ПЛЕНАРНЫЕ ДОКЛАДЫ

УДК 517.9:537.86:530.182

СПОСОБЫ СКРЫТОЙ ПЕРЕДАЧИ ИНФОРМАЦИИ НА ОСНОВЕ ХАОТИЧЕСКОЙ СИНХРОНИЗАЦИИ

О.И. МОСКАЛЕНКО[1,2], А.А. КОРОНОВСКИЙ[1,2], А.С. ПАВЛОВ[1], Н.С. ФРОЛОВ[1], А.Е. ХРАМОВ[1,2]

[1]ФГБОУ ВПО «Саратовский государственный университет имени Н.Г. Чернышевского»
ул. Астраханская, 83, г. Саратов, 410012, Российская Федерация
o.i.moskalenko@gmail.com

[2]ФГБОУ ВПО «Саратовский государственный технический университет имени Гагарина Ю.А.»
ул. Политехническая, 77, г. Саратов, 410054, Российская Федерация
hramovae@gmail.com

Представлен обзор результатов по использованию хаотической синхронизации для скрытой передачи информации. Рассмотрены способы скрытой передачи данных на основе различных типов синхронного поведения (полной, фазовой, обобщенной синхронизации и т.д.) и обсуждены их достоинства и недостатки по сравнению друг с другом. Намечены пути дальнейшего совершенствования этих способов передачи информации с целью устранения имеющихся недостатков.

Ключевые слова: динамический хаос, хаотическая синхронизация, скрытая передача информации, обобщенная синхронизация, генератор хаоса, шум.

Одним из наиболее важных практических приложений хаотической синхронизации является ее применение для скрытой передачи информации [1, 2]. Эта проблема берет свое начало еще с 1992 года и остается актуальной до сих пор, свидетельством чего служит непрерывный рост числа научных публикаций по данной тематике. Интерес к этой проблеме обусловлен, прежде всего, тем, что все известные до настоящего времени способы и устройства скрытой коммуникации обладают рядом принципиальных недостатков и трудностей при технической реализации, основными из которых являются низкая устойчивость к шумам, требование высокой степени идентичности к генераторам, располагающимся на различных сторонах канала связи, проблемы конфиденциальности (более детально см. обзор [2]). В последнее время появились попытки разработки способов скрытой передачи информации, лишенные в той или иной мере всех вышеперечисленных недостатков. В то же самое время совершенствование этих способов продолжается и по сей день.

В настоящем докладе представлен обзор последних работ, посвященных использованию хаотической синхронизации для скрытой передачи информации. Рассмотрены способы скрытой передачи данных на основе полной (хаотическая маскировка, переключение хаотических режимов, нелинейное подмешивание информационного сигнала к хаотическому, модулирование управляющих параметров) [1], фазовой [3] и обобщенной [4, 5] синхронизации, а также использующие несколько типов синхронного поведения одновременно [4, 6]. Путем численного моделирования проведен сравнительный

анализ вышеперечисленных способов скрытой коммуникации. В качестве генераторов передающего и принимающего устройств во всех случаях выбраны одни и те же генераторы низкочастотных колебаний (на основе систем Ресслера) с близкими значениями управляющих параметров, а в качестве информационных сигналов - простые последовательности бинарных битов. Сравнение осуществлялось путем расчета нескольких количественных характеристик работоспособности схем, основными из которых являются:

1. Отношение энергии на бит к спектральной плотности мощности шума [7, 8], при котором схема передачи данных становится неработоспособной:

$$\mathrm{SNR} = 10\lg\frac{E_b}{N_0}, \quad [\text{дБ}] \tag{1}$$

где $E_b = \mathrm{P}_{sign}T$ (P_{sign} - мощность передаваемого сигнала (в отсутствие шума), T - время передачи одного бита) - энергия сигнала, приходящаяся на один бит передаваемой информации, $N_0 = \mathrm{P}_{noise}/\Delta f$ (P_{noise} - мощность шума в канале связи, Δf - ширина полосы пропускания канала) - спектральная плотность мощности шума.

2. Зависимость вероятности ошибки на бит от отношения энергии на бит к спектральной плотности мощности шума [9]:

$$\mathrm{BER} = 2(P_{01}P_0 + P_{10}P_1), \tag{2}$$

где P_{00} (P_{11}) - вероятность корректной передачи бинарного бита 0 (1), $P_{01} = 1 - P_{00}$ ($P_{10} = 1 - P_{11}$) - вероятность ошибочного диагностирования бинарного бита 1 (0) при передаче бинарного бита 0 (1), P_0 (P_1) - вероятность появления символа 0 (1) в передаваемой последовательности.

3. Максимальное значение расстройки управляющих параметров (РМ, %) генераторов, которые изначально должны быть идентичными.

4. Максимальный уровень нелинейных искажений в канале связи

$$\mathrm{ND} = 10\lg\frac{\mathrm{P}_x}{\mathrm{P}_y}, \quad [\text{дБ}] \tag{3}$$

при котором схема работает. Здесь P_x - мощность сигнала $x(t)$ на выходе передающего генератора, P_y - мощность сигнала $y(t)$ на входе принимающего устройства. Нелинейные искажения имеют вид $y = x(1 - \alpha x^2)$, где α - малый параметр [1].

Результаты расчета указанных характеристик для всех рассмотренных способов передачи информации представлены в табл. 1. Видно, что способ на основе обобщенной синхронизации [5] (схема 9) становится неработоспособным при отрицательном значении отношения энергии на бит к спектральной плотности мощности шума ($\mathrm{SNR} = -10.01$ дБ), в то время как для других схем и устройств эта величина оказывается положительной. То есть, при наличии в канале связи шумов, мощность которых меньше мощности передаваемого сигнала, большинство известных схем становится неработоспособным. Понятно, что значения таких характеристик будут меняться от схемы к схеме. Из схем 1–8 в этом отношении лучшими являются показатели для схем на основе переключения хаотических режимов и модулирования управляющих параметров (схемы 2 и 4). Но положительное значение энергии на бит к спектральной плотности шума свидетельствует об ограниченной устойчивости к шумам и деструктивной роли шума при передаче информации. Схема 9 обладает значительной устойчивостью к шумам. При этом, еще более искажая передаваемый

сигнал, шум препятствует третьей стороне декодировать информационное сообщение. В этом случае можно говорить о конструктивной роли шума в плане повышения конфиденциальности передачи информации, в то время как в остальных случаях роль шума является деструктивной.

Табл. 1. Отношение энергии на бит к спектральной плотности шума (SNR , дБ), расстройка управляющих параметров (PM, %) изначально идентичных генераторов и уровень нелинейных искажений в канале связи (ND, дБ), до которых схемы остаются работоспособными

№	Название схемы	SNR, дБ	PM, %	ND, дБ
1	Хаотическая маскировка [1]	56.48	0.30	1.03
2	Переключение хаотических режимов [1]	30.76	2.00	23.3
3	Нелинейное подмешивание [1]	64.99	0.30	0.26
4	Модулирование управляющих параметров [1]	30.76	2.00	23.3
5	Схема на основе фазовой синхронизации [3]	32.40	0.80	10.7
6	Схема на основе обобщенной синхронизации [4]	39.52	1.00	7.75
7	Схема на основе обобщенной и полной синхронизации [4]	39.24	0.50	4.83
8	Схема с «комбинированным сигналом» [6]	61.47	0.20	2.63
9	Схема на основе обобщенной синхронизации [5]	–10.01	2.00	27.2

Справедливость вышеприведенных рассуждений подтверждается также зависимостью вероятности ошибки на бит от спектральной плотности мощности шума для различных схем передачи информации. Указанные зависимости представлены на рис. 1.

