Отчет о проверке

Вернуться в кабинет

Уважаемый пользователь!
Обращаем ваше внимание, что система Антиплагиат отвечает на вопрос, является ли тот или иной фрагмент текста заимствованным или нет. Ответ на вопрос, является ли заимствованный фрагмент именно плагиатом, а не законной цитатой, система оставляет на ваше усмотрение. Также важно отметить, что система находит источник заимствования, но не определяет, является ли он первоисточником.

Информация о документе:

Имя исходного файла:	00 Диссертация от 2018-01-15.pdf
Имя компании:	ТУСУР
Тип документа:	Прочее
Имя документа:	00 Диссертация от 2018-01-15.pdf
Дата проверки:	17.01.2018 14:59
Модули поиска:	Интернет (Антиплагиат), Модуль поиска ЭБС "Айбукс", Модуль поиска ЭБС "Лань", Университетская библиотека онлайн, Диссертации и авторефераты РГБ, Цитирования, Модуль поиска ЭБС БиблиоРоссика

Текстовые статистики:

Индекс читаемости:	сложный
Неизвестные слова:	в пределах нормы
Макс. длина слова:	в пределах нормы
Большие слова:	в пределах нормы

Тип отчета: Улучшенный О типах отчетов

■	Источник	Ссылка на источник	Коллекция/модуль поиска	Доля в отчёте	Доля в тексте
☐	**[1]** Д.О. Маркин. Исследо...	http://rsreu.ru/ru/component/docman/doc_download/6967-d-o-ma...	Интернет (Антиплагиат)	0	6,44%
☑	**[2]** Модели безопасности ...	http://ibooks.ru/reading.php?short=1&productid=344413	Модуль поиска ЭБС "Айбукс"	3,47%	3,47%
☑	**[3]** 63235	http://e.lanbook.com/books/element.php?pl1_id=63235	Модуль поиска ЭБС "Лань"	0,05%	3,41%
☑	**[4]** 275208	http://biblioclub.ru/index.php?page=book_red&id=275208	Университетская библиотека онлайн	0%	3,4%
☐	**[5]** Сборник научных труд...	http://www.ssau.ru/files/events/2016/sb_trudov_pit2016.pdf	Интернет (Антиплагиат)	0	2,03%
☑	**[6]** Диссертация на соиск...	http://www.tu-bryansk.ru/doc/diss/makeev/diss.pdf	Интернет (Антиплагиат)	1,38%	1,38%
☑	**[7]** Теоретические основы...	http://pandia.ru/text/78/407/35629-6.php	Интернет (Антиплагиат)	0,01%	1,36%
☑	**[8]** Дунин, Вадим Сергеев...	http://dlib.rsl.ru/rsl01005000000/rsl01005521000/rsl01005521...	Диссертации и авторефераты РГБ	1,18%	1,24%
☑	**[9]** 253178	http://biblioclub.ru/index.php?page=book_red&id=253178	Университетская библиотека онлайн	0,08%	1,04%
☑	**[10]** Обзорные лекции по м...	http://www.lib.tsu.ru/mminfo/000349342/P_02/image/P_02_151.p...	Интернет (Антиплагиат)	0%	1,03%
☑	**[11]** Базовая модель угроз...	http://www.linguanet.ru/svd/svd3/zpd/nbpd7.pdf#2	Интернет (Антиплагиат)	0,11%	1%
☑	**[12]** Аютова, Ирина Владим...	http://dlib.rsl.ru/rsl01005000000/rsl01005473000/rsl01005473...	Диссертации и авторефераты РГБ	0,03%	0,98%
☑	**[13]** Базовая модель угроз...	https://linguanet.ru/svd/svd3/zpd/nbpd7.pdf	Интернет (Антиплагиат)	0%	0,98%
☑	**[14]** Источник 14	http://www.nsu.ru/xmlui/bitstream/handle/nsu/1327/Text_Batal...	Интернет (Антиплагиат)	0,13%	0,87%
☑	**[15]** Козачок, Александр В...	http://dlib.rsl.ru/rsl01006000000/rsl01006523000/rsl01006523...	Диссертации и авторефераты РГБ	0,37%	0,86%
☑	**[16]** ko`chirish	http://library.tuit.uz/knigiPDF/106.pdf	Интернет (Антиплагиат)	0%	0,79%
☑	**[17]** Ерохин, Сергей Серге...	http://dlib.rsl.ru/rsl01004000000/rsl01004721000/rsl01004721...	Диссертации и авторефераты РГБ	0,55%	0,73%
☑	**[18]** Источник 18	http://window.edu.ru/resource/546/38546/files/shamkin2.pdf	Интернет (Антиплагиат)	0,02%	0,71%
☑	**[19]** Сборник научных труд...	http://ssau.ru/files/events/2015/pit_2015_2.pdf	Интернет (Антиплагиат)	0,64%	0,68%
☑	**[20]** pdf	http://jre.cplire.ru/alt/oct14/7/text.pdf	Интернет (Антиплагиат)	0,67%	0,67%
☑	**[21]** Козачок, Андрей Васи...	http://dlib.rsl.ru/rsl01004000000/rsl01004638000/rsl01004638...	Диссертации и авторефераты РГБ	0,17%	0,65%
☑	**[22]** S2 - 2016	http://h-es.ru/images/archive/Nom-s2-2016.pdf	Интернет (Антиплагиат)	0,58%	0,64%

☑	**[23]** №3 - 2015 (5/6)	http://h-es.ru/images/archive/Nom-3-2015.pdf#5	Интернет (Антиплагиат)	0,19%	0,61%
☑	**[24]** Конфиденциальное дел...	http://ibooks.ru/reading.php?short=1&productid=29403	Модуль поиска ЭБС "Айбукс"	0,06%	0,6%
☑	**[25]** Критически важные об...	http://ibooks.ru/reading.php?short=1&productid=29335	Модуль поиска ЭБС "Айбукс"	0,26%	0,57%
☐	**[26]** Источник 26		Цитирования	0	0,52%
	[27] Чемин, Александр Але...	http://dlib.rsl.ru/rsl01004000000/rsl01004594000/rsl01004594...	Диссертации и авторефераты РГБ	0%	0,5%
	[28] Критически важные об...	http://ibooks.ru/reading.php?short=1&productid=29334	Модуль поиска ЭБС "Айбукс"	0%	0,49%
	[29] Конфиденциальное дел...	http://biblioclub.ru/index.php?page=book_red&id=84996	Университетская библиотека онлайн	0%	0,49%
	[30] здесь	http://school.uni-altai.ru/files/822.pdf	Интернет (Антиплагиат)	0,49%	0,49%
	[31] Конфиденциальное дел...	http://www.bibliorossica.com/book.html?&currBookId=14488	Модуль поиска ЭБС БиблиоРоссика	0%	0,46%
	[32] Компьютерное моделир...	http://www.bibliorossica.com/book.html?&currBookId=8694	Модуль поиска ЭБС БиблиоРоссика	0,01%	0,44%
	[33] Зыков, Владимир Дмит...	http://dlib.rsl.ru/rsl01004000000/rsl01004824000/rsl01004824...	Диссертации и авторефераты РГБ	0,01%	0,44%
	[34] 276557	http://biblioclub.ru/index.php?page=book_red&id=276557	Университетская библиотека онлайн	0,02%	0,44%
	[35] Климушев, Николай Ко...	http://dlib.rsl.ru/rsl01004000000/rsl01004395000/rsl01004395...	Диссертации и авторефераты РГБ	0,01%	0,43%
	[36] PDF	http://proceedings.spiiras.nw.ru/ojs/index.php/sp/issue/down...	Интернет (Антиплагиат)	0,08%	0,43%
	[37] Павельев, Сергей Вла...	http://dlib.rsl.ru/rsl01004000000/rsl01004236000/rsl01004236...	Диссертации и авторефераты РГБ	0%	0,42%
	[38] Эдель, Дмитрий Алекс...	http://dlib.rsl.ru/rsl01006000000/rsl01006605000/rsl01006605...	Диссертации и авторефераты РГБ	0,07%	0,4%
	[39] ko`chirish	http://library.tuit.uz/knigiPDF/92.pdf	Интернет (Антиплагиат)	0,01%	0,4%
	[40] Бизнес в законе	http://ibooks.ru/reading.php?short=1&productid=338633	Модуль поиска ЭБС "Айбукс"	0,1%	0,35%
	[41] Колегов, Денис Никол...	http://dlib.rsl.ru/rsl01004000000/rsl01004406000/rsl01004406...	Диссертации и авторефераты РГБ	0,05%	0,35%
	[42] Крылов, Григорий Оле...	http://dlib.rsl.ru/rsl01004000000/rsl01004039000/rsl01004039...	Диссертации и авторефераты РГБ	0,01%	0,33%
	[43] Материалы Второй меж...	http://ibooks.ru/reading.php?short=1&productid=29317	Модуль поиска ЭБС "Айбукс"	0,03%	0,33%
	[44] Ястребов, Илья Серге...	http://dlib.rsl.ru/rsl01004000000/rsl01004896000/rsl01004896...	Диссертации и авторефераты РГБ	0,23%	0,31%
	[45] 231889	http://biblioclub.ru/index.php?page=book_red&id=231889	Университетская библиотека онлайн	0,02%	0,29%
	[46] Политики безопасност...	http://biblioclub.ru/index.php?page=book_red&id=85101	Университетская библиотека онлайн	0%	0,27%
	[47] 40030	http://e.lanbook.com/books/element.php?pl1_id=40030	Модуль поиска ЭБС "Лань"	0%	0,27%
	[48] 3032	http://e.lanbook.com/books/element.php?pl1_id=3032	Модуль поиска ЭБС "Лань"	0%	0,27%
	[49] Чечулин, Андрей Алек...	http://dlib.rsl.ru/rsl01006000000/rsl01006751000/rsl01006751...	Диссертации и авторефераты РГБ	0,01%	0,26%
	[50] Вестник Томского гос...	http://ibooks.ru/reading.php?short=1&productid=342112	Модуль поиска ЭБС "Айбукс"	0,04%	0,26%
	[51] Суворова, Вероника А...	http://dlib.rsl.ru/rsl01004000000/rsl01004895000/rsl01004895...	Диссертации и авторефераты РГБ	0,01%	0,25%
	[52] Защита компьютерной ...	http://ibooks.ru/reading.php?short=1&productid=26730	Модуль поиска ЭБС "Айбукс"	0,01%	0,25%
	[53] Организация и технол...	http://ibooks.ru/reading.php?short=1&productid=352907	Модуль поиска ЭБС "Айбукс"	0,02%	0,25%
	[54] 66085	http://e.lanbook.com/books/element.php?pl1_id=66085	Модуль поиска ЭБС "Лань"	0%	0,24%
	[55] Защита компьютерной ...	http://www.bibliorossica.com/book.html?&currBookId=5631	Модуль поиска ЭБС БиблиоРоссика	0%	0,24%
	[56] 1122	http://e.lanbook.com/books/element.php?pl1_id=1122	Модуль поиска ЭБС "Лань"	0%	0,24%
	[57] 50578	http://e.lanbook.com/books/element.php?pl1_id=50578	Модуль поиска ЭБС "Лань"	0,01%	0,24%
	[58] Научно-технический в...	http://www.bibliorossica.com/book.html?&currBookId=17605	Модуль поиска ЭБС БиблиоРоссика	0,01%	0,23%
	[59] 227774	http://biblioclub.ru/index.php?page=book_red&id=227774	Университетская библиотека онлайн	0%	0,23%
	[60] Организация и технол...	http://biblioclub.ru/index.php?page=book_red&id=74298	Университетская библиотека онлайн	0%	0,22%
	[61] Информационная безоп...	http://www.bibliorossica.com/book.html?&currBookId=19051	Модуль поиска ЭБС БиблиоРоссика	0,03%	0,22%
	[62] 59240	http://e.lanbook.com/books/element.php?pl1_id=59240	Модуль поиска ЭБС "Лань"	0%	0,22%
	[63] Вестник Томского гос...	http://ibooks.ru/reading.php?short=1&productid=342104	Модуль поиска ЭБС "Айбукс"	0%	0,22%
	[64] 59434	http://e.lanbook.com/books/element.php?pl1_id=59434	Модуль поиска ЭБС "Лань"	0%	0,21%
☑	**[65]** Конявский, Валерий А...	http://dlib.rsl.ru/rsl01002000000/rsl01002752000/rsl01002752...	Диссертации и авторефераты РГБ	0%	0,21%

