 39-50.
8. Маркин Д.О., Комашинский В.В., Двилянский А.А. Модель состояний мобильного абонентского устройства в помещениях с разными требованиями по защищенности // Промышленные АСУ и контроллеры. 2016. № 10. С. 49-60.
9. 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.
10. Свидетельство о государственной регистрации программы для ЭВМ № 2014617119 Российская Федерация. Автоматизированная система оценки параметров защищенности удаленного доступа к услугам защищенной корпоративной сети пользователя мобильного устройства / Д. О. Маркин, Л. К. Саморцев, А. А. Смыкалов; заявл. 21.05.2014; зарегистрировано в Реестре программ для ЭВМ 11.07.2014 г.
11. 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.

METHODS FOR ASSESSMENT OF THE INFORMATION SECURITY EFFICIENCY WHEN EMPLOYING MOBILE USER DEVICES IN THE CORPORATE NETWORKS WITH VARIOUS SECURITY REQUIREMENTS

Markin D.O. [4]***, Komashinskij V.V.*** [5]***, Senotrusov I.A.*** [6]

The paper proposes methods to calculate the rate of the information security efficiency when using mobile user devices in the corporate networks with various security requirements. The task for developing the methods for assessment of the information security was formally described. The paper describes limitations and assumptions, within which framework the suggested methods can be applied. It provides examples for calculating such parameters as probability of information confidentiality breach, probability of preserving confidentiality of the information, service availability ratio, and probability of the service availability assurance and resource intensity of the information protection process. The calculations used source data from the regulatory and legal framework, known published works of the author and other sources. The paper specifies the results of assessment of the information security performance and the effect from implementing the assessed information security system. The suggested methods can be used to assess performance of

4 Dmitrij Markin, independent expert, Orjol, admin@nikitka.net.
5 Vladimir Komashinskij, Ph.D., Assistant Professor, independent expert, Oryol, vladkom-orel@mail.ru.
6 Igor› Senotrusov, Ph.D., Assistant Professor, independent expert, Oryol, wsilvez@mail.ru.

promising information security tools that are under development in order to ensure information security in the secure corporate networks, which provide for the use of mobile user devices for access to the sensitive information and services with various security– level requirements.

***Keywords**: information security effectiveness evaluation, mobile device, information confidentiality, protection tools*

References:

1. Markin D.O., Komashinskiy V.V., Baranov I.Yu. Model' upravleniya profilem zashchity mobil'nogo ustroystva pri dostupe k uslugam s raznym urovnem konfidentsial'nosti, Informatsionnye tekhnologii. 2015. T. 21. No 8, pp. 611-618.
2. Petukhov G.B. Osnovy teorii effektivnosti tselenapravlennykh protsessov. Chast' 1. Metodologiya, metody, modeli. Uchebnoe posobie. M.: Izdatel'stvo MO SSSR, 1989. 660 P.
3. Bochkov M.V. Adaptivnaya zashchita informatsii ot nesanktsionirovannogo dostupa v vychislitel'nykh setyakh / M.V. Bochkov, S.N. Bushuev, V.A. Loginov, I.B. Saenko. SPb.: VAS, 2005. 172 P.
4. Devyanin, P.N. Teoreticheskie osnovy komp'yuternoy bezopasnosti : Ucheb. posobie dlya vuzov / P.N. Devyanin, O.O., Mikhal'skiy, D.I. Pravikov, A.Yu. Shcherbakov. M.: Radio i svyaz', 2000. 192 P.
5. Bel'tov A.G., Zhukov I.Yu., Novitskiy A.V., Mikhaylov D.M., Starikovskiy A.V. Voprosy bezopasnosti mobil'nykh ustroystv, Bezopasnost' informatsionnykh tekhnologiy. 2012. No 2s, pp. 5-7.
6. Desnitskiy, V.A. Konfigurirovanie bezopasnykh vstroennykh ustroystv s uchetom pokazateley resursopotrebleniya: avtoreferat dis. ... kandidata tekhnicheskikh nauk : 05.13.19 / Sankt-Peterburgskiy institut informatiki i avtomatizatsii Rossiyskoy akademii nauk. Sankt-Peterburg, 2013.
7. Markin D.O., Komashinskiy V.V., Dvilyanskiy A.A. Algoritm upravleniya programmno-apparatnoy konfiguratsiey zashchishchennogo mobil'nogo abonentskogo ustroystva, Promyshlennye ASU i kontrollery. 2016. No 9, pp. 39-50.
8. Markin D.O., Komashinskiy V.V., Dvilyanskiy A.A. Model' sostoyaniy mobil'nogo abonentskogo ustroystva v pomeshcheniyakh s raznymi trebovaniyami po zashchishchennosti, Promyshlennye ASU i kontrollery. 2016. No 10, pp. 49-60.
9. Svidetel'stvo o gosudarstvennoy registratsii programmy dlya EVM № 2013618388 Rossiyskaya Federatsiya. Analizator konteksta dostupa mobil'nogo ustroystva / D. O. Markin, S. V. Shekshuev, V. V. Komashinskiy ; zayavl. 19.07.2013; zaregistrirovano v Reestre programm dlya EVM 06.09.2013 g.
10. Svidetel'stvo o gosudarstvennoy registratsii programmy dlya EVM № 2014617119 Rossiyskaya Federatsiya. Avtomatizirovannaya sistema otsenki parametrov zashchishchennosti udalennogo dostupa k uslugam zashchishchennoy korporativnoy seti pol'zovatelya mobil'nogo ustroystva / D. O. Markin, L. K. Samortsev, A. A. Smykalov ; zayavl. 21.05.2014; zaregistrirovano v Reestre programm dlya EVM 11.07.2014 g.
11. Svidetel'stvo o gosudarstvennoy registratsii programmy dlya EVM № 2015615631 Rossiyskaya Federatsiya. Avtomatizirovannaya sistema opredeleniya mestopolozheniya pol'zovateley mobil'nykh ustroystv vnutri zdaniya na osnove signalov besprovodnoy seti / D. O. Markin, N. I. Birkun, A. O. Zozulya ; zayavl. 24.03.2015; zaregistrirovano v Reestre programm dlya EVM 21.05.2015 g.