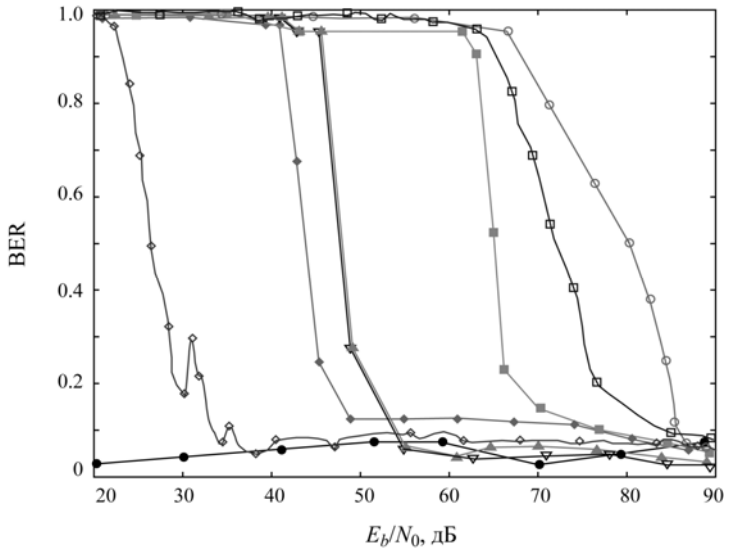


Рис. 1. Зависимости вероятности ошибки на бит (BER) от отношения энергии на бит к спектральной плотности мощности шума (E_b/N_0) для различных схем передачи информации: ○ - хаотическая маскировка, ♦ - переключение хаотических режимов (модулирование управляющих параметров), ■ - нелинейное подмешивание, ◊ - схема на основе режима фазовой синхронизации, ▲ - схема на основе режима обобщенной синхронизации, Δ - схема на основе обобщенной и полной синхронизации, □ - схема с «комбинированным» сигналом, ● - схема на основе обобщенной синхронизации, устойчивая к шумам

Видно, что для различных способов передачи информации (табл. 1, схемы 1–8) вероятность ошибки на бит достаточно быстро становится равной 1, в то время как для

схемы 9 она оказывается близкой к 0, независимо от интенсивности шума, воздействующего на систему, что достаточно хорошо согласуется с результатами, представленными выше.

Что же касается влияния расстройки управляющих параметров на эффективность работы рассмотренных способов, то здесь максимальными показателями обладают сразу три схемы (2, 4 и 9 табл. 1). Однако, схема 9 обладает принципиальным достоинством и в этом отношении. Изначально идентичные хаотические генераторы в схемах 2 и 4 должны располагаться на различных сторонах канала связи. В последнем же случае идентичные генераторы располагаются только на принимающей стороне канала связи, что позволяет легко осуществить их юстировку. Кроме того, схема 9 оказывается более устойчивой и по отношению к влиянию нелинейных искажений в канале связи по сравнению с другими рассмотренными способами передачи данных.

Более того, высокая устойчивость схемы передачи информации на основе обобщенной синхронизации [5] по отношению к шумам позволяет предложить сразу две ее возможные модификации [10, 11], направленные на повышение конфиденциальности передачи данных путем изменения характеристик передаваемого сигнала при помощи дополнительного генератора шума. В то же самое время, и эти способы не свободны от недостатков. В частности, как отмечалось выше, все они по-прежнему характеризуются нестабильностью работы при неидентичности параметров генераторов, однако в отличие от других известных способов передачи информации изначально идентичные хаотические генераторы в них располагаются на одной стороне канала связи, что позволяет осуществлять их юстировку.

Юстировка генераторов хаотических колебаний оказывается не всегда возможной. Более того, эта проблема усугубляется в процессе длительной эксплуатации устройств, что делает способы [5, 10, 11] неработоспособными в долгосрочной перспективе. В то же самое время режим обобщенной синхронизации может наблюдаться не только в случае воздействия хаотического сигнала на хаотические генераторы, но и при воздействии того же хаотического сигнала на генераторы периодических колебаний [12]. Разработка идентичных генераторов периодических колебаний является менее сложной задачей, чем реализация хаотических генераторов. Более того, в данном случае нестабильность работы генераторов при неидентичности параметров выражена намного меньше, чем в случае использования генераторов хаоса, что сделает подобную схему стабильной и работоспособной в течение длительного времени. При этом качество передачи информации будет более высоким.

На основании вышесказанных аргументов предложена модификация способа передачи информации на основе обобщенной синхронизации путем замены хаотических генераторов принимающего устройства на аналогичные генераторы периодических колебаний. Принципиальная схема для реализации этого способа приведена на рис. 2. Способ скрытой передачи информации заключается в следующем. Полезный информационный сигнал $m(t)$ *1* кодируется в виде бинарного кода. Один или несколько управляющих параметров передающего генератора $\mathbf{x}(t)$ *2* модулируется информационным сигналом таким образом, чтобы характеристики передаваемого сигнала менялись незначительно, но при этом оставалась возможность возникновения/разрушения режима обобщенной синхронизации в зависимости от передаваемого бинарного бита. Сигнал, генерируемый передающей системой, передается по каналу связи *3*. Принимающее устройство находится на другой стороне канала связи. Оно представляет собой два идентичных генератора периодических колебаний, второй $\mathbf{u}(t)$ *4* и третий $\mathbf{v}(t)$ *5*, способных находиться в режиме обобщенной синхронизации с передающим *2*. Принцип

работы принимающего устройства основан на диагностике режима обобщенной синхронизации при помощи метода вспомогательной системы. Сигнал с канала связи поступает на генераторы принимающего устройства. Полученные на выходе сигналы проходят через вычитающее устройство *6*, и затем детектируется восстановленный полезный сигнал *7*, представляющий собой чередующуюся последовательность участков с несинхронным и синхронным поведением, по которой исходный информационный сигнал может быть легко детектирован.

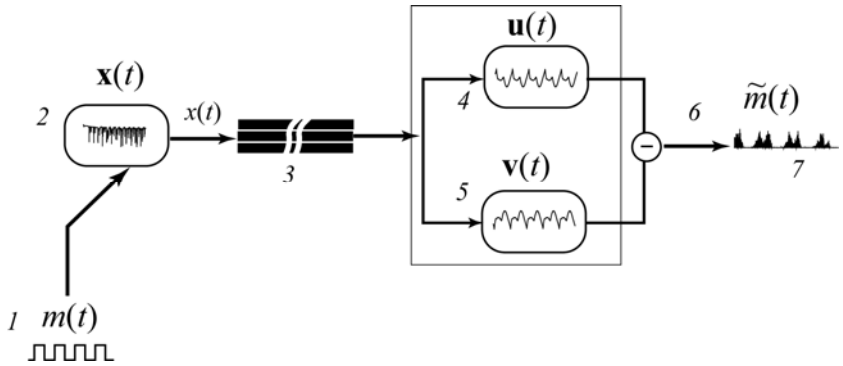


Рис. 2. Схема для скрытой передачи информации на основе обобщенной синхронизации в случае воздействия хаотического сигнала на генераторы периодических колебаний: *1* - полезный бинарный сигнал $m(t)$, *2* - первый (передающий) генератор, *3* - канал связи, *4* – второй (принимающий) генератор, *5* - третий генератор, идентичный второму генератору *4* по управляющим параметрам, *6* - вычитающее устройство, *7* - восстановленный полезный сигнал $\tilde{m}(t)$

Эффективность предложенного способа проверена путем численного моделирования при использовании систем Ресслера и низковольтных виркаторов в качестве генераторов передающего и принимающего устройств. Показано, что в обоих случаях способ работает эффективно, при этом его устойчивость к шумам оказывается выше, чем при использовании генераторов хаоса в принимающем устройстве.

Работа выполнена при поддержке Российского фонда фундаментальных исследований (проект № 12-02-33071) и Совета по грантам Президента Российской Федерации для государственной поддержки молодых российских ученых – докторов наук (МД-345.2013.2).

Список литературы

1. *Дмитриев А.С., Панас А.Н.* Динамический хаос. Новые носители информации для систем связи. М.: Физматлит, 2002.

2. *Короновский А.А., Москаленко О.И., Храмов А.Е.* // Успехи физических наук. 2009. Т. 179, № 12. С. 1281–1310.

3. *Chen J.Y., Wong K.W., Cheng L.M. et al.* // CHAOS. 2003. V. 13, № 2. P. 508–514.

4. *Terry J.R., VanWiggeren G.D.* // Chaos, Solitons and Fractals. 2001. V. 12. P. 145–152.

5. *Короновский А.А., Москаленко О.И., Попов П.В., Храмов А.Е.* // Изв. РАН. Сер. физическая. 2008. Т. 72, № 1. С. 143–147.

6. *Murali K., Lakshmanan M.* // Phys. Lett. A. 1998. V. 241. P. 303–310.

7. *Скляр Б.* Цифровая связь. Теоретические основы и практическое применение. М., 2003.

8. *Побережский Е.С.* Цифровые радиоприемные устройства. М., 1987.

9. *Abel A., Schwarz W.* // Proceedings of the IEEE.2002. V. 90, № 5. P. 691-710.