	[66] Краткий энциклопедич...	http://ibooks.ru/reading.php?short=1&productid=337423	Модуль поиска ЭБС "Айбукс"	0%	0,21%
	[67] Обеспечение информац...	http://www.bibliorossica.com /book.html?&currBookId=14618	Модуль поиска ЭБС БиблиоРоссика	0%	0,2%
	[68] Куркин, Андрей Влади...	http://dlib.rsl.ru/rsl01005000000/rsl01005390000 /rsl01005390...	Диссертации и авторефераты РГБ	0,14%	0,19%
	[69] Технические науки – ...	http://www.bibliorossica.com /book.html?&currBookId=15342	Модуль поиска ЭБС БиблиоРоссика	0%	0,15%
	[70] Информационная безоп...	http://www.bibliorossica.com /book.html?&currBookId=6182	Модуль поиска ЭБС БиблиоРоссика	0%	0,15%
	[71] Базы данных / Технол...	http://www.studfiles.ru/dir/cat32/subj95/file2869 /view3900/p...	Интернет (Антиплагиат)	0,01%	0,14%
	[72] Диссертация	https://www.mirea.ru/upload/medialibrary /0f8/dissertatsiya.p...	Интернет (Антиплагиат)	0,09%	0,14%
	[73] Модели безопасности ...	http://ibooks.ru/reading.php?short=1&productid=333393	Модуль поиска ЭБС "Айбукс"	0,01%	0,13%
	[74] Известия Томского по...	http://biblioclub.ru/index.php?page=book_red&id=99214	Университетская библиотека онлайн	0%	0,12%
	[75] Салех Хади Мухаммед ...	http://dlib.rsl.ru/rsl01006000000/rsl01006702000 /rsl01006702...	Диссертации и авторефераты РГБ	0,05%	0,11%
	[76] Морозов, Игорь Андре...	http://dlib.rsl.ru/rsl01003000000/rsl01003321000 /rsl01003321...	Диссертации и авторефераты РГБ	0,05%	0,08%
	[77] Научно-технический в...	http://www.bibliorossica.com /book.html?&currBookId=17604	Модуль поиска ЭБС БиблиоРоссика	0%	0,08%
	[78] Современная компьюте...	http://www.bibliorossica.com /book.html?&currBookId=7563	Модуль поиска ЭБС БиблиоРоссика	0%	0,08%
	[79] Современная компьюте...	http://biblioclub.ru/index.php?page=book_red&id=89798	Университетская библиотека онлайн	0%	0,08%
	[80] Сухов, Владимир Алек...	http://dlib.rsl.ru/rsl01005000000/rsl01005484000 /rsl01005484...	Диссертации и авторефераты РГБ	0,02%	0,07%
	[81] Основы информационно...	http://ibooks.ru/reading.php?short=1&productid=27907	Модуль поиска ЭБС "Айбукс"	0%	0,06%
	[82] 10927	http://e.lanbook.com/books/element.php?pl1_id=10927	Модуль поиска ЭБС "Лань"	0%	0,06%
	[83] Информационная безоп...	http://ibooks.ru/reading.php?short=1&productid=351301	Модуль поиска ЭБС "Айбукс"	0%	0,06%
	[84] 1049	http://e.lanbook.com/books/element.php?pl1_id=1049	Модуль поиска ЭБС "Лань"	0%	0,06%
	[85] 56372	http://e.lanbook.com/books/element.php?pl1_id=56372	Модуль поиска ЭБС "Лань"	0,03%	0,06%
	[86] Естественные и техни...	http://ibooks.ru/reading.php?short=1&productid=340210	Модуль поиска ЭБС "Айбукс"	0%	0,05%
	[87] 5155	http://e.lanbook.com/books/element.php?pl1_id=5155	Модуль поиска ЭБС "Лань"	0,02%	0,04%
	[88] 65912	http://e.lanbook.com/books/element.php?pl1_id=65912	Модуль поиска ЭБС "Лань"	0%	0,03%
	[89] Применение математич...	http://ibooks.ru/reading.php?short=1&productid=340980	Модуль поиска ЭБС "Айбукс"	0%	0,03%
	[90] Технические средства...	http://www.bibliorossica.com /book.html?&currBookId=6569	Модуль поиска ЭБС БиблиоРоссика	0%	0,03%
	[91] Численные методы	http://www.bibliorossica.com /book.html?&currBookId=8268	Модуль поиска ЭБС БиблиоРоссика	0,03%	0,03%
	[92] 120213	http://biblioclub.ru/index.php?page=book_red&id=120213	Университетская библиотека онлайн	0%	0,03%
	[93] Источник 93	http://window.edu.ru/resource/302/75302/files/%D0%9F %D0%B5%D...	Интернет (Антиплагиат)	0,03%	0,03%
	[94] Вестник новых медици...	http://www.bibliorossica.com /book.html?&currBookId=16416	Модуль поиска ЭБС БиблиоРоссика	0,02%	0,03%
	[95] 219845	http://biblioclub.ru/index.php?page=book_red&id=219845	Университетская библиотека онлайн	0%	0,03%
	[96] 8718	http://e.lanbook.com/books/element.php?pl1_id=8718	Модуль поиска ЭБС "Лань"	0,02%	0,02%
	[97] Вестник РГГУ. № 12 (...	http://www.bibliorossica.com /book.html?&currBookId=17913	Модуль поиска ЭБС БиблиоРоссика	0%	0,02%
	[98] 50569	http://e.lanbook.com/books/element.php?pl1_id=50569	Модуль поиска ЭБС "Лань"	0%	0,02%
	[99] Электронная лаборато...	http://www.bibliorossica.com /book.html?&currBookId=10601	Модуль поиска ЭБС БиблиоРоссика	0%	0,02%
	[100] 13745	http://e.lanbook.com/books/element.php?pl1_id=13745	Модуль поиска ЭБС "Лань"	0%	0,02%
	[101] Научно-технический в...	http://www.bibliorossica.com /book.html?&currBookId=17606	Модуль поиска ЭБС БиблиоРоссика	0%	0,02%
	[102] Нечеткое моделирован...	http://ibooks.ru/reading.php?short=1&productid=335302	Модуль поиска ЭБС "Айбукс"	0%	0,02%
	[103] Компьютерные сети. 5...	http://ibooks.ru/reading.php?short=1&productid=344101	Модуль поиска ЭБС "Айбукс"	0%	0,02%
	[104] 225482	http://biblioclub.ru/index.php?page=book_red&id=225482	Университетская библиотека онлайн	0,02%	0,02%
	[105] Защита от хакеров бе...	http://www.bibliorossica.com /book.html?&currBookId=5743	Модуль поиска ЭБС БиблиоРоссика	0,01%	0,01%
	[106] Одномерные дискретны...	http://www.bibliorossica.com /book.html?&currBookId=18811	Модуль поиска ЭБС БиблиоРоссика	0,01%	0,01%
	[107] Экспериментальная пс...	http://www.bibliorossica.com /book.html?&currBookId=10813	Модуль поиска ЭБС БиблиоРоссика	0,01%	0,01%
☑	**[108]** Экспериментальная пс...	http://biblioclub.ru/index.php?page=book_red&id=87641	Университетская библиотека онлайн	0%	0,01%

Внимание! В отчете присутствуют удаленные блоки или источники.

Пересчитать | Другие действия | Печать

Оригинальные блоки: 88,2%
Заимствованные блоки: 11,8%
Заимствование из "белых" источников: 0%
Итоговая оценка оригинальности: **88,2%**

Страницы: 1 2 3 4 Все

АКАДЕМИЯ ФЕДЕРАЛЬНОЙ СЛУЖБЫ ОХРАНЫ РОССИЙСКОЙ ФЕДЕРАЦИИ
На правах рукописи
[6]

Маркин Дмитрий Олегович
УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ МОБИЛЬНЫХ АБОНЕНТСКИХ
УСТРОЙСТВ В КОРПОРАТИВНЫХ СЕТЯХ

Специальность 05.13.19 – [15]Методы и системы защиты информации,
информационная безопасность
[8]Диссертация на соискание ученой степени
кандидата технических наук
Научный руководитель:
кандидат технических наук, доцент
[6]

Комашинский Владимир Владимирович
Орёл 2017
2
ОГЛАВЛЕНИЕ

3

6

ВВЕДЕНИЕ

Актуальность темы. [6]

Развитие современных многофункциональных мобильных абонентских устройств (МАУ) [69] и информационных технологий, пропускной способности каналов связи, в том числе беспроводных, приводят к постоянному росту потребности в доступе к информации [71], причем независимо от того, где находится пользователь. В этом отношении не являются исключением и корпоративные сети, в том числе, защищенные (ЗКС), предоставляющие доступ к инфокоммуникационным услугам и ресурсам с разными требованиями по защищенности. К таким сетям относятся, в том числе, информационные системы общего пользования, информационные системы, обрабатывающие персональные данные, а также геоинформационные системы.

Удаленный доступ с использованием МАУ к корпоративным сетям с разными требованиями по защищенности подразумевает применение соответствующих систем защиты безопасности, позволяющих обеспечить требуемый уровень обеспечения безопасности информации независимо от уровня защищенности сегмента защищенной корпоративной сети. При этом принципиальным требованием является использовании сотрудниками (пользователями) ЗКС единого мобильного устройства для осуществления такого доступа. Различие по требованиям защищенности в ЗКС, как правило, делит такую сеть на контуры обработки информации, которые, в свою очередь, обычно ограничены специализированными помещениями с известным расположением на объектах организации.

Однако использование современных МАУ, обладающих значительными вычислительными и коммуникационными ресурсами, для обработки конфиденциальной информации ограничено в ��вязи с рядом существенных особенностей, касающихся их эксплуатации: размерами, мобильностью пользователей, многофункциональностью.

Указанные особенности определяют совершенно иной спектр угроз информационной безопасности при работе с МАУ по сравнению со стационарными средствами вычислительной техники (СВТ). Постоянная смена местоположения
7
пользователей МАУ, беспроводный удаленный доступ к сетям с разными требованиями по защищенности, ограниченные вычислительные возможности с одной

стороны и высокоскоростные коммуникационные с другой создают большое количество угроз информационной безопасности, связанных в первую очередь с угрозами нарушения конфиденциальности информации [17].

С другой стороны перспективным направлением совершенствования современных корпоративных сетей является обеспечение предоставления защищенного доступа абонентам к информации и услугам с разными требованиями по защищенности при использовании единого МАУ [10, 30, 58]. При этом к предоставляемым услугам в соответствие относятся:

телефонная и видеосвязь с дополнительными видами обслуживания;

защищенный электронный почтовый обмен с элементами учета входящих и исходящих документов;

видеоконференцсвязь;

доступ к базам и банкам данных, сетевым приложениям и информационным ресурсам.

Необходимость предоставления указанного перечня услуг с использованием одного универсального абонентского устройства пользователям, учитывая, что услуги могут предоставляться сетями с разными требованиями по защищенности, позволяет говорить о том, что существует объективная потребность в разработке универсального МАУ и системы защиты информации (СЗИ), позволяющей обеспечить конфиденциальность информации [17] при своевременном [18] предоставлении доступа к указанному перечню услуг с использованием одного МАУ. Задачей СЗИ будет являться обеспечение безопасности информации при доступе к услугам сетей с разными требованиями по защищенности с использованием МАУ, путем управления безопасностью МАУ с помощью адаптивного изменения его программно-аппаратной конфигурации, позволяющего согласовывать состояние МАУ с условиями (атрибутами) доступа, требованиям безопасности корпоративной сети, а также требованиями по качеству предоставляемых услуг.

8

Анализ существующих научных исследований [47], технических и программно-аппаратных решений, а также нормативно-правовой базы в области защиты информации при работе с МАУ показал, что в настоящее время:

1) существующие технические решения, позволяющие управлять функциональностью (конфигурацией) МАУ, не предполагают определения вероятности нахождения пользователя МАУ в специальных помещениях, к которым предъявляются повышенные требования по обеспечению информационной безопасности (ИБ) в корпоративной сети, и не позволяют заблаговременно предотвращать работу МАУ тех режимах, которые при текущем местоположении МАУ запрещены;

2) доступ к сетям с разными требованиями по защищенности осуществляется либо с использованием нескольких зарегистрированных в корпоративной сети МАУ, соответствующих необходимому уровню защиты либо с использованием автоматизированного переключения режимов работы; отсутствует автоматическое управление МАУ в зависимости от требований защищенности сети, к которой предоставляется доступ, а также местоположения МАУ; в случае доступа к информационным ресурсам сторонней организации с использованием личных или корпоративных МАУ в настоящее время действуют организационно-технические ограничения.

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 других. В области защиты информации при эксплуатации

9

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 доступа к услугам корпоративных сетей с разными требованиями по защищенности рассмотрены недостаточно полно.

На основе анализа тенденций и перспектив развития современных корпоративных сетей выявлено противоречие между требованиями, предъявляемыми к безопасности информации [18] при доступе к защищенным услугам и информации с использованием универсальных МАУ, и техническими возможностями СЗИ, позволяющих обеспечить безопасность информации при осуществлении такого доступа в корпоративных сетях с разными требованиями по защищенности.

На основании этого выдвинута гипотеза исследования, заключающаяся в том, что для повышения вероятности обеспечения безопасности информации при эксплуатации МАУ и обеспечении безопасного доступа к услугам корпоративных 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 научнотехнические предложения по реализации системы управления безопасностью МАУ в корпоративных сетях с разными требованиями по защищенности.

Перечисленные факторы обусловливают актуальность темы диссертационного исследования: "Управление безопасностью мобильных абонентских устройств в корпоративных сетях".

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

10

корпоративных сетях с разными требованиями по защищенности при использовании единого МАУ.

Научная задача исследования: на основе формальной модели безопасности МАУ разработать алгоритм управления безопасностью 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.

Частные научные задачи исследования:

1) провести анализ существующих научных исследований и технических решений по защите информации в МАУ, а также способов построения систем защиты информации при доступе к сетям с разными требованиями по защищенности с использованием единого устройства; разработать систему показателей качества, позволяющую оценить эффективность процесса защиты информации при эксплуатации системы управления безопасностью МАУ в корпоративных сетях с разными требованиями по защищенности;

2) разработать формальную модель безопасности МАУ, отличающуюся от известных учетом местонахождения МАУ в специальных помещениях, к которым предъявляются повышенные требования по ИБ, обосновать ее корректность;

3) разработать алгоритм управления безопасностью МАУ, учитывающий атрибуты доступа пользователей МАУ, включающие в себя, в том числе, вероятность нахождения МАУ в специальном помещении, а также требования по качеству предоставляемых услуг; разработать моделирующий алгоритм и осуществить имитационное моделирование функционирования системы управления безопасностью МАУ для получения оценки эффективности предложенных технических решений;

4) сформировать научно-технические предложения по практической реализации системы управления безопасностью МАУ в корпоративных сетях, а также

11
рекомендации по выбору параметров алгоритмов определения местоположения
МАУ в помещениях корпоративной сети и алгоритма вычисления вероятности
нахождения МАУ в специальном помещении.

Решение научной задачи основывается на использовании теории машинного обучения, [15]

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.
Основные положения, выносимые на защиту:
1. Модель безопасности мобильного абонентского устройства в корпоративных сетях с разными требованиями по защищенности [39, 46, 50, 43, 51, 76, 79].
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 [41, 48, 49, 77].
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 [40, 45, 47, 60, 61, 62, 75, 78, 80].
Научная новизна диссертационной работы заключается:
в разработке и обосновании корректности новой формальной модели безопасности МАУ, отличающейся от известных учетом оценки его местонахождения в специальном помещении, других атрибутов доступа, а также реализацией
требований мандатной и ролевой политик безопасности в корпоративных сетях с
разными требованиями в отношении единого МАУ;
в разработке нового алгоритма управления безопасностью МАУ, отличающийся от известных определением оптимальной с точки зрения обеспечения конфиденциальности информации и качества предоставляемых пользователю
12
услуг программно-аппаратной конфигурации МАУ с учетом вероятности его
нахождения в специальных помещениях и других атрибутов доступа;
разработке системы управления безопасностью мобильных абонентских
устройств, отличающаяся возможностью удаленного управления программноаппаратной конфигурацией МАУ в зависимости от условий доступа, требований политик безопасности и качеству 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, 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 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-
13
стоположения МАУ, 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.

Структурно диссертационная работа [15]состоит из введения, четырех разделов,
заключения, библиографического списка, [6]включающего 150 источник, 2 приложений. Текст диссертации изложен на 234 страницах, включая 52 рисунка и 31
таблицу.
В первом [15]

разделе проведен анализ состояния научных исследований в области защиты информации при использовании МАУ. Рассмотрены существующие
формальные модели безопасности компьютерных систем, выделены их недостатки в случае их использования применительно к МАУ. Изучены отличительные особенности МАУ, влияющие на обеспечение безопасности информации. Выделены актуальные факторы, воздействующие на безопасность информации. На их основе разработана модель угроз информации в корпоративных сетях при доступе
к ней пользователей МАУ. Проведен анализ современных технических решений
по защите информации в МАУ. Проанализированы способы построения комплексных СЗИ при доступе к сетям с разными требованиями по защищенности.
Сформулирована задача диссертационного исследования.
Во втором разделе предложена модель безопасности МАУ, отличающаяся
от известных учетом его местонахождения в специальных помещениях, к которым предъявляются повышенные требования по ИБ. Показано, что основным параметром, вносящим неопределенность для определения условий предоставления
доступа МАУ, является его местоположение. Исследованы современные подходы,
используемые в технологиях определения местоположения пользователей МАУ в
14
помещениях внутри здания. В ходе исследований установлено, что для определения данного параметра необходимо использовать технологии определения местоположения пользователей МАУ в помещениях внутри здания с использованием
сигналов беспроводных сетей передачи данных (БСПД) в диапазонах частот 2,4-5
ГГц (стандарт 802.11). Для обоснования алгоритмической разрешимости задачи
определения местоположения и вычисления вероятности нахождения МАУ в специальном помещении на основе использования БСПД исследована эффективность технологий определения местоположения на основе методов трилатерации, к ближайших соседей и байесовского подхода (скрытой марковской модели).

Предложено использовать теорию машинного обучения и метод статистических испытаний (метод Монте-Карло) в качестве численного метода, позволяющего получить оценку вероятности нахождения МАУ в специальном помещении на основе
известной карты помещений корпоративной сети и предварительных исследований статистики ошибок определения местоположения. Осуществлена оценка качества предложенной модели. Приведены результаты моделирования с численным примером расчета.
В третьем разделе представлено описание разработанного алгоритма
управления безопасностью МАУ и входящих в его состав компонентов, включающих комплекс алгоритмов определения местоположения МАУ, в том числе, алгоритм вычисления вероятности нахождения МАУ в специальном помещении, а
также алгоритм формирования конфигурации МАУ в зависимости от текущих атрибутов доступа и действующей в корпоративной сети политики безопасности
МАУ и оценки информационной скорости передачи данных в БСПД. Осуществлена проверка основных свойств алгоритма. Получена оценка эффективности разработанного алгоритма.
В четвертом разделе описаны научно-технические предложения по практической реализации системы управления безопасностью МАУ в корпоративных
сетях. Разработаны рекомендации по формированию оптимальных параметров
системы определения местоположения. Проведено комплексное оценивание эффективности разработанных научно-технических предложений с расчетом показа-
15
телей эффективности системы управления безопасностью МАУ в корпоративных
сетях.
В заключении перечислены полученные научные и практические результаты, раскрыта степень их новизны и значение для теории и практики, а также
предложены перспективные направления дальнейших исследований, направленных на повышение вероятности обеспечения безопасности информации при эксплуатации МАУ в корпоративных сетях с разными требованиями по защищенности.
Апробация работы и ее

основных результатов, полученных в ходе работы,
была осуществлена на следующих конференциях:
6, 7-я [15] Межрегиональные научно-практические конференции "[68]Информационная безопасность и защита персональных данных: Проблемы и пути их решения" (г. [22]

Брянск, БГТУ, 2014, 2015, 2016 гг.) [39, 40, 42, 52];
12-е

Всероссийское совещание по проблемам управления ВСПУ-2014
(Москва, ИПУ им. В. А. Трапезникова РАН, 16-19 июня 2014 г.) [49];
Международной научно-технической конференции "Перспективные информационные технологии (ПИТ 2015)" (г. Самара, [19]

Самарский научный центр
РАН, 2015, 2016 гг.) [50, 53].
Публикации по теме диссертационной работы включают в себя 6 статей, в
том числе 5 статей в рецензируемых журналах, входящих в перечень

ВАК Минобрнауки России, 7 тезисов докладов, 6 свидетельств об официальной регистрации
программ для ЭВМ: № 2013612870 [15]

от 14.03.2013 г. "DNS-коммутатор" [74],
№ 2013615947 от 24.09.2013 г. "Автоматизированная система оценки вероятности
отказа в обслуживании запросов пользователей при построении сети как системы
массового обслуживания" [75], № 2013618388 от 06.09.2013 г. "Анализатор контекста доступа мобильного устройства" [76], № 2014617119 от 11.07.2014 г. "Автоматизированная система оценки параметров защищенности удаленного доступа
к услугам защищенной корпоративной сети пользователя мобильного
устройства" [77], № 2014617940 от 06.08.2014 г. "Автоматизированная система
мониторинга и управления информационной безопасностью сетевого трафика при
16
доступе к услугам информационных сервисов, использующих систему доменных
имен" [78], № 2015615631 "Автоматизированная система

определения местоположения пользователей мобильных устройств внутри здания на основе сигналов
беспроводной сети[19]

" [79], № 20166111210 "Программный агент удаленного управления функциональностью мобильного абонентского устройства" [80], 3 патента
на изобретения: № 2503059 от 27.12.2013 г. "Способ удаленного мониторинга и
управления информационной безопасностью сетевого взаимодействия на основе
использования системы доменных имен" [60], № 2530691 от 10.10.2014 г. "Способ
защищенного удаленного доступа к информационным ресурсам" [61], № 2546236
от 10.04.2015 г. "Способ анализа информационного потока и определения состояния защищенности сети на основе адаптивного прогнозирования и устройство для его осуществления" [62].
Акты внедрения научных результатов диссертационного исследования получены в Спецсвязи ФСО России, ФГУП "Государственный научноисследовательский институт прикладных проблем" ФСТЭК России.
17
1. АНАЛИЗ СОСТОЯНИЯ НАУЧНЫХ ИССЛЕДОВАНИЙ И
ТЕХНИЧЕСКИХ РЕШЕНИЙ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ
ПРИ ИСПОЛЬЗОВАНИИ МОБИЛЬНЫХ АБОНЕНТСКИХ УСТРОЙСТВ
В данном разделе проведен анализ условий функционирования и требований, предъявляемых к МАУ в корпоративных сетях, недостатков существующих
средств защиты информации и проблем, связанных с обеспечением безопасности
информации при работе с МАУ. Дана характеристика существующим формальным моделям безопасности компьютерных систем и системам контроля доступа, построенным на их основе. Выделены недостатки существующих формальных
моделей при использовании их в отношении современных МАУ. Исследованы
критические с точки зрения обеспечения безопасности информации особенности
современных МАУ. На основе анализа нормативно-правовых документов выделен перечень актуальных факторов, воздействующих на безопасность информации при эксплуатации МАУ, а также предложены модели угроз и нарушителя, отражающие состав угроз безопасности информации и возможности нарушителей безопасности при использовании МАУ в корпоративных сетях с разными требованиями по защищенности. Проведен анализ существующих защищенных МАУ, программных и программно-аппаратных мобильных технических решений, а также технических решений, позволяющих осуществлять доступ к сетям с разными требованиями по защищенности с использованием одного абонентского устройства. Описаны особенности эксплуатации МАУ в защищенных корпоративных сетях. Обоснована необходимость учета местоположения МАУ в корпоративной
сети для обеспечения эффективной работы СЗИ. Проведен анализ способов и технических решений по определению местоположения МАУ в помещениях внутри здания, представлена их классификация, выделены их достоинства и недостатки.
Обосновано использование БСПД для решения задачи вычисления вероятности
нахождения МАУ в специальных помещениях. Сформулирована научная задача
диссертационного исследования.

18

1.1. Условия функционирования и требования, предъявляемые к мобильным абонентским устройствам

В настоящее время использование современных МАУ в защищенных корпоративных сетях существенно ограниченно в связи с отсутствием эффективных СЗИ, гарантирующих обеспечение безопасности информации. Вместе с тем перспективным направлением совершенствования современных корпоративных сетей является обеспечение защищенного доступа абонентам к информации и услугам с разными требованиями по защищенности при использовании единого МАУ [10, 30, 58].