10. *Moskalenko O.I., Koronovskii A.A., Hramov A.E.* // Phys. Lett. A. 2010. V. 374. P. 2925–2931.

11. *Короновский А.А., Москаленко О.И., Храмов А.Е.* // Журнал технической физики. 2010. Т. 80, № 4. С. 1–8.

12. *Короновский А.А., Москаленко О.И., Павлов А.С., Фролов Н.С., Храмов А.Е.* // Журнал технической физики. 2014. Т. 84, № 5. С. 1–8.

ЭЛЕКТРОННОЕ ПРАВИТЕЛЬСТВО. ТЕХНОЛОГИИ БЕЗОПАСНОСТИ

Ю.И. МОСИЕНКО, М.Н. БОБОВ

ОАО «АГАТ-системы управления» – управляющая компания холдинга «Геоинформационные системы управления»
пр-т Независимости, 117, г. Минск, 220114, Республика Беларусь

По определению ООН «Электронное правительство – это такое правительство, которое применяет ИКТ с целью преобразования своих внутренних и внешних взаимоотношений». Более широкое определение данного понятия Евросоюза «Электронное правительство – это применение информационных и коммуникационных технологий в органах государственного управления, что в сочетании с организационными изменениями и внедрением новых навыков призвано совершенствовать государственные услуги и демократические процессы и обеспечивать поддержку институтам государственной политики». Схожее определение приведено в Концепции формирования в Российской Федерации электронного правительства «Новая форма организации деятельности органов государственной власти, обеспечивающая за счет широкого применения ИКТ качественно новый уровень оперативности и удобства получения организациями и гражданами государственных услуг и информации о результатах деятельности государственных органов».

Таким образом, электронное правительство является не частичным затратным технологическим решением, а концепцией осуществления управления государством и элементом масштабного информационного преобразования общества.

Общепризнано, что электронное правительство действует в трех направлениях:

• от правительства к правительству (G2G). К числу таких относятся проекты: создание межведомственных сетей, государственных и корпоративных баз данных, реестров введения электронного документооборота и т.п.;

• от правительства к населению (G2C). Проекты: предоставление сведений о свободных рабочих местах, выдача свидетельств о рождении, регистрация и голосование избирателей, медицинская информация и т.п.;

• от правительства к бизнесу (G2B). Проекты: проведение государственных закупок, выдача лицензий и разрешений и т.п.

Реализация этих направлений возможна в условиях обеспечения межведомственного информационного взаимодействия, создания интегрированного информационного пространства и решения ряда сформулированных ниже задач.

1. Интеграция информационных ресурсов различных ведомственных систем, как по горизонтали, так и по вертикали.

2. Определение правового статуса ведомственных информационных ресурсов, режимов их использования, оценки и включения в общегосударственное пользование – создание государственных информационных ресурсов (ГИР).

3. Разработка необходимой нормативно-правовой базы, принятие организационных решений по совершенствованию структуры и функций органов государственного управления.

4. Создание закрытой правительственной интранет-сети, обслуживающей различные ведомства и обеспечивающей интеграцию ведомственных информационных систем и ресурсов и их взаимодействие при оказании государственных услуг и принятии управленческих решений.

5. Определение на государственном уровне административных регламентов оказания государственных услуг, определяющих властные полномочия и обязанности различных ведомств, последовательность их взаимодействия в процессе оказания услуги, способ ее инициирования и активизации госорганом.

6. Разработка электронных административных регламентов на основе государственных административных регламентов, определяющих процесс административной деятельности по реализации государственных услуг в форме электронных документов и неразрывно взаимосвязанных с ними соответствующих формальных описаний этих процессов, поддержанных программной системой.

7. Создание правительственных шлюзов, позволяющих обеспечить взаимодействие между закрытым правительственным Интранетом и общедоступными системами для оказания услуг населению и бизнесу.

8. Разработка профиля технических нормативных правовых актов (ТНПА) межведомственного взаимодействия, ведения ГИР и регламентов их функционирования и использования.

9. Формирование единого расчетно-информационного пространства для онлайновой оплаты предоставляемых услуг по тарифам административных регламентов.

10. Разработка механизмов обеспечения безопасности инфотелекоммуникационной платформы для реализации полномочного доступа физических и юридических лиц к государственным информационным ресурсам и создания системы обращения юридически значимых электронных документов.

11. Создание специальной системы подготовки и переподготовки государственных служащих в области технологий информационного общества.

Концептуальная схема инфотелекоммуникационной платформы, необходимой для функционирования электронного правительства с учетом указанных направлений его деятельности в рамках определенных задач, представлена на рис. 1.

Концептуальная схема
инфотелекоммуникационной платформы электронного правительства

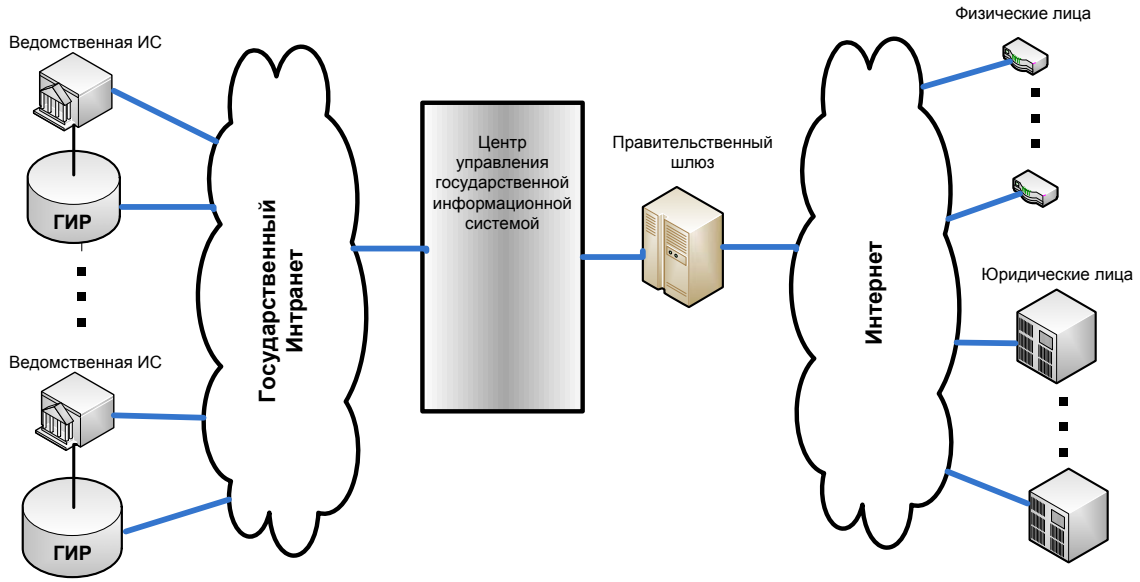


Рис. 1

Рис. 1. Концептуальная схема инфотелекоммуникационной платформы

Для создания и развития электронного правительства в Республике Беларусь правительством была принята Государственная программа информатизации Республики Беларусь на 2003–2005 годы и на перспективу являлось формирование в республике единого информационного пространства как одного из этапов перехода к информационному обществу, обеспечивающего создание условий для повышения эффективности функционирования экономики, государственного и местного управления, обеспечения прав на свободный поиск, передачу, распространение информации о состоянии экономического и социального развития общества.

Базовым проектом Программы «Электронная Беларусь» стало создание общегосударственной автоматизированной информационной системы (ОАИС), предназначенной для автоматизации деятельности государственных органов по предоставлению информационных услуг другим государственным органам, организациям и гражданам.

Целью создания ОАИС являлось повышение эффективности и качества функционирования государственных органов, а основные задачи создания ОАИС включали в себя:

– интеграцию базовых информационных ресурсов, имеющих государственное значение (ГИР), и формирование объединенного информационного ресурса государственных органов Республики Беларусь (ОГИР);

– реализацию полномочного доступа к объединенному ГИР, а также обеспечение его защищенности от несанкционированного доступа в соответствии с действующими в Республике Беларусь нормативными документами;

– формирование реестра информационных услуг, предоставляемых государственными органами;

– разработка государственного профиля взаимодействия открытых систем как методологической основы для интеграции и взаимодействия существующих и разрабатываемых информационных систем (ИС) государственных органов.

Таким образом, создание ОАИС позволило решить большинство задач, необходимых для функционирования электронного правительства в Республике Беларусь, и обеспечить основу для наращивания и развития государственных услуг с использованием информационно-телекоммуникационных технологий (ИКТ).