Современные корпоративные сети, в которых предусмотрено использовние МАУ, представляют собой аналоги структуры [30, 58], представленной на рисунке 1.1.

Рисунок 1.1 – Типовая структура корпоративных сетей с МАУ

19

При наличии в организации информации, требующей более высокого уровня защиты, внутри нее создаются несколько корпоративных сетей с разными требованиями по защищенности. Как правило, для получения доступа к ресурсам корпоративных сетей с разными требованиями по защищенности используются различные МАУ с необходимыми уровнями защищенности, что создается определенные неудобства. Для решения данной проблемы и обеспечения безопасности информации при работе на едином МАУ в настоящее время используется два подхода:

установка специализированных СЗИ (MDM-решения) [3, 30, 55, 58] на личные МАУ сотрудников организации в рамках концепции BYOD (Bring Your Own Device);

эксплуатация корпоративных защищенных МАУ [2, 35, 55, 83, 84, 85, 88].

Однако данные решения не обладают достаточной эффективностью с точки зрения защиты информации по различным причинам [3, 23, 25, 27, 41, 46]:

отсутствуют обоснованные формальные модели безопасности компьютерных систем, в которых предусмотрена эксплуатация МАУ и учитывается мобильность пользователей;

системы определения местоположения МАУ в помещениях на территории организации, как правило, строятся на основе БСПД стандарта 802.11 [43, 51] и обладают низкой точностью с ошибкой определения местоположения порядка 2 метров, что создается угрозу некорректного применения установленной в корпоративной сети политики безопасности МАУ;

существующие MDM-решения [55, 58, 146] и корпоративные защищенные МАУ [2, 35, 84, 85] не предполагают аппаратной переконфигурации МАУ, что является причиной наличия технических каналов утечки информации внутри устройства за пределы контролируемой зоны;

большинство современных МАУ построены на базе импортной электроники, которая не является доверенной [23], а существующие методики сертификации СЗИ не позволяют гарантировать отсутствие программных и аппаратных закладок.

20

Несмотря на наличие современных СЗИ, направленных на обеспечение безопасности информации при работе с МАУ, принципиальной проблемой является вопрос доверия к аппаратным платформам МАУ, которые реализуются, как правило, на базе импортной электроники и технологии SoC (System-on-Chip). Согласно исследованиям компании "Алладин Р. Д." [23] в большинстве современных МАУ используется архитектура ARM процессоров, в которых внедрена технология "TrustZone", разработанная английской компанией ARM. Сделано это для аппаратной изоляции (виртуализации) двух параллельных процессов – доверенного (безопасного) в рамках работы, так называемой ОС "Secure OS" и обычного (где работают приложения под управлением привычных операционных систем – Android, iOS, Linux, Tizen, Sailfish) – "RichOS" (гостевая ОС) [23]. Доверенные процессы в "TrustZone" обладают полным контролем над обычной ОС, включая полицейские функции и функции разведки. Приложения из "TrustZone" управляются доверенной операционной системой "Secure OS", которая внедряется в микросхему на этапе ее производства. При этом обычная ОС "RichOS", например, Android не имеет функциональных возможностей по определению наличия ОС "Secure OS". Данное исследование [23] также показало, что в более 95% современных процессорах с ARM-архитектурой внедрена технология "TrustZone", включая защищенные смартфоны типа "Коперник С1", Samsung Z3, YotaPhone, YotaPhone 2, а также сертифицированные ОС "Android 6.0 Marshmallow", ядро Astra Linux Special Edition 1.4 (релиз "Новороссийск" для ARM), ядро Linux 4.5.

Анализ нормативно-правовой базы и требований по обеспечению ИБ при использовании в защищенных корпоративных сетях [10, 18] 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 корпоративной политике ИБ в ЗКС;

21

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

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 [2, 27, 28, 35, 54, 55, 83, 84, 88] услуг представлен на рисунке 1.2.

Рисунок 1.2 – Сравнительный анализ количества услуг, предоставляемых МАУ

В связи с отсутствием эффективных СЗИ, позволяющих обеспечить безопасность информации, эксплуатация МАУ для доступа к перечню услуг, включающих в себя, как защищенные, так и незащищенные, в ЗКС существенно ограничена. Повысить вероятность обеспечения безопасности информации при доступе к услугам и ресурсам ЗКС предлагается за счет использования управляемого МАУ, взаимодействующего с системой управления безопасностью МАУ, позволяющей управлять программно-аппаратной конфигурацией МАУ в зависимости от условий его эксплуатации (атрибутов доступа). Структура и топология системы управления безопасностью МАУ в корпоративной сети в этом случае может выглядеть так, как показано на рисунке 1.3 [30, 58].

22

Рисунок 1.3 – Структура и топология системы управления безопасностью МАУ в корпоративной сети

Основным недостатком подобной архитектуры системы управления безопасностью МАУ является отсутствие формальной модели безопасности МАУ, учитывающей при этом местоположение МАУ в корпоративной сети, доказательства ее корректности, а также недостаточно эффективные существующие технологии по определению местоположения МАУ в помещениях внутри здания. Указанные факторы свидетельствуют об актуальности рассматриваемой проблемы и необходимости решения поставленной научной задачи.

1.2. Модели безопасности компьютерных систем, включающих в свой состав мобильные абонентские устройства

Для формального описания процесса обеспечения безопасности информации в компьютерных системах и обоснования ее защищенности используют формальные модели безопасности, на основе которых строятся различные механизмы

23

защиты информации, включая систему контроля доступа. Основной задачей системы

контроля доступа является предотвращение любой деятельности, которая
может привести к нарушению безопасности [44]

компьютерной системы [25, 135]. Эта
задача может решаться путем предотвращения

действий или операций, которые
могут выполнять в рамках системы [44]

пользователи или запущенные от имени пользователя процессы, а также путем ограничения доступных пользователю компьютерной системы действий.

Большинство современных систем управления доступом строится на основе
модели [44]

Лэмпсона, описанной в работах [122, 123] и представленной на
рисунке 1.4.
Источник запроса
Запрос на
выполнение
операции
Монитор обращений Объект
Источник Запрос Защита Ресурс
Рисунок 1.4 – Модель системы управления доступом Лэмпсона
В данной модели задача контроля доступа возлагается на монитор обращений, являющийся

посредником при каждой попытке источника запроса обратиться к ресурсам системы ([44]

объектам доступа).
В существующей теории компьютерной безопасности для описания элементов компьютерной системы (КС) используется ряд понятий, таких как "сущность", "объект", "субъект", "доступ", "контейнер" [5]. В зависимости от текущих
условий любая сущность КС может быть обозначена тем или иным понятием.

Для выполнения операций над сущностями КС субъекты осуществляют к
ним доступы. В большинстве случаев рассматриваются:
доступ на чтение из сущности;
доступ на запись в сущность;
доступ на запись в конец слова, описывающего состояние сущности;
24
[2]

доступ на активизацию (исполнение) субъекта из сущности.
Остальные виды доступов, как правило, могут быть реализованы с использованием рассмотренных [25].
Система контроля доступа в КС создается как средство защиты от угроз
безопасности информации. Согласно [26]

при классификации угроз выделяют три
основных свойства: [2]

конфиденциальность, целостность и доступность информации [18, 19, 72], которые и определяют три

классических угрозы безопасности
информации – угрозы конфиденциальности, целостности и доступности [41]

информации, а также еще одну – угрозу раскрытия параметров КС [25].
В соответствие с [19] управление доступом является одной из услуг защиты,
входящих в общую архитектуру защиты информации наряду с такими услугами
как аутентификация, конфиденциальность данных, целостность данных, безотказность. Для обеспечения тех или иных услуг защиты существуют специальные механизмы защиты [19], одним из которых является механизм управления доступом. В некоторых случаях для оказания ряда услуг защиты могут задействоваться несколько механизмов защиты.
В

КС доступ субъекта к сущности разрешается системой управления доступом при наличии у субъекта соответствующего права доступа к сущности. Способ
задания разрешенных прав доступа субъектов к сущностям КС регламентируется
реализуемой в КС политикой управления доступом, являющейся составной частью политики безопасности КС [72].
Известны следующие виды политик управления доступом, определяющих
способ задания разрешенных прав доступа субъекта к сущностям:
дискреционная политика управления доступом [111];
[2] мандатная (полномочная) политика управления доступом [106];
политика ролевого управления доступом [33, 139];
политика [9]безопасности информационных потоков [24];
[43] политика безопасности изолированной программной среды ([73]

ИПС) [97];
Формальные модели безопасности КС [25, с.25], описывающие порядок
функционирования той или иной политики управления доступом, используются
25
для обоснования защищенности современных и перспективных КС. Очевидно,
что технологическое развитие КС находится в постоянном движении и с появлением новых функциональных возможностей возникают и новые факторы, создающие угрозы безопасности информации, защита от которых в существующих
формальных моделях безопасности не предусмотрена. Поэтому каждая новая
формальная модель пытается учесть вновь возникающие факторы, приводящие к
появлению новых угроз безопасности информации. Классификация и взаимосвязь
ряда формальных моделей безопасности КС изображена на рисунке 1.5.
В настоящее время существуют и множество различных формальных моделей безопасности КС, ставящих перед собой цель с одной стороны осуществить
более полный учет всех факторов, достижение которой позволить сделать модель
безопасности КС более гибкой и адаптивной к условиям функционирования реальных КС, а с другой – использовать более совершенные механизмы управления доступом, упрощающие процедуры администрирования сложных КС.

К таким моделям безопасности КС можно отнести следующие:
политика безопасности на основе решеток – LBAC (Lattice-Based Access
Control) [136, 138];
политика безопасности на основе местоположения – LBAC (LocationBased Access Control) [102, 110, 118, 129, 133];
политика безопасности на основе контекста – CBAC (Context-Based Access Control) [100, 121, 141];
атрибутная политика безопасности – ABAC (Attribute-Based Access Control) [94, 115, 148].
Помимо влияния допущений на безопасность КС при ее разработке серьезное влияние оказывает и невозможность учесть все возможные условия функционирования КС в реальной среде и, соответственно, выполнение требований безопасности КС.
26
Модель ХРУ
Модель типизированной
матрицы доступов
Классическая модель Take-Grant
Расширенная модель TakeGrant
Базовая ДП-модель

ДП-модель с функционально
ассоциированными с субъектами
сущностями
ДП-модель для политики
безопасного администрирования
[2]

Субъектноориентированная модель
ИПС
ДП-модель с
функционально и пара
метрически
ассоциированными с
субъектами сущностями
ДП-модель файловых систем
Безопасность
информационных потоков
Программная модель
Автоматная модель
Вероятностная модель
Классическая модель
Белла-ЛаПадулы
Модель Биба ОСМ ДП-модель
ПСМ ДП-модель
Ролевое управление
доступом
Модель ролевого
администрирования
Дискреционное
управление доступом
Мандатно-

ролевая модель
Мандатная сущностно ролевая ДП-модель
Базовая ролевая модель
[9]

Управление доступом на основе атрибутов

Управление доступом на основе местоположения
Управление доступом на основе контекста
[44]

Формальные модели безопасности
Изолированная
программная среда (ИПС)

ДП-модель для политики абсолютного
разделения административных и
пользовательских полномочий
[2]

Мандатная
ДП-модель
Модель системы военных сообщений
Модель безопасности переходов
БДМ ДП-модель
БК ДП-

модель
Мандатное управление
доступом
БД ДП-модель
[9]

Рисунок 1.5 – Классификация и взаимосвязь отдельных формальных моделей
безопасности КС
С точки зрения реализации формальных моделей безопасности для управления доступом пользователей МАУ возникает объективная потребность учитывать местоположение как фактор, влияющий на состояние безопасности информации в КС. В работах [102, 110, 118, 129, 133] приведено описание формальных
27

моделей безопасности КС, учитывающих местоположение пользователей и
устройств. Однако при более детальном рассмотрении проблемы учета местоположения в данных моделях отчетливо виден ряд недостатков, серьезно влияющих на адекватность модели реальным КС и безопасность функционирования таких
систем. К данным недостаткам относятся следующие:
вопрос непосредственного определения местоположения как координат
пользователей и устройств либо помещений, в которых находятся пользователи,
выносится за рамки рассмотрения данных работ;
не учитывается ошибка определения местоположения устройств, возникающая вследствие несовершенства современных способов определения местоположения МАУ, как на открытой местности, так и в помещениях внутри здания;
не рассматривается вопрос оценки требований безопасности к устройствам, в зависимости от их местоположения и уровня требования по защищенности специальных помещений, в которых они находятся, а также уровня конфиденциальности информации и услуг, к которым запрашивается доступ;
в качестве СЗИ в КС не используются возможности интеллектуального
блокирования МАУ или их отдельных функциональных блоков, представляющих
в определенных условиях доступа угрозу информационной безопасности в ЗКС.
Вывод: наличие указанных недостатков свидетельствует о том, что существующие модели безопасности КС, учитывающие такой фактор как местоположение устройств и пользователей, требуют серьезной доработки, поскольку не являются адекватными реальным КС и не гарантируют безопасность информации
при использовании МАУ.