Архитектура ОАИС включает набор средств и методов для объединения и согласования функциональных, информационных и технических требований с возможностями информационных технологий, применяемых для ее реализации. Архитектура ОАИС представляет собой многоуровневую модель, приведенную на рис. 2.

Рис. 2. Архитектура ОАИС

Данным особенностям ОАИС наиболее полно и всесторонне удовлетворяет сервис-ориентированная архитектура (SOA – Service Oriented Architecture), которая позволяет представить бизнес-процессы (процессы взаимодействия ОАИС) в виде множества отдельных логических элементов (служб) с возможностью их комбинирования (и перекомбинирования) в различные решения и сценарии использования. С точки зрения требований к ОАИС, SOA позволяет обеспечить гибкость представления процессов взаимодействия.

Совокупность всех вариантов вызова сервиса должна быть предварительно определена; вызов должен быть осуществлен стандартным образом, результат вызова должен быть известен заранее (предварительно описан). Наиболее распространенным и, очевидно, оптимальным подходом, удовлетворяющим вышеприведенным требованиям и согласующимся с концепцией SOA являются Web–сервисы – совокупность технологий, позволяющих описывать сервисы, определять правила взаимодействия сервисов, создавать каталоги сервисов.

Web-сервисы находятся в строгом соответствии с рядом ключевых стандартов SOA, таких, как:

– WSDL (Web Services Description Language) – единый интерфейсный язык описания (дескриптора) Web-сервисов с точки зрения их использования;

– SOAP (Simple Object Access Protocol, в более позднем переводе Service Oriented Architecture Protocol) – по сути, механизм создания структурированных пакетов данных и обмена ими между сервисами;

– UDDI (Universal Description, Discovery and Integration) – реестр Web-сервисов, содержащий исчерпывающую информацию обо всех сервисах, опубликованных для использования провайдерами сервисов и обеспечивающий соединение Пользователя с провайдером сервиса.

Все три стандарта базируются на языке XML (EXtensible Markup Language) и являются открытыми, т.е. развиваются и модифицируются независимыми комитетами по стандартизации.

Центр управления государственной информационной системой образует ядро ОАИС, программно-техническая архитектура которого представлена на рис. 3.

Рис. 3. Программно-техническая архитектура ядра ОАИС

Система защиты информации ОАИС включает в себя комплекс технических и организационных мероприятий. Комплекс технических и программных средств распределен на серверах ядра ОАИС и АРМ администратора защиты (АЗ) ядра ОАИС. Организационные мероприятия по обеспечению безопасности осуществляет или контролирует их выполнение АЗ ядра ОАИС. Средства защиты, располагающиеся на уровне ведомственных ИС, разрабатываются самими ведомствами с учетом технических решений по защите информации ядра ОАИС.

Система защиты информации в ядре ОАИС имеет два уровня. Первый уровень – защита от физического доступа посторонних лиц к техническим средствам ядра ОАИС. Реализация первого уровня защиты обеспечивается организационно-техническими мероприятиями, которые реализуются эксплуатирующей организацией и направлены на предотвращение доступа посторонних лиц в помещения и контроль доступа персонала к техническим средствам ядра ОАИС. Второй уровень – защита от несанкционированного доступа (НСД) к объединенному государственному информационному ресурсу ОАИС, к ПО и данным ядра ОАИС. Реализация второго уровня защиты включает в себя:

– создание демилитаризованной зоны ядра ОАИС путем внешнего и внутреннего межсетевого экранирования http-сервера;

– обеспечение защищенного обмена пользователей с порталами ОАИС по протоколу TLS;

– обеспечение защищенного обмена пользователей с веб-сервисами ядра ОАИС или ядра ОАИС с веб-сервисами ГИР с использованием средств шифрования SOAP-конвертов;

– обеспечение защищенного обмена адаптера ядра ОАИС с ИС, содержащими ГИР с использованием протоколов защиты IP уровня;

– подтверждение подлинности SOAP конвертов путем выработки и проверки их ЭЦП;

– управление доступом к веб-сервисам ядра ОАИС и программному обеспечению ядра ОАИС;

– непрерывный контроль доступа к ПО и данным ядра ОАИС и аудит событий безопасности;

– контроль целостности ПО и данных ядра ОАИС;

– создание АРМ АЗ.

Схема распределения основных функций защиты по элементам ядра ОАИС приведена на рис. 4.

Создание демилитаризованной зоны осуществляется с помощью внешнего и внутреннего МСЭ. Внешний МСЭ (Cisco ASA 5520) предназначен для защиты http-сервера от внешних атак, а также для контроля исходящего из ядра ОАИС трафика. Внутренний МСЭ (Cisco ASA 5520) предназначен для защиты ресурсов ядра от несанкционированного проникновения со стороны http-сервера, а также http-сервера от внутренних атак из внутренней сети ядра ОАИС. Внешний и внутренний МСЭ обеспечивают:

– защиту IP адреса и портов http-сервера;

– защиту от сетевых атак;

– оповещение администратора защиты ядра ОАИС о контролируемых событиях и их аудит.

Защита IP адреса и портов http-сервера реализуется с использованием функции трансляции сетевых адресов (NAT) и трансляции адресов портов (PAT).

Защита от сетевых атак включает:

– защиту от DoS атак – функция Anti DoS;

– защиту от спуфинга – функция Anti спуфинг;

– защиту от сканирования портов.

Защита от сканирования портов реализуется МЭ постоянно в автоматическом режиме. Настройка перечня выполняемых МСЭ функций, формирование перечня кон-

тролируемых событий для организации оповещения и аудита осуществляются администратором защиты ядра ОАИС со своего АРМ через графический интерфейс пользователя (GUI – Graphic User Interface) или интерфейс командной строки (CLI – Command Line Interface).

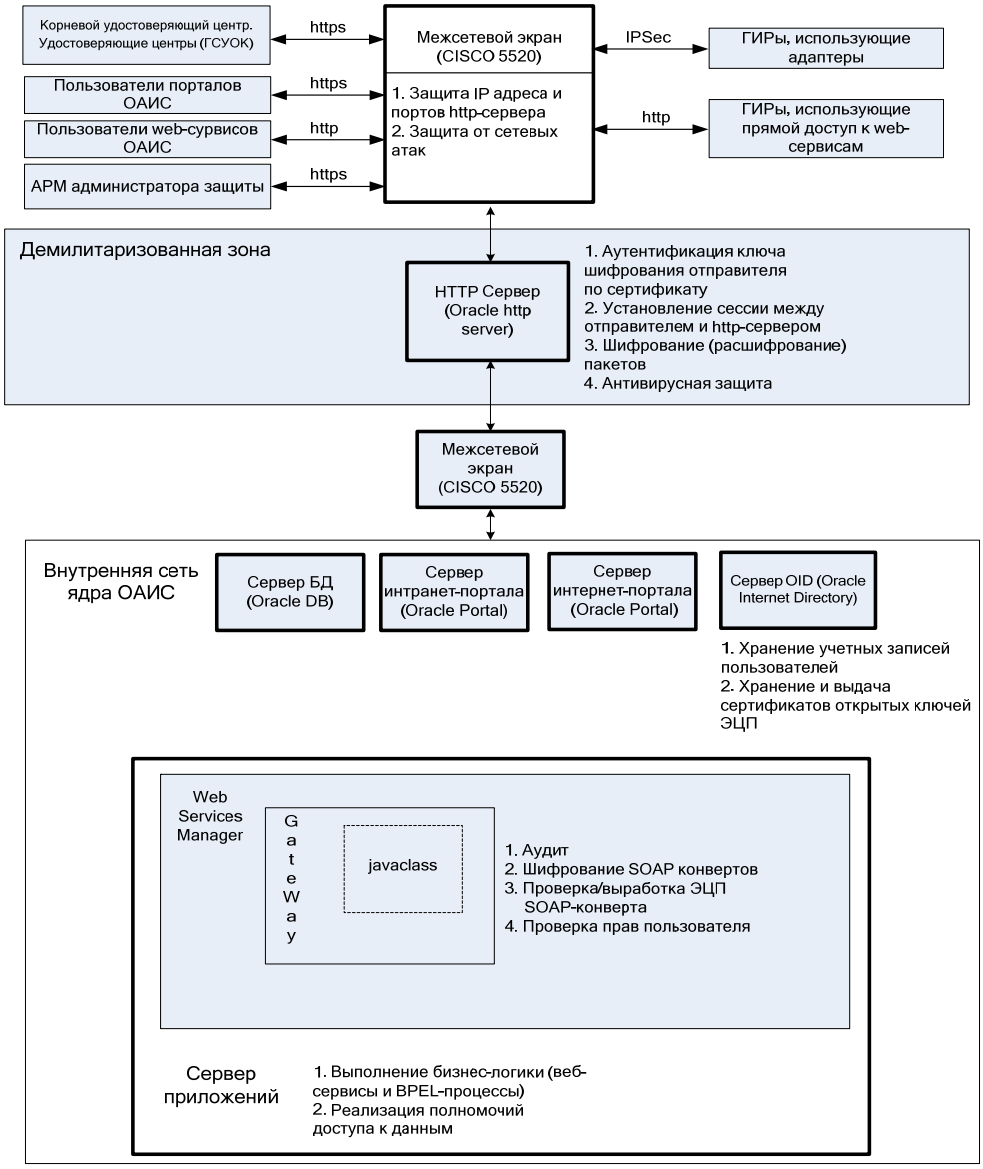


Рис. 4. Схема распределения основных функций защиты по элементам ядра ОАИС

Конфиденциальность и целостность информации в каналах связи при обмене ядра ОАИС с авторизованными пользователями и ГИР обеспечивается применением криптографических средств, реализующих алгоритмы по ГОСТ 28147-89. Защищенный обмен с пользователями порталов реализуется при помощи http-сервера с поддержкой модуля, реализующего протокол TLS с использованием криптографического алгоритма по ГОСТ 28147-89 и алгоритма выработки общего ключа по РД РБ «Банковские технологии. Протоколы формирования общего ключа». Для реализации защищенного обмена на http-сервере выполняются следующие функции:

– идентификация и аутентификация ключа отправителя запроса в ядро ОАИС (зарегистрированного пользователя);

– синхронизация с удостоверяющим центром списка действующих и отозванных цифровых сертификатов ключей шифрования;

– установление защищенной сессии и шифрование пакетов.

Защищенный обмен с пользователями веб-сервисов реализуется при помощи шифрования SOAP-конвертов в Web Services Manager с использованием сертифицированных ОАЦ программных средств криптографической защиты.

Защищенный обмен ядра ОАИС с ГИР через адаптеры ИС реализуется при помощи протокола ESP из состава стека протокола IPSec в транспортном режиме. При отправке IP пакетов осуществляется зашифрование их содержательной части и формирование имитоприставки для контроля целостности. На приемной стороне осуществляется расшифрование и проверка целостности принятых пакетов. Для организации защищенного соединения ядра ОАИС с адаптером ИС формируются общие ключи на основе имеющихся личных ключей шифрования ядра ОАИС и ИС в соответствии с РД РБ «Банковские технологии. Протоколы формирования общего ключа».

Подтверждение подлинности SOAP конвертов осуществляется с использованием механизма ЭЦП по СТБ 1176.2-99. Формирование и проверка ЭЦП SOAP конвертов осуществляется в WSM с использованием сертифицированного ОАЦ программного средства ЭЦП.

Схема подключения механизмов защиты в процессе обработки запроса участников информационного обмена в ОАИС приведена на рис. 5, 6.

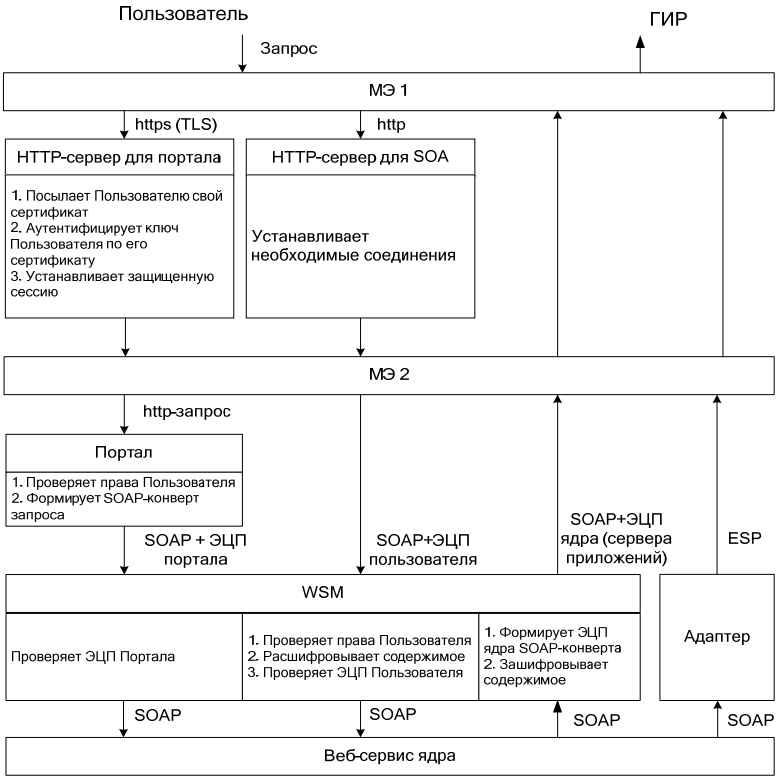


Рис. 5. Схема подключения механизмов защиты в процессе обработки запроса (пользователь – ядро ОАИС – ГИР)

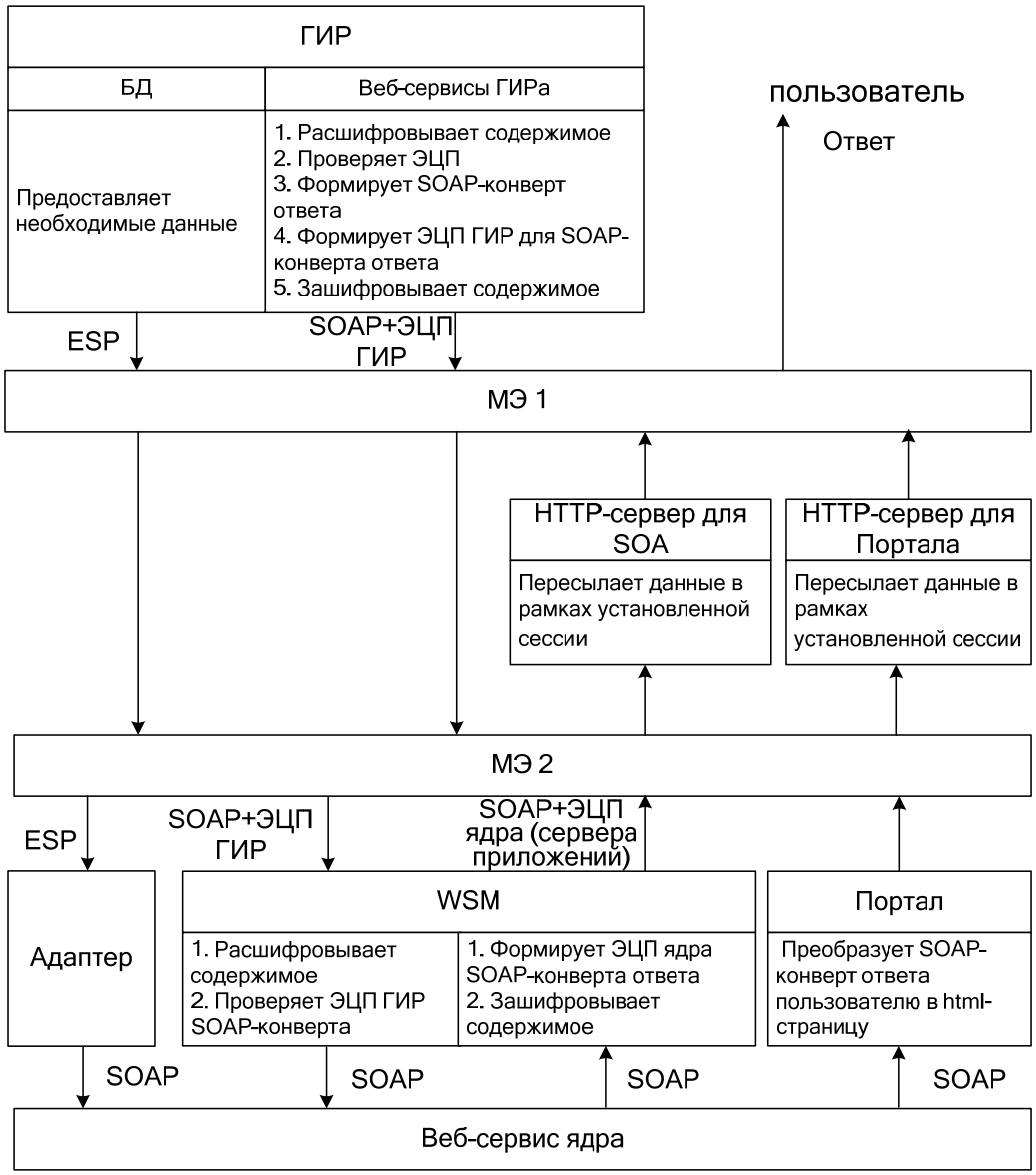


Рис. 6. Схема подключения механизмов защиты в процессе формирования ответа на запрос (ГИР – ядро ОАИС – пользователь)

Управление доступом включает в себя:

– назначение прав пользователям и процессам;

– проверку полномочий пользователя при его обращении к ядру ОАИС.