1.3. Модели угроз и нарушителя информационной безопасности при
эксплуатации мобильных абонентских устройств и анализ технических решений
для защиты от них

1.3.1. Характеристика и особенности современных мобильных абонентских
устройств

28

Современные МАУ, обладающие и вычислительными и коммуникационными ресурсами, представляют собой многофункциональное медиаустройство, в котором функция телефонных переговоров не является первостепенно важной [93]. Для улучшения показателя экономичности основные узлы современных МАУ агрегированы в составе микросхемы класса SoC (System-on-Chip – системе
на чипе), на которую возлагается весь перечень задач сбора, обработки, хранения
и обмена пользовательской и служебной информацией [28]. Такая SoC зачастую
объединяет на одном кристалле несколько ядер процессора, коммуникационный
процессор, графический сопроцессор и др. Добавление при необходимости микроконтроллеров для кодирования речи, высокочастотных блоков для работы в различных стандартах сети сотовой связи, интерфейсных блоков Wi-Fi или иной
беспроводной сети, модулей GPS/ГЛОНАСС/Galileo/Beidou, а также набор интерфейсов для взаимодействия с различными типами устройств (USB, SD, MMC, UART и др.) обеспечивает конфигурирование МАУ для решения различных задач
и требований пользователей и обеспечивает многофункциональность современных МАУ.
При эксплуатации МАУ существует ряд важных особенностей, оказывающих существенное влияние на состояние защищенности информационного взаимодействия в рамках работы в ЗКС [49]. К ним относятся:
1. Миниатюрность МАУ. Данное свойство МАУ приводит к ограничению
возможностей интерфейса взаимодействия с пользователем, влияет на вычислительные и функциональные возможности, повышает риск утраты МАУ и, соответственно, использование его неавторизованным пользователем.
2. Мобильность. Данное свойство МАУ позволяет использовать функциональные возможности МАУ независимо от местоположения пользователя, однако в сочетании с миниатюрностью позволяет незаметно осуществить пронос и использование МАУ внутри помещений с повышенными требованиями по защищенности.
3. Ограниченность вычислительных ресурсов МАУ. Данный фактор оказывает влияние на выполняемые в МАУ вычислительные процессы. Поскольку про-

29

цессы, отвечающие за функции защиты информации (ЗИ), как правило, должны
выполняться в фоновом режиме и постоянно задействовать определенную часть
вычислительных ресурсов, то в условиях ограниченности этих ресурсов в МАУ
возникают и ограничения на функциональность и возможности таких процессов.
4. Мультифункциональность МАУ. К современным функциям МАУ можно
отнести:
использование МАУ в виде фото- и видеокамеры;
использование МАУ как навигационного устройства;
использование МАУ в качестве модема;
использование МАУ в качестве переносной точки доступа;
использование МАУ в качестве диктофона;
использование МАУ в качестве съемного носителя информации.
5. Доступ к услугам корпоративной сети на основе использования принципа
однократного входа SSO ("Single Sign-On"). Данная особенность является следствием миниатюрности МАУ и сложности человеко-машинного взаимодействия, характерного для МАУ. В сочетании с мобильностью и миниатюрностью МАУ
использование режима SSO приводит к увеличению рисков использования МАУ
неавторизованным пользователем.
6. Доступ к информационным ресурсам сетей с разными требованиями по
защищенности. Использование МАУ для доступа к сетям с разными требованиями по защищенности в настоящее время ограничено, поскольку не существует эффективных СЗИ, обеспечивающих безопасность информации. Существующие
подходы по ЗИ, используемые в стационарных СВТ, не применимы в полной мере
к МАУ из-за ограниченности их вычислительных ресурсов, а также особенностей
их программно-аппаратной архитектуры.
Указанные особенности увеличивают вероятность осуществления угроз ИБ
при работе с МАУ в условиях ЗКС, поэтому необходимо учитывать факторы,
влияющие на безопасность информации.
Существенное значение при разработке СЗИ для МАУ имеют вопросы их
конфигурирования с учетом показателей ресурсопотребления [27], предусматри-

30

вающие выбор и разработку СЗИ путем комбинирования отдельных компонентов
защиты с учетом их свойств, ограничений и требований к ним со стороны МАУ.

1.3.2. Актуальные факторы, воздействующие на безопасность информации
при использовании мобильных абонентских устройств

На основе ГОСТ Р 51275-2006 [16] и с учетом того, что эксплуатация МАУ
предполагается в сетях с разными требованиями по защищенности, а также учитывая указанные отличительные особенности МАУ по сравнению со стационарными СВТ, были выделены актуальные факторы, воздействующие на безопасность информации при использовании МАУ в ЗКС. Перечень указанных факторов представлен в таблице 1.1.
Анализ представленных факторов позволяет сделать следующие выводы:
1) значительная доля факторов, влияющих на ИБ при работе с МАУ, является субъективной, т.е. зависящей от пользователей;
2) большая часть выделенных объективных внутренних факторов, воздействующих на безопасность информации, является следствием наличия в составе

МАУ функциональных блоков (модулей), создающих технические каналы утечки
информации при их использовании внутри или вблизи специальных помещений
ЗКС, а также при незащищенном доступе к конфиденциальной информации.
Проведенный анализ актуальных факторов, влияющих на безопасность информации при работе с МАУ, позволяет сформировать перечень угроз безопасности информации, а также модель нарушителя при эксплуатации МАУ в ЗКС.
31
Таблица 1.1 – Актуальные факторы, воздействующие на безопасность информации при эксплуатации МАУ
1. Объективные факторы 2. Субъективные факторы
1.1. Внутренние факторы 2.1. Внутренние факторы 2.2. Внешние факторы
1.1.1.

Передача сигналов
в) в диапазоне радиоволн и в оптическом диапазоне длин волн ([34]

при
передаче информационного сигнала с использованием модулей беспроводной связи Bluetooth, Wi-Fi,
GSM, UMTS, LTE и т.п.;)
1.1.2.

Излучения сигналов, функционально присущие техническим
средствам (ТС) объекта информатизации:
а) излучения акустических сигналов сопутствующие [23]

произносимой
или воспроизводимой ТС речи
(при функционировании динамика
МАУ как в режиме телефона, так и
в режиме громкой связи);
б) электромагнитные излучения и
поля (в радиодиапазоне при передаче информации с использованием модулей Bluetooth, WiFi (802.11), GSM (2G), UMTS (3G),
LTE (4G) и т.п.);
1.1.6

Наличие акустоэлектрических преобразователей в элементах
ТС.
1.1.7. Дефекты, сбои и отказы, аварии ТС и систем.
1.1.8. Дефекты, сбои и отказы программного обеспечения ([23] ПО)
2.1.1. Разглашение защищаемой информации имеющими к ней
право доступа через
б) передачу информации по открытым линиям связи;
в) обработку информации на незащищенных [17]ТС обработки [23]информации;
д) копирование информации на незарегистрированный носитель
информации;
ж) утрату носителя информации;
2.1.2. Неправомерные действия со стороны лиц, имеющих право
доступа к защищаемой информации, путем:
а) несанкционированное изменение информации;
б) несанкционированное копирование защищаемой информации;
2.1.3. Несанкционированный доступ к информации путем:
а) подключения к техническим средствам и системам объекта информатизации;
б) использования закладочных средств ([17]устройств);
в) [23]использования программного обеспечения технических средств
[17]объекта [24]информатизации [37]через
1) маскировку под зарегистрированного пользователя;
2) дефекты и уязвимости ПО объекта информатизации;
3) внесение программных закладок;
4) применение вирусов или другого вредоносного программного
кода ([17]троянские программы, клавиатурные шпионы, активное
содержимое документов);
г) хищения носителя защищаемой информации;
д) нарушения функционирования ТС обработки информации;
2.1.5. Ошибки, обслуживающего персонала объекта информатизации при
а) эксплуатации ТС;
б) [23]эксплуатации программных средств;
в) эксплуатации средств и систем защиты информации;
2.2.2. Несанкционированный доступ к защищаемой информации путем:
а) подключения к техническим средствам и
системам объекта информатизации;
б) использования закладочных
средств ([17]устройств);
в) использования [23]

ПО технических средств
объекта информатизации

через:
1) маскировку под зарегистрированного пользователя;
2) дефекты и уязвимости ПО объекта информатизации;
3) внесение программных закладок;
4) применение вирусов или другого вредоносного программного кода ([17]троянские программы, клавиатурные шпионы, активное содержимое документов);

г) [23]несанкционированного физического доступа
к объекту информатизации;
д) хищения носителя информации;
2.2.3. Блокирование доступа к защищаемой
информации путем перегрузки технических
средств обработки информации ложными заявками [17]на ее обработку;
2.2.5. [23]Искажения, уничтожение или блокирование информации с применением технических средств путем:
в) использования программных или программно-аппаратных средств при осуществлении:
1) компьютерной атаки;
2) сетевой атаки.
32
1.3.3. [17]

Модель угроз и нарушителя безопасности при использовании мобильных абонентских устройств в корпоративных сетях с разными требованиями по защищенности
Совокупность перечисленных актуальных факторов, воздействующих на
безопасность информации при эксплуатации МАУ, позволяет сформировать модель угроз информации в ЗКС при доступе к ней пользователей МАУ. В ряде случаев информационный доступ может быть подвержен угрозам ИБ, возникающим
вследствие использования сторонних приложений, а также устройств, взаимодействующих с МАУ в рамках информационного взаимодействия внутри ЗКС. В работах [44, 48, 75] приводится описание модели доступа к информационным сервисам, при которой возможна реализация атаки типа "отказ в обслуживании" в связи с наличием подобных сторонних приложений и информационного взаимодействия с ними, методика расчета оценки защищенности такой системы, а также методики обнаружения и противодействия данному виду атак.
При разработке модели угроз необходимо учитывать особенности МАУ, отличающие их от стационарных СВТ, а также принципы обеспечения ИБ в ЗКС с использованием МАУ [3]:
1. Принцип отсутствия доверия к импортной электронике на базе SoC, а
также архитектуры наиболее распространенных процессоров с ARMархитектурой с аппаратной виртуализацией основной ОС (например, Android) и закрытой доверенной ("Trusted OS"). Средствами защиты может выступать собственная доверенная ОС с доверенным начальным загрузчиком (аппаратнопрограммным модулем доверенной загрузки) для процессоров с ARMархитектурой с контролем отсутствия скрытых аппаратных не декларируемых возможностей.
2. Принцип ненадежности МАУ. Требует наличия СЗИ, позволяющих гарантировать требуемый уровень защиты информации в ЗКС при условии отсутствия доверия к МАУ. Средствами защиты могут выступать:
33
запрет или ограничение на использование личных МАУ;
запуск корпоративных приложений в изолированных контейнерах;
использование приложений, отслеживающих состояние МАУ;
использование доверенной программно-аппаратной среды.
3. Принцип небезопасности беспроводных соединений, используемых
МАУ. Требует наличия СЗИ, позволяющих гарантировать аутентичность сторон,
участвующих в беспроводном сетевом взаимодействии, а также защищенность
передаваемых данных. Средствами защиты могут выступать:
применение шифрования при передаче данных;
использование взаимной аутентификации на основе криптографических
алгоритмов.
4. Принцип небезопасности сторонних приложений. Предполагается, что
любые внешние приложения небезопасны и создают каналы утечки защищаемой
информации с МАУ и из ЗКС. Требует наличия СЗИ, обеспечивающих доверенность используемых в МАУ приложений, а также отсутствие каналов утечки информации, возникающих в процессе запуска установленных в МАУ приложений.
Средствами защиты могут выступать:
изолированная программная среда (ИПС);
безопасный изолированный контейнер для корпоративных приложений
(например, средства программной или аппаратной виртуализации);
терминальный доступ к приложениям, расположенным на удаленном защищенном корпоративном сервере;
доверенные гипервизоры для запуска приложений в изолированной защищенной оболочке.
5. Принцип небезопасности устройств, взаимодействующих с МАУ. Современное МАУ является многофункциональным медиаустройством с различными коммуникационными функциями, способное взаимодействовать с большим количеством разнообразных устройств и носителей информации. Обеспечение требуемой защищенности подразумевает гарантированность того, что все подключае-
34
мые и взаимодействующие с МАУ устройства безопасны и являются доверенными. Средствами защиты могут быть:
средства контроля подключаемых к МАУ устройств;
средства контроля состояния и функциональных возможностей отдельных
модулей МАУ;
средства контроля передаваемых данных в процессе взаимодействия МАУ
с другими устройствами.
С учетом данных принципов, а также на основе исследований [10, 81, 90] и
проведенного анализа факторов, воздействующих на безопасности информации
при эксплуатации МАУ, выделены актуальные угрозы ИБ. Угрозы ИБ при эксплуатации МАУ представлены в виде:
<угроза> := <

источник угрозы>, <уязвимость>, <способ реализации угрозы>,<объект воздействия (программа, протокол, данные и т.д.>,<[11]

деструктивное
воздействие>.
Описательная модель угроз и нарушителя ИБ при эксплуатации МАУ с учетом указанного представления изображена на рисунке 1.6.
35

Источник угрозы
Нарушитель
Внешний
[33]Лица, имеющие санкционированный доступ в ЗКС,
но не имеющие доступа к [8]

защищаемой информации
(ЗИ)
Зарегистрированный пользователь, имеющий

ограниченные права доступа к ЗИ на МАУ
Пользователи, осуществляющие удаленный доступ к ЗИ по ЗКС посредством МАУ

Зарегистрированный пользователь с полномочиями администратора безопасности
Программисты-разработчики прикладного ПО и лица, обеспечивающие его сопровождение
Разработчики и лица, обеспечивающие поставку, сопровождение
Другие категории лиц в соответствии с оргштатной структурой организации
Программно-аппаратная закладка
Конструктивно встроенная
Автономная
Вредоносная программа
Программные закладки
Программные вирусы
Вредоносные программы, распространяющиеся по сети (черви)
[8]Другие [11]вредоносные программы
Уязвимости
[8]Уязвимости ПО
[11]Уязвимости микропрограмм, прошивок
Уязвимости драйверов аппаратных средств
Уязвимости операционных систем (ОС)
в процессе инициализации ОС
в незащищенном режиме работы процессора
в [8]процессе функционирования ОС в привилегированном режиме
[11]Уязвимости прикладного ПО
Уязвимости специального ПО
Уязвимости ПО пользователя
Уязвимости, вызванные наличием программноаппаратных закладок
Уязвимости, связанные с реализацией протоколов сетевого взаимодействия и каналов передачи данных
Уязвимости, вызванные недостатками организации [8] защиты информации от НСД
[11]Уязвимости СЗИ
Уязвимости программно-аппаратных средств в результате сбоев в работе, отказов этих средств
Наличие технических каналов утечки информации
Внутренний
Способ реализации угрозы
Использование существующих уязвимостей программно-аппаратного обеспечения, [8]позволяющих:
[11]Обходить СЗИ
Деструктивно воздействовать на СЗИ
Вскрывать или перехватывать пароли
Использовать [8]уязвимости [11]протоколов сетевого взаимодействия и каналов передачи данных, позволяющие:
Перехватывать информацию
Модифицировать передаваемые данные
Перегружать ресурсы (отказ в обслуживании)
Внедрять вредоносные программы
Получать удаленный НСД к системе
Разглашать и организовывать утечку информации на незащищенные рабочие места
Использовать остаточную неучтенную информацию
Использовать нетрадиционные (стеганографические) каналы [8]передачи информации
[11]Внедрение (внесение) новых уязвимостей на этапе проектирования, разработки и сопровождения
Использование нештатного ПО

Внесение уязвимостей с
использованием штатных средств
Обмен программами и данными,
[8]содержащими выполняемые модули
[11]Изменение конфигурации ПО
Модификация ПО и данных
Разработка вредоносных программ
Публикация, разглашение ЗИ
Объект воздействия
Информация, обрабатываемая на МАУ
(узле), находящаяся:
На отчуждаемых носителях
информации
На накопителях электронной памяти
типа флеш
На встроенных носителях
долговременного хранения [8] информации
В ПЗУ
В [12]перепрограммируемых
(перезаписываемых) запоминающих
устройствах
В средствах обработки и хранения
оперативной памяти
В оперативной памяти
В кеш-памяти, в буферах ввода/
вывода
В видео-памяти
В оперативной памяти
[8]подключаемых устройств
[11]Информация в средствах, реализующих
сетевое взаимодействие, и в каналах
передачи данных в сети
В маршрутизаторах
В [8]

точках доступа беспроводной сети
В каналах беспроводной сети
В устройствах коммутации
Деструктивное воздействие

Нарушение конфиденциальности
[11]Утечка информации
Несанкционированное копирование
Перехват информации в каналах
передачи данных
Разглашение (публикация) защищаемой
информации
Нарушение целостности (уничтожение,
модификация, дезинформация)
Воздействие на [8]ПО и данные
пользователя
[11]Воздействие на микропрограммы,
данные и драйверы МАУ
Воздействие на микропрограммы,
данные и драйверы устройств,
обеспечивающих загрузку ОС МАУ и
СЗИ и их функционирование
Воздействие на программы и данные
прикладного и специального ПО
[8]Внедрение вредоносной программы,
[11]программно-аппаратной закладки
Воздействие на средства управления
конфигурацией сети
Воздействие на средства управления
конфигурацией МАУ
Воздействие на СЗИ
Нарушение доступности
[8]Нарушение функционирования и
[11]отказы средств обработки информации,
средств ввода/вывода, [8]

хранения
информации, функциональных модулей
МАУ и каналов передачи данных
Нарушение и отказы в
функционировании СЗИ
Информация, обрабатываемая в
защищаемых помещениях охраняемых

объектов
Рисунок 1.6 – Описательная модель угроз и модель нарушителя ИБ при эксплуатации МАУ в ЗКС
36
Основным источником угроз ИБ, рассматриваемым в данной работе, является внутренний нарушитель, поскольку для эффективной защиты от других источников пригодны имеющиеся СЗИ:
1) для защиты от внешнего нарушителя – комплекс организационнотехнических мер по выполнению требований ИБ в ЗКС;
2) для защиты от программно-аппаратных закладок и вредоносных программ – комплекс мер по лицензированию и сертификации МАУ, а также применение изолированной программной среды в составе системного ПО МАУ, доверенной ОС и АПМДЗ.
Основными уязвимостями являются:
уязвимости, связанные с недостатками организации ЗИ от НСД;
наличие технических каналов утечки информации (ТКУИ) [91, 92] в МАУ
в условиях эксплуатации МАУ в запрещенных режимах работы.
В связи с необходимостью использования единого МАУ для доступа к корпоративным сетям с разными требованиями по защищенности принципиальной задачей является создания условий для такого управления программноаппаратной конфигурацией МАУ, при котором будет исключено наличие ТКУИ при доступе с использованием единого МАУ к ресурсам корпоративных сетей с
разными требованиями по защищенности. Типовая схема ТКУИ в МАУ представлена на рисунке 1.7.
37
Источник
сигнала
Техническое
средство
перехвата
информации
Помехи
Среда
распространения
сигнала
Модуль МАУ
Информационный
сигнал
Граница
контролируемой
зоны объекта
(помещения)
- радиоинтерфейсы
- экран (излучение оптического сигнала)
- микрофон и динамик (излучение акустических сигналов)
- запоминающие устройства
- проводные линии связи (питание, USB и др. интерфейсы)
- воздушная среда
- линии электропитания и заземления
- посторонние проводники
- соединительные линии
Рисунок 1.7 – Схема технического канала утечки информации, обрабатываемого
средствами вычислительной техники
Одним из эффективных средств предотвращения утечки информации по
ТКУИ может быть система управления программно-аппаратной конфигурацией
МАУ, позволяющая отключать модули МАУ (например, микрофон, радиоинтерфейс, запоминающие устройства), создающие информационные источники сигнала, в зависимости от условий (атрибутов доступа), в которых находится МАУ и к
которым можно отнести, в том числе, местоположение. При отсутствии такой системы внутренний нарушитель имеет техническую возможность использовать МАУ как средство связи независимо от условий доступа и своего местоположения в организации. Например, в случае несанкционированного или случайного проноса МАУ в специальное помещение, в котором запрещена обработка открытой информации и использование МАУ, данное устройство становится источником информационных сигналов, с��держащих конфиденциальную информацию.
Схема утечки информации представлена на рисунке 1.8.
38
Специальное помещение
Незащищенный
радиоканал связи
МАУ
ПЗУ
Запись конфиденциальной
информации на ПЗУ с
использованием
(микрофона, видеокамеры
и других устройств ввода/
вывода)
Источник сигнала
(конфиденциальной
информации)
Среда
распространения
сигнала
Интерф. вв/выв
Рисунок 1.8 – Схема утечки информации при несанкционированном
использовании МАУ в специальном помещении
В настоящее время существует ряд СЗИ в виде MDM-решений, позволяющих блокировать работу МАУ в запрещенных режимах. Данные решения не предполагают аппаратной переконфигурации устройства и работают на уровне
приложений, что является существенным недостаткам с учетом принципов отсутствия доверия к импортной электроники, ненадежности МАУ и отсутствия доверия к сторонним приложениям.
Контроль вноса незащищенных МАУ осуществляется, как правило, организационно-техническими мерами, которые сравнительно легко преодолеваются
при отсутствии эффективного контроля выполнения данных мер.
Таким образом, существует объективная потребность в разработке таких
СЗИ, которые позволят в автоматическом режиме управлять не только программной, но и аппаратной конфигурацией МАУ, блокируя возможные каналы утечки

информации при использовании устройства в организациях, в которых предусмотрена обработка конфиденциальной информации, независимо от местоположения МАУ на территории данной организации.
39
Разрабатываемая система управления безопасностью МАУ направлена в
первую очередь на защиту от угроз, связанных с:
обходом СЗИ;
деструктивными воздействиями на СЗИ;
перехватом и модификации передаваемой информации;
разглашением и организации утечки информации в незащищенных местах
доступа;

использованием нештатного ПО;
внесением уязвимостей с использованием штатных средств.
[8]

Основными объектами защиты информации при реализации разрабатываемой СЗИ является:
информация, обрабатываемая МАУ;

информация в средствах, реализующих сетевое взаимодействие, а также в
каналах передачи данных в сети;
[8]