Назначение прав доступа пользователям, процессам и администраторам ядра ОАИС осуществляется АЗ с использованием средств Oracle, ОС Linux, МСЭ, http-сервера на основе межведомственных соглашений по порядку предоставления информации и услуг при доступе к ГИР и в соответствии с регламентом доступа к ядру ОАИС. Доступ пользователей к ГИР осуществляется только через веб-сервисы ядра ОАИС после проверки их полномочий. Проверка полномочий пользователей осуществляется при помощи Web Services Manager, который выполняет следующие функции:

– определяет для каждого веб-сервиса перечень групп пользователей, которым разрешен доступ;

– идентифицирует пользователя путем проверки его идентификатора в SOAP-запросе. Учетные записи пользователей хранятся в LDAP-каталогах на сервере OID (Oracle Internet Directory);

– аутентифицирует пользователя по его цифровой подписи SOAP конверта;

– предоставляет или блокирует пользователю доступ к веб-сервису в зависимости от принадлежности пользователя к группе, имеющей доступ к данному веб-сервису.

Состав информации, выдаваемой пользователю, определяется на уровне выполняющих бизнес-логику процессов.

Контроль целостности прикладного ПО серверов ядра ОАИС и АРМ администратора защиты, а также настраиваемых значений средств защиты осуществляется прикладной программой, обеспечивающей:

– формирование эталонных значений характеристик целостности;

– настройку администратором защиты перечня контролируемых объектов;

– периодический контроль состояния характеристик целостности контролируемых объектов;

– формирование и доведение на АРМ АЗ информации о результатах контроля целостности.

Контроль целостности данных, хранящихся в базе данных, осуществляется средствами Oracle. Контроль целостности информации, передаваемой по каналам связи, осуществляется с использованием криптографических алгоритмов протокола TLS.

Непрерывный контроль доступа и аудит событий безопасности осуществляется при помощи следующего ряда процедур. Аудит событий безопасности БД Oracle, сервера приложений Oracle, http-сервера осуществляется средствами Oracle. Аудит событий безопасности на МСЭ осуществляется средствами его программного обеспечения путем соответствующей настройки. Журналы событий на МСЭ могут вестись на встроенной FLASH памяти, на внешнем FLASH носителе – Compact Flash, на любом из серверов ядра ОАИС, либо на АРМ АЗ. Выбор места ведения журналов производится при развертывании ядра ОАИС. Аудит событий ОС осуществляется службой журналирования Linux. Журналы аудита могут вестись как непосредственно на каждой ПЭВМ, так и на сервере аудита (в качестве сервера аудита может быть использовано АРМ АЗ). Оповещение АЗ о событиях аудита реализуется с использованием программы анализатора журналов ОС Linux. В части организации аудита ПО АРМ АЗ обеспечивает:

– настройку состава данных аудита безопасности;

– доступ ко всем журналам аудита;

– отображение сообщений оповещения о событиях аудита.

Администрирование подсистемы защиты информации осуществляет администратор защиты информации системы с помощью программных средств АРМ АЗ. Администратором защиты выполняются следующие функции:

– администрирование МСЭ;

– администрирование средств защиты на http-сервере;

– администрирование полномочий доступа к веб-сервисам;

– мониторинг событий безопасности;

– управление аудитом событий безопасности;

– управление средствами контроля целостности.

Администрирование МСЭ включает управление средствами защиты от внешних и внутренних сетевых атак. Администрирование средств защиты на http-сервере включает:

– настройку работы протокола TLS;

– обновление базы сигнатур вредоносных программ.

Администрирование полномочий доступа к веб-сервисам включает определение групп пользователей, которым разрешен доступ к каждому веб-сервису, из числа зарегистрированных в ядре ОАИС и назначение соответствующих полномочий по доступу в OID. Мониторинг событий безопасности включает настройку перечня событий, о которых осуществляется оповещение, анализ оповещений о нарушениях безопасности, анализ данных аудита. Управление аудитом событий безопасности заключается в настройке перечня регистрируемых событий и периодическом архивировании журналов аудита.

Управление средствами контроля целостности включает:

– настройку перечня контролируемых файлов;

– настройку периодичности контроля целостности;

– формирование эталонных значений целостности по необходимости.

Антивирусная защита осуществляется на всех серверах ядра ОАИС с использованием программных средств, сертифицированных Оперативно-аналитическим центром безопасности информации при Президенте Республики Беларусь.

UDC 621.396.677

PLANAR MICROSTRIP ANTENNA ARRAYS WITH ONE-DIMENSIONAL SCANNING

O.A. YURTSEV[1], N.M. NAUMOVICH[1], JIANG BO[2], MA TONG BIAN[2], CHENG HUI BIN[2]

[1]*Belarusian State University of Informatics and Radioelectronics*
6, Brovki Str., Minsk, 220013, Republic of Belarus

[2] *North-China Electromagnetic Protection Research Institute*
No. 68, Changfeng Str., Taiyuan, Shanxi 030006, China

A scheme for constructing, radiator design and the results of numerical modeling of planar microstrip antenna array with one-dimensional by electrical scanning are described.

Keywords: microstrip antenna array, numerical simulation, one-dimensional scanning.

Introduction

In surveillance radar stations (radars) electrical scanning is usually done one-dimensional. If the scanning plane is vertical, the radar identifies two angular coordinates of some aerodynamic object. In the vertical plane it is done by electrical scanning and in a horizontal plane with the mechanical rotation of the antenna. If electrical scanning is used to determine the angular ordinates in the horizontal plane, the vertical angular coordinate of the object is not defined. In this case, the width of the main lobe (ML) angular pattern (AP) in the vertical plane ($2\theta^{v}_{0,5}$) is selected from the tactical considerations.

Typically, the $2\theta_{0,5}^{y}$ value is equal to 5° -8°. In some cases, the AP in the vertical plane is as "Cosecant" type. Array with electrical scanning in one plane and having a predetermined width of AP ML is described in the article. Array itself is a linear antenna array of microstrip radiators, arranged along the Y axis. Each radiator, in turn, is a linear array antenna of microstrip rectangular radiators arranged along the X axis. All linear antenna array radiators (planar array lines) are sequentially excited by a microstrip line. Planar antenna array of three lines is shown schematically in Fig.1. The dots indicate the place of linear antenna arrays excitation. In the illustrated planar antenna array electrical scanning is performed in the *YZ* plane. For the array shown in Fig. 1, the plane *YZ* is an E plane; plane XZ is an N plane. There may be other polarization variants.

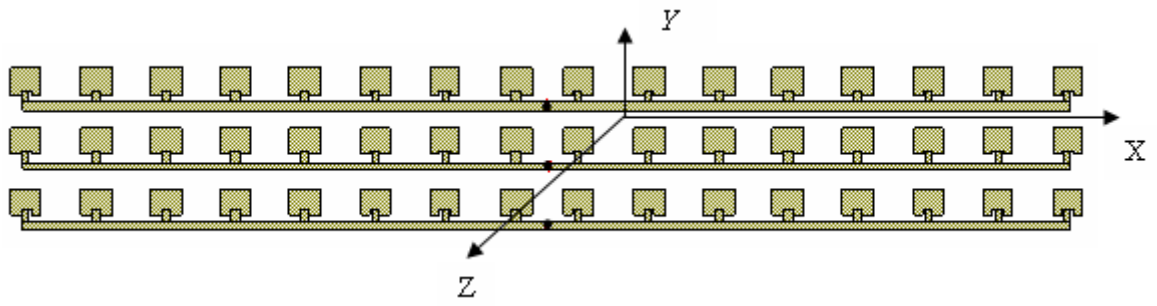


Fig. 1. Planar microstrip antenna array

The results of different variants of linear antenna arrays with consistent power supply circuit numerical modeling are given in the article. Software Microwave Office (MWO) for electro-dynamic modeling is used. Planar antenna array simulation when scanning along *Y* axis (vertical plane) is implemented with using the multiplication angular patterns theorem. MWO software is used in the analysis of the planar array to account the relationship influence between each line but no more than 11. While angular pattern of the planar antenna array line in the vertical plane taking into account interrelationship calculated in MWO was approximated.