информация, обрабатываемая в специальных помещениях ЗКС.
Указанные описательные модели угроз и нарушителя ИБ при использовании МАУ позволяют более детально сформировать требования к разрабатываемой системе управления безопасностью МАУ и реализуемых СЗИ для обеспечения безопасности информации в корпоративных сетях с разными требованиями
по защищенности.
1.3.4. Технические решения для защиты информации при эксплуатации мобильных абонентских устройств
В настоящее время для защиты информации при эксплуатации МАУ в ЗКС
разработано достаточно большое количество программных, программноаппаратных решений, выполняющих функции СЗИ. Среди ПО для защиты информации в МАУ и управления доступом к услугам ЗКС известны такие продукты, как программные комплексы "ViPNet Client" [146], CISCO для управления до-
40
ступом Cisco Unified Access, Cisco Identity Services Engine [58], Cisco Secure
ACS [30], "MobileIron", "Kaspersky Security 10" для мобильных устройств,
"McAfee Enterprise Mobility Management", "Afaria", "SOTI Mobicontrol", "AirWatch
MDM", "Samsung Enterprise Access Layer", "Juniper Junos Pulse MSS".
Данные решения представляют собой реализации технологии MDM (Mobile
Device Management – управление МАУ), MAM (Mobile Application Management –
управление корпоративными приложениями на МАУ) и MIM (Mobile Information
Management – управление корпоративными документами с использованием
МАУ), представляющие собой элементы комплексного ПО для работы с корпоративными системами при помощи МАУ, обеспечивающее безопасность, контроль и поддержку МАУ, используемых персоналом компаний. Как видно из названия
технологии, управление МАУ осуществляется на уровне приложений и доступов
к документам.
Существенным недостатком данных решений является использование только лишь программного управления МАУ, что не позволяет в полной мере гарантировать безопасность информации при доступе к защищенным услугам, а также
отсутствие математически доказанного корректного формального аппарата моделирования безопасности МАУ в ЗКС.
К аппаратным и программно-аппаратным защищенным техническим решениям в настоящее время относятся [47]:
защищенные мобильные телефоны;
технические средства защищенного терминального доступа;
защищенные планшетные компьютеры;
защищенные мобильные компьютеры.
В настоящее время известны следующие решения в области защищенных
мобильных телефонов:
1. Защищённый телефон стандарта GSM "Талисман 395" [88].
2. Специализированный терминал мобильной связи "Сапфир-К" [83].
3. Специальный сотовый телефон "SMP-АТЛАС/2" [85].
4. Аппаратура шифрования речевых сообщений "Аппаратура 605" [2].
41
5. Специальный микросотовый телефон "М-549М" [84].
К известным техническим средствам защищенного терминального доступа
можно отнести:
1. Терминальный клиент "ViPNet Terminal" [147].
2. Терминальный клиент "КАМИ-Терминал" [32].
3. Терминальный клиент "HELIOS ProfyShield LT-A330–1s" [113].
Известен защищенный планшетный компьютер "Континент Т-10" [35], сертифицированный ФСТЭК и ФСБ, а также ряд таких защищенных мобильных компьютеров как:
1. Мобильное защищенное автоматизированное рабочее место доступа в
сеть Интернет "МАРМ ДСИ" [54].
2. Мобильный вычислительный комплекс "ИНФОПРО" МВК-2 [55].
Большинство представленных технических решений позволяют обеспечивать защищенный доступ к конфиденциальной информации. Некоторые обеспечивают защищенный доступ к сведениям, содержащим информацию, отнесенную
к государственной тайне. Однако на данный момент отсутствуют технические
решения, позволяющие обеспечивать доступ к сетям с разными требованиями по
защищенности с использованием одного МАУ. Другим недостатком является то,
что не существуют эффективных СЗИ, учитывающих местоположение МАУ.
Данные недостатки СЗИ в настоящее время устраняются путем применения организационных мер в отношении МАУ и их пользователей, включающих в себя, в том числе, запрет на пронос личных МАУ и их использования в ЗКС.
Существует ряд технических решений от иностранных производителей, таких как у компании CISCO [30, 58], позволяющих обеспечивать управление доступом пользователей МАУ в зависимости от их местоположения в ЗКС. Однако
в данных решениях местоположение определяется лишь точкой подключения к
БСПД ЗКС, при этом уровень конфиденциальности доступа определяется уровнем конфиденциальности точки доступа, а не реальным местоположением пользователя МАУ.
42
Одним из наиболее существенных недостатков современных защищенных

МАУ является ограниченный перечень предоставляемых услуг. Отсутствие возможности совмещать функциональность современных смартфонов и защищенных технических мобильных решений, которые допустимо использовать в ЗКС при
условии выполнения требований ИБ, сказывается на доступности и своевременности предоставления абонентам услуг. Это связано с отсутствием эффективных СЗИ, позволяющих гарантировано исключить работу МАУ в небезопасных режимах (конфигурациях), а также обеспечить отсутствие технических каналов утечки информации в период нахождения пользователя МАУ в зоне доступа ЗКС.
Таким образом, на основе проведенного анализа существующих защищенных технических мобильных решений выделены следующие недостатки:
отсутствие СЗИ, позволяющих обеспечить безопасный доступ к сетям с
разными требованиями по защищенности с использованием одного устройства;
отсутствие технических решений, позволяющих определять местоположение МАУ и учитывать требования ИБ к МАУ, предъявляемые к СВТ в данном местоположении в ЗКС;
ограниченное количество предоставляемых пользователям МАУ услуг в
защищенных мобильных решениях.
1.4. Способы построения комплексной системы защиты информации при
доступе к сетям с разными требованиями по защищенности
Для защиты информации, обрабатываемой в ЗКС, применяются СЗИ, параметры которых определяются политикой безопасности данной ЗКС на основании уровня конфиденциальности обрабатываемой информации и соответствующими
нормативно-правовыми актами [56, 59]. При обеспечении доступа МАУ к конфиденциальной информации и сетям с разными требованиями по защищенности в настоящее время применяется схема, представленная на рисунке 1.9 [35].
43
Конфиденциальная информация
Открытая
информация
Личные МАУ
Служ. МАУ/Личные МАУ
с MDM-решением
Предоставляемые пользователю услуги
а)
б) в)
г) д)
Рисунок 1.9 – Схема доступа в ЗКС к информации с разным уровнем
защищенности при использовании МАУ: а) обобщенная;
б-д) варианты подключения на примере защищенного планшета "Континент Т-10"
Порядок и режим доступа к конфиденциальной информации с использованием указанной схемы определяется, в том числе, и комплексом организационных и организационно-технических мер по ЗИ в ЗКС.
44
Как видно из рисунка 1.9 в настоящее время могут применяться несколько
МАУ для работы в сетях с разными требованиями по защищенности. Однако в
ряде случаев необходимо сопряжение данных сетей (контуров обработки информации с разными требованиями по защищенности). При этом выполнение требований по ИБ должно соответствовать уровню защиты, предъявляемому к контуру
с более высокими требованиями по защищенности.
В настоящее время известны несколько подходов для сопряжения контуров
обработки информации с разными требованиями по защищенности. К ним относятся:
1. Технологии однонаправленных шлюзов. Гарантируют передачу информации в одном направлении. В настоящее время известны такие технические решения как однонаправленный шлюз "Атликс-Шлюз-К" [57], система однонаправленной передачи данных "ДИОД" [82] и другие.
2. Технологии виртуализации. Использование доверенных гипервизоров,
позволяющих в одном корпусе объединить несколько защищенных программноаппаратных контейнеров, в которых допустимо обрабатывать информацию с разными требованиями по защищенности.
3. Технологическое объединение в едином корпусе программно-аппаратных
платформ, выполненное с использованием оптоэлектронной, трансформаторной
развязки, позволяющее разделить и изолировать тракты прохождения информации с разным требованиями по защищенности друг от друга.
4. Терминальный доступ. Реализация технологий тонкого клиента с использованием серверов приложений.
С точки зрения реализации сопряжения контуров обработки информации с
разными требованиями по защищенности при эксплуатации МАУ технологии однонаправленных шлюзов применимы лишь как вспомогательные средства. Технологии виртуализации требуют серьезных вычислительных ресурсов, которыми
обладают только планшетные и мобильные компьютеры и достаточно ограниченно – смартфоны.
45
Технологическое объединение в едином корпусе программно-аппаратных
платформ, позволяющее разделить и изолировать тракты прохождения информации, к которым предъявляются разные требования по защищенности, друг от друга, в настоящее время реализовано только лишь для стационарных вычислительных систем. В то же время данное направление является перспективным для
МАУ, поскольку технический уровень в настоящее время позволяет объединять в
едином корпусе многопроцессорные системы, в том числе и в МАУ.
Терминальный доступ является наиболее оптимальным средством при доступе к информации с разными требованиями по защищенности. Однако реализация данных технологий не позволяет осуществлять управление функциональностью МАУ, исключая его работу и работу отдельных функциональных модулей
МАУ в запрещенных режимах, а также не решает задачи определения местоположения МАУ.
Таким образом, для устранения проблемы реализации сопряжения контуров
обработки информации с разными требованиями по защищенности в МАУ необходимо решение следующих задач:
1) разработка формальной модели безопасности МАУ, учитывающей программно-аппаратную конфигурацию МАУ и его местоположение;
2) разработка системы определения местоположения МАУ, позволяющей с
требуемой достоверностью определять местонахождения МАУ в специальных
помещениях ЗКС в режиме реального времени;
3) разработка системы управления безопасностью (программно-аппаратной
конфигурации) МАУ в зависимости от его местоположения и других атрибутов
доступа, а также требований по качеству предоставляемых услуг;
4) разработка технических предложений по реализации системы управления
безопасностью МАУ, позволяющей функционировать данному устройству в сетях
с разными требованиями по защищенности, с учетом местоположения МАУ и
иных атрибутов доступа.
Решение данных задач возможно с помощью применения агентноориентированного подхода [34, 98, 114], являющегося элементом искусственного
46
интеллекта и построенного на основе классической клиент-серверной архитектуры. Обобщенная схема доступа в этом случае может иметь вид, представленный на рисунке 1.10.
Конфиденциальная информация
Контроллер доступа

мобильных абонентских устройств
Система
определения
местоположения
МАУ
Мобильное абонентское устройство
Конф. № 0
Открытая
инфомация
Конф. № 3 Конф. № 1 Конф. № 2
Предоставляемые пользователю услуги
Рисунок 1.10 – Схема доступа к информации с использованием различных конфигураций МАУ

Для решения задачи определения местоположения МАУ в качестве агентов могут выступать точки доступа БСПД, собирающие сведения об уровне сигнала МАУ, на основе которого будет осуществляться расчет местоположения МАУ в пределах области покрытия БСПД. Данный расчет может осуществляться, как в контроллере беспроводной сети, так и централизованно в точке принятия решения по управлению конфигурацией МАУ. Прототип такой многоагентной системы представлен на рисунке 1.11.

47

Сети беспроводных точек
доступа
Сеть контроллеров
беспроводных сетей
Центр управления
информационной
безопасностью
сенсоры агенты эффекторы планировщик
Рисунок 1.11 – Многоагентная система определения местоположения МАУ

Задача по управлению конфигурацией МАУ в зависимости от предъявляемых требований ИБ может решаться за счет внедрения в МАУ программноаппаратного агента, например, на базе доверенного аппаратно-программного модуля доверенной загрузки (АПМДЗ), обменивающегося информацией по защищенному каналу управления через доверенную беспроводную сеть доступа с центром управления информационной безопасности (ЦУИБ) ЗКС. Схема такой системы управления конфигурацией МАУ представлена на рисунке 1.12.

МАУ
Беспроводная сеть доступа
Центр управления
информационной
безопасностью
Система
определения
местоположения
АПМДЗ
Агенты:
сенсоры/
эффекторы
планировщик сенсоры
Рисунок 1.12 – Схема подсистемы управления конфигурацией МАУ

Реализация представленных систем совместно с использованием технологий терминального доступа, виртуализации или оптоэлектронной развязки объединенных программно-аппаратных платформ в едином корпусе позволит обеспечить защищенный удаленный доступ к сетям с разными требованиями по защищенности с использованием одного МАУ.

48

1.5. Постановка задачи диссертационного исследования

Для повышения вероятности обеспечения безопасности информации при доступе к инфокоммуникационным услугам и информации в корпоративных сетях с разными требованиями по защищенности, необходимо разработать систему управления безопасностью МАУ, позволяющую управлять программноаппаратной конфигурацией МАУ и доступом мобильных пользователей к инфокоммуникационным услугами и ресурсам в зависимости от атрибутов доступа, включая местоположение устройства, а также требований по безопасности информации и качеству предоставляемых услуг.

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.

Исходные данные:

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

2) множество возможных конфигураций МАУ – CONF ;

3) расположение и параметры помещений:

1 1 2 2
(,), (,),..., (,),
i
i i i i i in in Room
Rooms room x y x y x y L , 1,
Rooms
iN , (1.1)

где

i
Room

L – уровень требований по защищенности помещения,

1 1 2 2
(,), (,),..., (,)
i i i i i in in
x y x y x y – координаты n углов помещений,
Rooms

N – количество
помещений;
4) расположение точек доступа беспроводной сети ,
j j j
AP AP x y ,
1,
AP
jN , где (,)
jj
xy – координаты точек доступа,
AP
N – количество точек доступа;
49
5) множество пороговых значений частных показателей эффективности
треб доп
β β RECONF
,
Room Room RECONF
H P L L P T T ;
6) совокупность атрибутов доступа
i
Aa , включающая:
идентификационные данные о пользователе, МАУ, операционной системе
(ОС) и приложениях МАУ;
сетевая адресная информация;
уровень конфиденциальности и идентификатор запрашиваемой услуги (ресурса).
Требуется:
1) разработать модель безопасности МАУ Z , учитывающую вероятность
нахождения МАУ в специальных помещениях, обосновать ее корректность и оценить качество;
2) разработать алгоритм управления безопасность�� 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:
(, , ,)
1
треб
БИ БИ
F MD Rooms AP A
i
t
Z CONF
P T P T
; (1.2)
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;
50
МАУ имеет возможность функционировать в различных программноаппаратных 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;
4) оценить эффективность разработанной системы управления безопасностью МАУ.
Для получения оценки эффективности предложенной системы управления
безопасностью МАУ, а также

оценки степени достижения цели диссертационного
исследования целесообразно воспользоваться критерием превосходства [64], [15]

исходя из специфики предъявляемых к системе требований.
Система показателей качества [45] построена из следующих соображений.
Поскольку цель разрабатываемой системы – обеспечение безопасности информации (защиты информации) при эксплуатации МАУ в корпоративных сетях с разными требованиями по защищенности, то степень достижения данной цели согласно теории эффективности целенаправленных процессов [64] может быть представлена в виде выражения
тр доп доп
ЗИМАУ
P P REZ REZ P RES RES P OPR OPR , (1.3)
где REZ – результативность процесса защиты информации;
треб
REZ – требуемое
значение результативности процесса защиты информации; RES – ресурсоемкость
процесса защиты информации;
доп
RES – максимально допустимый расход ресурсов для процесса защиты информации; OPR – затраты операционного времени
для достижения цели функционирования системы;
доп
OPR – максимально допустимое время для достижения цели функционирования системы.
В соответствие с [7, 15, 17, 26] безопасность информации является комплексным свойством и обеспечивается за счет выполнения требований по обеспе-
51

чению конфиденциальности, целостности и доступности информации. Исходя из
этого, результативность процесса защиты информации при эксплуатации МАУ
может быть представлена в виде выражения
БИ КИ ЦИ ДИ
P T P T P T P T , (1.4)
где
КИ
PT – вероятность обеспечения конфиденциальности информации в течение времени T ;
ЦИ
PT – вероятность обеспечения целостности информации;
ДИ
PT – вероятность обеспечения доступности информации.
Вопросы обеспечения целостности информации в работе не рассматриваются, поэтому показатель при расчетах принят равным единице:
ЦИ
1 PT .
Вероятность обеспечения доступности информации предлагается оценивать
по своевременности обработки запросов на доступ к услугам [18] с учетом количества доступным услуг
ДУ
N относительно их общего числа
У
N . Тогда вероятность предоставления информации или услуг
ДИ ДИ
() PT за заданное время
зад
ДИ
T будет определяться с помощью табулированной неполной гамма-функции [18]:
ДУ ДУ у
ДИ ДИ ДИ ДИ
УУ
( ) ( ) (т) т т / (у)
0
У
NN
P T P T exp d
NN
, (1.5)
где
2
у зад
полн
ДИ
2
полн
2 полн
( ) (т) т т / (у) - гамма функция, у,
0
у
T
exp d T
T
TT
,(1.6)
где
полн
T и
2
T – 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),
зад
ДИ
T – 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
52
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 [7, 18]. Исходя из этих соображений, показатель вероятности обеспечения конфиденциальности может быть представлен в виде выражения
КИ НСД СК
( ) 1 P T P P T , (1.7)
где
НСД
P – вероятность НСД к информации;
СК
PT – 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
доп доп
НСД

11 ββ
Room Room
P P CONF CONF P L L
, (1.8)
доп доп
ββ Room Room
P CONF CONF P P L L P
, (1.9)
где CONF – конфигурация МАУ, сформированная системой управления безопасностью МАУ;
доп
CONF – 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
доп доп
/
RECONF RECONF
P T T CONF CONF
, а также
вероятностью преодоления СЗИ за данный период времени
ПрЗ
P [7, 18]. Данный
показатель может быть представлен в виде выражения:
доп доп
СК ПрЗ
/1
RECONF RECONF RECONF
P T P T T CONF CONF P
. (1.10)
53
В соответствие с [18, с. 41-42] показатель
ПрЗ
P может быть рассчитан как
ПрЗ НСД
1
1
м
к
м
PP
, (1.11)

где к – количество преград, которое необходимо преодолеть нарушителю, чтобы получить доступ к [21]

информационным и программным ресурсам,
НСД
м
P – вероятность преодоления нарушителем м-той преграды (средства защиты).

Для экспоненциальной аппроксимации распределений исходных характеристик при их независимости:
м
[21]

НСД
м
мм
f
P
fu
, (1.12)
где
м
f – среднее время между соседними изменениями параметров м-й преграды
системы защиты (время между сменой конфигураций);
м
и – среднее время расшифровки (вскрытия) значений параметров м-й преграды системы защиты. Показатель
ПрЗ
P в рамках работы вынесен в ограничения и принят равным нулю.
Ресурсоемкость процесса защиты информации [7] при эксплуатации МАУ
может быть определена, исходя из выражения:
МАУ
ЗИМАУ ИВР ВР ИТР ТР ИСУ СУМАУ
ИСОМ СОМ МАУ Польз
1
,
i
N
i
RES K C K C K C
K C C N
(1.13)
где

ИВР
K – коэффициент использования вычислительных ресурсов;
ВР
C – стоимость вычислительных ресурсов;
ИТР
K – коэффициент использования телекоммуникационных ресурсов;
ТР
C – стоимость телекоммуникационных ресурсов;
ИСУ
K – коэффициент использования системы управления безопасностью МАУ;
СУМАУ
C – стоимость системы управления безопасностью МАУ;
ИСОМ
K – коэффициент использования системы определения местоположения МАУ;
СОМ
C – стоимость системы определения местоположения МАУ;
МАУ
i
C – стоимость i -го МАУ,
54
необходимого для доступа к услугам;
МАУ
N – количеством МАУ, необходимых
для доступа ко всему перечню услуг;
Польз
N – количество пользователей МАУ.
Решение научной задачи предполагается проводить в рамках структуры исследования, представленной на рисунке 1.13.
I. Формирование основных исходных данных для проведения исследования,
их анализ и обобщение
1. Характеристика условий функционирования и требований, предъявляемых к МАУ в корпоративных
сетях с разным уровнем конфиденциальности
3. Характеристика моделей угроз и нарушителя ИБ при эксплуатации МАУ и технических решений
для защиты от них
5. Исследование технологий определения местоположения пользователей МАУ в помещениях внутри
здания
1. Модель безопасности МАУ, отличающаяся от известных учетом его местонахождения в
корпоративных сетях с различными требованиями по защищенности
6. Постановка задачи на проведение исследований и ее декомпозиция на систему частных задач,
формулировка цели, объекта, предмета исследования, допущений, ограничений
III. Научно-технические предложения по практической реализации системы управления
безопасностью МАУ в корпоративных сетях
4. Анализ способов построения комплексной СЗИ при доступе к сетям с разными требованиями по
защищенности
II. Решение научной задачи
2. Оценка качества предложенной модели и сравнение полученных результатов с прототипом
2. Анализ существующих систем контроля доступа и актуальных формальных моделей безопасности
компьютерных систем
1. Предложения по использованию алгоритмов определения местоположения МАУ на основе БСПД,
исследование их эффективности в зависимости от карты расположения помещений и обоснование
оптимальных параметров данных алгоритмов.
2. Предложения по применению численного метода на основе метода Монте-Карло для определения
вероятности нахождения МАУ в специальном помещении.
3. Предложения по применению алгоритма управления безопасностью МАУ в системе управления
безопасностью МАУ в корпоративных сетях.
4. Оценка эффективности предложенной системы управления безопасностью МАУ
4.1. Оценка результативности процесса защиты информации при эксплуатации МАУ
4.1.1. Оценка вероятности обеспечения конфиденциальности информации
4.1.2. Оценка вероятности сохранения конфиденциальности информации за заданный период
4.1.3. Оценка вероятности обеспечения доступности информации
4.2. Оценка ресурсоемкости процесса защиты информации при эксплуатации МАУ5. Научнотехнические предложения по реализации системы управления безопасностью МАУ
3. Алгоритм управления безопасностью МАУ, учитывающий атрибуты доступа мобильных
пользователей
4. Комплексная оценка эффективности и свойств предложенного алгоритма.
Рисунок 1.13 – Структурно-логическая схема исследования
55
Выводы по первому разделу
1. Использование вычислительных ресурсов современных МАУ в корпоративных сетях и обеспечение доступа к широкому перечню услуг корпоративных сетей, в том числе, защищенных является актуальной задачей. В настоящее время
она не решена, поскольку отсутствуют эффективные СЗИ, нейтрализующие угрозы ИБ, связанные с использованием МАУ, в том числе при доступе к сетям с разными требованиями по защищенности.
2. Существует ряд недостатков современных формальных моделей безопасности компьютерных систем применительно к обеспечению безопасности информации при использовании МАУ, включая существующие технические и программно-аппаратные решения:
1) отсутствуют технические решения по определению местоположения
МАУ, обладающие достаточной точностью;
2) отсутствует техническая возможность интеллектуального программноаппаратного блокирования МАУ или их отдельных функциональных блоков, представляющих при определенных условиях угрозу ИБ в ЗКС;
3) доступ к сетям с разными требованиями по защищенности с использованием МАУ осуществляется либо с использованием разных МАУ соответствующих необходимому уровню защищенности либо с ручным переключением режимов работы; отсутствует автоматическое управление программно-аппаратной конфигурацией МАУ в зависимости от уровня конфиденциальности предоставляемых услуг, местоположения МАУ и других атрибутов доступа.
Наличие указанных недостатков свидетельствует о необходимости учета такого фактора как местоположение МАУ, а также доработки формальных моделей безопасности и обоснования их корректности. Необходима разработка новых технических предложений по реализации программно-аппаратной платформы универсального единого МАУ, позволяющего обеспечить защищенный доступ к

услугам сетей с разными требованиями по защищенности.
56
3. Для решения задачи сопряжения контуров обработки информации с разными требованиями по защищенности в современных МАУ предлагается использовать агентно-ориентированный подход, являющийся элементом искусственного
интеллекта и построенный на основе клиент-серверной архитектуры. Данный
подход позволит применить технологию удаленного управления программноаппаратной конфигурацией МАУ на основе информации о его местоположении на
и других атрибутах доступа.
4. 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.
57
2. МОДЕЛЬ БЕЗОПАСНОСТИ МОБИЛЬНОГО АБОНЕНТСКОГО
УСТРОЙСТВА В КОРПОРАТИВНЫХ СЕТЯХ С РАЗНЫМИ
ТРЕБОВАНИЯМИ ПО ЗАЩИЩЕННОСТИ
Данный раздел посвящен разработке формальной модели безопасности
МАУ. Отличительной особенностью данной модели является учет атрибутов доступа, включая местонахождение МАУ в специальных помещениях здания, в котором развернуты корпоративные сети с разными требованиями по защищенности. Предложена модель безопасности МАУ, обоснована ее корректность. На основе анализа технологий определения местоположения МАУ в помещениях внутри зданий предложено технологическое решение, позволяющее повысить достоверность определения местоположения МАУ в помещениях с разными требованиями по защищенности за счет применения метода статистических испытаний.
Обосновано применение предложенного технологического решения для оценивания местонахождения МАУ на территории помещений организации с заданной точностью. Разработана имитационная модель, позволяющая оценить оптимальные параметры алгоритмов определения местоположения, проведена оценка его качества. Представлены результаты моделирования.
2.1. Постановка задачи на разработку модели
Рассматриваемая в качестве объекта исследования в диссертационной работе система управления безопасностью МАУ в корпоративных сетях с разными требованиями по защищенности может быть отнесена к компьютерной системе (КС). В

соответствии с [5] при анализе безопасности КС, которые должны обладать высоким уровнем доверия, начиная с оценочного уровня доверия 5, согласно классификации по [5], требуется, чтобы при разработке КС была использована формальная модель политики безопасности.
58
[2]

Для анализа безопасности предлагаемой в работе системы управления МАУ
и достижения цели исследования, заключающейся в повышении вероятности
обеспечения безопасности информации при эксплуатации МАУ необходимо разработать модель безопасности МАУ, отличающуюся от известных учетом его местонахождения в корпоративных сетях с разными требованиями по защищенности. Формальная постановка задачи на разработку модели: на основе теорий множеств, конечных автоматов, машинного обучения, математической статистики и
численных методов разработать модель безопасности МАУ.
Предлагаемая в работе модель безопасности МАУ базируется на классической модели Белла-ЛаПадулы [106], элементах ролевой [135, 139] и
атрибутной [115] моделях управления доступом, а также и моделях безопасности,
учитывающих местоположение субъектов [100, 102, 118].
Исходные данные:
1) элементы классической модели Белла-ЛаПадулы:
S – множество субъектов системы;
MD – множество МАУ, при этом MD S ;
O – множество объектов системы, включая функциональные блоки МАУ;
, , , P

read write append **[7]**execute – множество видов **[2]**

Страницы: 1 2 3 4 Все