1. Linear microstrip array modeling

A number of options for linear microstrip antenna arrays are considered. Fig. 2 shows the linear microstrip antenna array consisting of N=8 rectangular shape radiators. Character 1 indicates the excitation location by perpendicular probe. Dimensions *A, B, Dx* and substrate parameters indicate angular pattern and array integration in a given frequency range. The "C" elements are intended to adjust the array by the frequency integration.

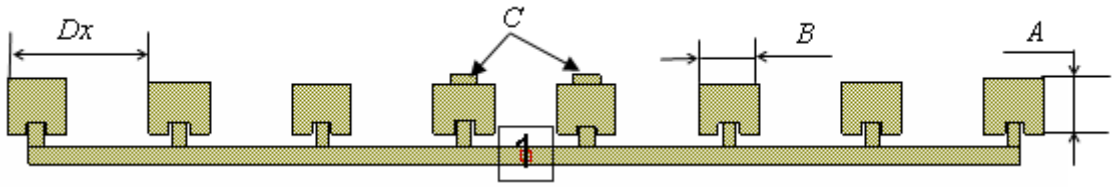
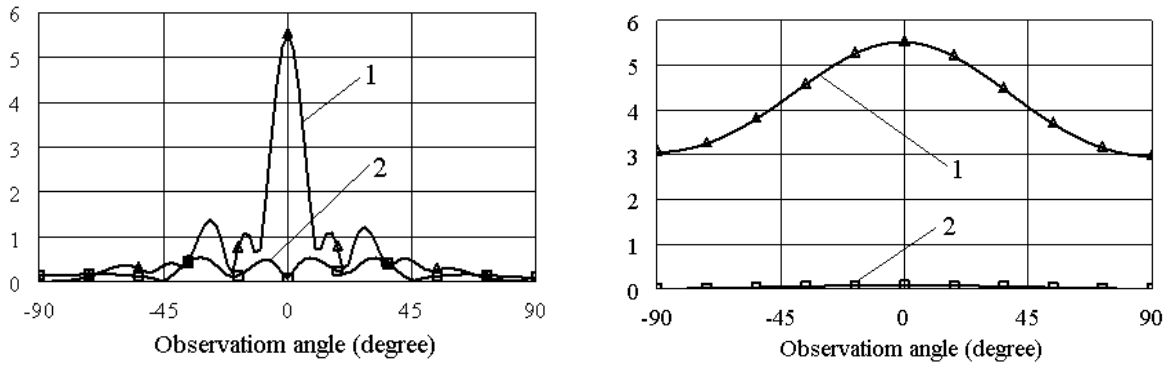


Fig. 2. Microstrip linear antenna array

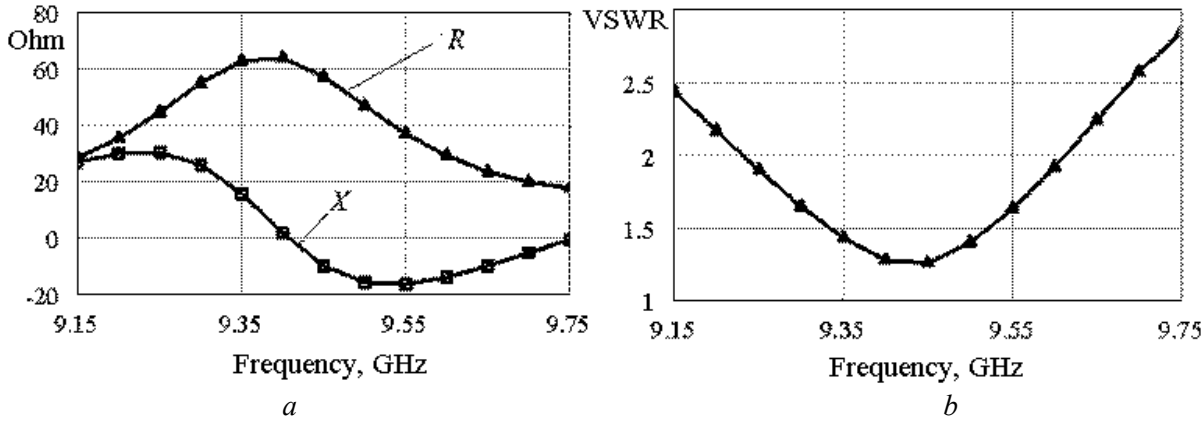
Figure 3 shows the non-normalized angular patterns (AP) in the plane H: (*a*); in the plane E: (b) on a main (1) and cross-polarization (2) for array, designed for the average frequency f = 9.4 GHz. Elements sizes are: A = 7.5 mm, B = 9 mm; Dx = 21,5 mm.



a *b*

Fig. 3. Array angular patterns in two planes:
a – *H* plane (*XZ*): *b* – *E* plane (*YZ*); frequency f = 9.4 GHz

Figure 4 shows the dependence of the active and reactive parts of the input impedance *(R, X)* and the standing wave ratio (VSWR) from the frequency.



a *b*

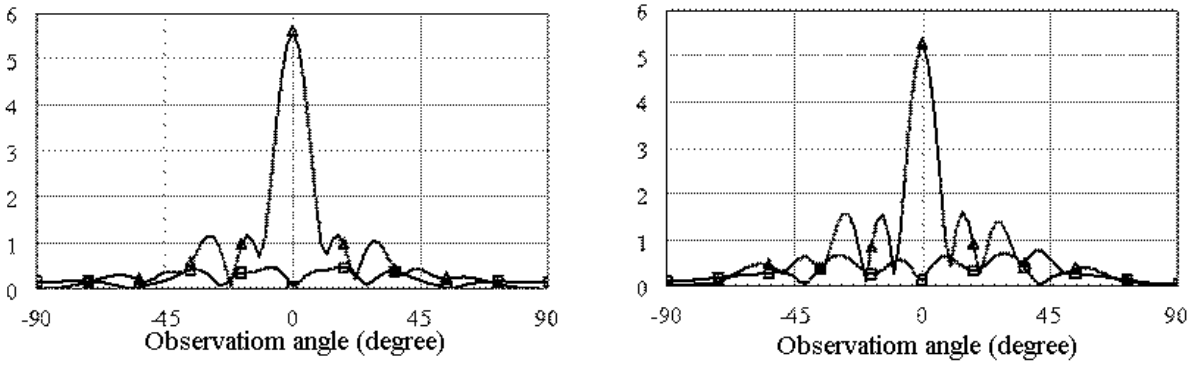
Fig. 4. Impedance (*a*) and VSWR (*b*) depending on the frequency

As can be seen from the Figure, the array is excited at the center, i.e. consists of two identical parts. In each part the radiators are excited sequentially from the microstrip transmitter line. The distance between the transmitters at the center frequency is chosen so that the neighboring radiators were placed at wavelength in the transmission line. In this case, all the radiators are excited in phase. On deviation frequency from the mean for each half of the array linear phase angular distribution is set, the main lobe of the AP is deviated to phase downward on array, but on different sides to the normal. As a result, angular pattern main lobe (ML) deviates from the normal to the array, but on the ML operating frequency range borders extends and can split in two. To illustrate this, Fig.5 shows the array AP (Fig. 2) at frequencies corresponding to VSWR=2.

The width of the AP main lobe in the plane H ($2\theta^{h}_{0,5}$) depends on the number of radiators in the array. When the number of the vibrators is from 4 to 16 $2\theta^{h}_{0,5}$ value of the on the

average frequency varies from 20° to 5°. The maximum side lobe level remains at (–13...–14) dB. This level can be somewhat reduced (at 1–2 dB) by mismatch radiators located at the edges of the array. This decreases the amplitude of the excitation.

Figure 3*a* and Figure 5 shows that the field cross-polarization level in the *H* plane is approximately –20 dB. This level can be reduced by 2–4 dB, cutting slits at the radiators perpendicular to the currents, creating field cross-polarization component. Figure 6 shows a fragment of an array and its AP in the *H* plane for an average frequency of 9.4 GHz (the number of radiators in the array $N = 8$ in the same way as in Fig. 2.) Figure 6 should be compared with the Figure 3*a*.



a b

Fig. 5. Angular pattern at frequencies 9.2 GHz (a) and 9.6 GHz (b)

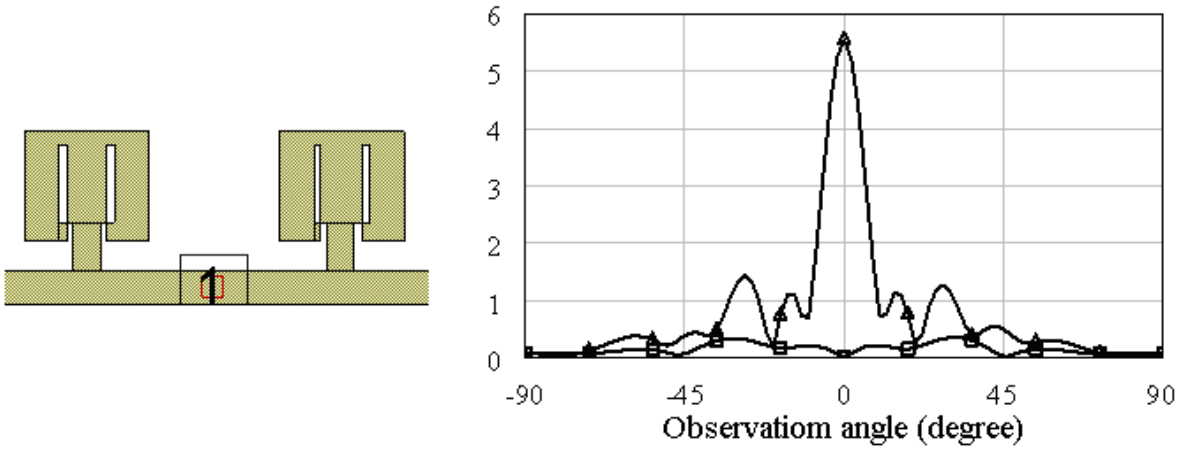


Fig. 6. Array with a cross-polarization reduced level radiation

Angular pattern of N-line in planar antenna array (Fig.1) in the *E*-plane based on the number of rows in the array (Ny), and the distance between lines (Dy). AP Change associated with the mutual influence of the lines. With the increasing number of rows to 7–9 AP change increases in this plane in comparison to the AP of one isolated row (linear array) shown in Fig. 3*b*. Mutual influence is increased with decreasing the distance between adjacent rows of a planar array. AP in the plane *E* is weakly dependent on the number of radiators in each row (Nx). Figure 7 shows AP in E-plane of antenna array with the number of rows Ny = 9 and the number of radiators in row Nx = 4. An array is also shown schematically. The distance between adjacent array rows is Ny = 17 mm. This AP provides electrical scanning of E-plane

with sector angles of –45°...45° with almost no changes in the array antenna gain coefficient (AGC) due to unevenness of the AP in one row in this plane. Figure 8 shows the dependence of the coefficients of the power transmission from input 1 to inputs 2, 3, 4, 5 (denoted by the symbols S12, S13, S14, S15).

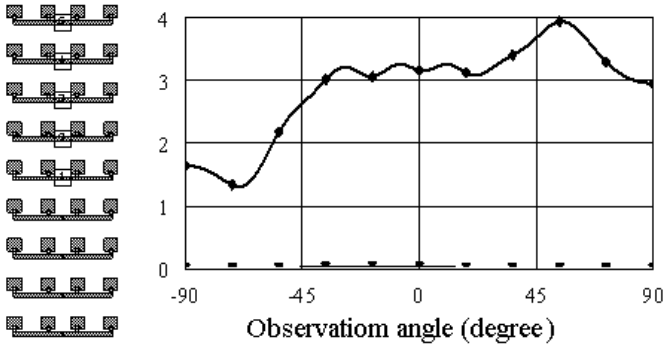


Fig. 7. Planar array and its AP in E-plane

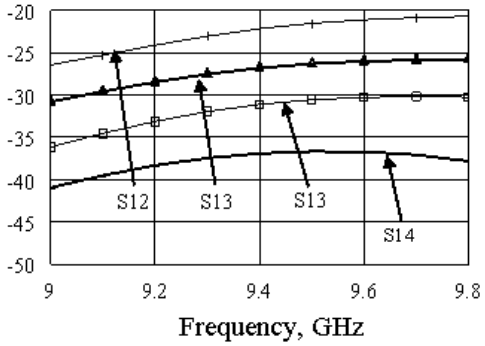
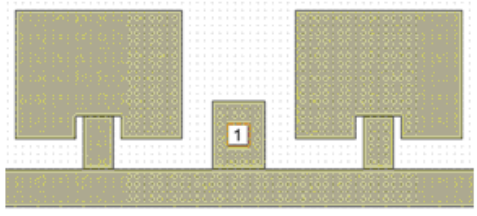


Fig. 8. Transmission coefficients

Revised array is very narrow-band as agreed. Fig.4b implies that the relative frequency band VSWR ≤ 2 is 3.7% is $\delta f = 2\dfrac{f\,max - f\,min}{f\,max + f\,min}100\% \approx$. Widening frequency band is possible in case of changing the point of linear array (row) excitation. Figure 9 shows the middle part of one of the variants and the dependence of the VSWR from such linear array frequency. Radiators sizes and their number is the same as in Figure 2. Figure 9 shows that the relative bandwidth is $\delta f \approx 14$ %.



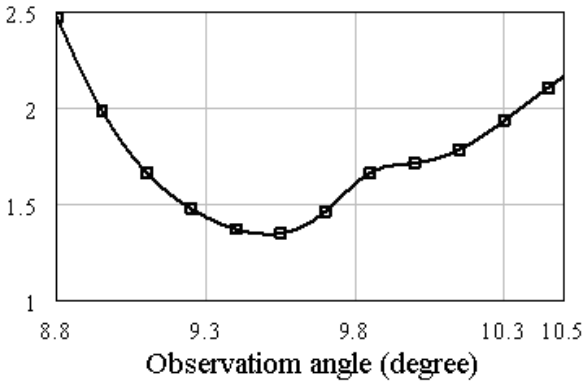


Fig. 9. Array with extended bandwidth as agreed

As with the frequency deviation from the average, as previously mentioned, the phase distribution in the two halves of the row become linear; array in bandwidth, in terms of saving the AP form Fig.9 is less than as agreed. By resizing some radiators a relative bandwidth by AP shape retention and agreement of approximately $\delta f \approx 10\%$ can be provided.

2. Planar microstrip array modeling

Onwards there are the results of the planar array simulation, consisting of a linear Ny microstrip arrays (rows), discussed above. Simulation results of such arrays in the MWO software are used. Angular pattern in the YZ-plane (E-plane) is calculated using AP multiplying theorem [1]:

$$f(\theta) = f_1(\theta) \cdot f_c(\theta), \quad (1)$$

Where $f_1(\theta)$ is one row AP in E-plane taking into account interaction between the rows

$f_c(\theta)$ is array system multiplier in E-plane:

$$f_c(\theta) = \left| \sum_{n=1}^{Ny} Any \cdot e^{i\Psi ny} e^{ik \cdot Dy \cdot \sin\theta} \right|. \quad (2)$$

In equation (2) the following values are:

Any – the excitation row normalized amplitude with number *n* (amplitude distribution);

Ψny – row excitation phase with number *n* (phase distribution);

θ – угол наблюдения, отсчитываемый от нормали к плоскости решетки;

$k = \frac{2\pi}{\lambda}$ – Free space wave number, λ – wavelength.

Equation (1) does not account boundary effects in the array and is therefore approximate.

Figure 10 shows the calculated average frequency of AP in the E-plane for the array with parameters Dy = 7, Ny = 32. Two scanning angles are 0 and 45°. Excitation amplitude distribution is done falling to the ends of the array according to cosine-law to the power P = 2 to the level of 0.2 at the ends of the array (at the top and bottom row).

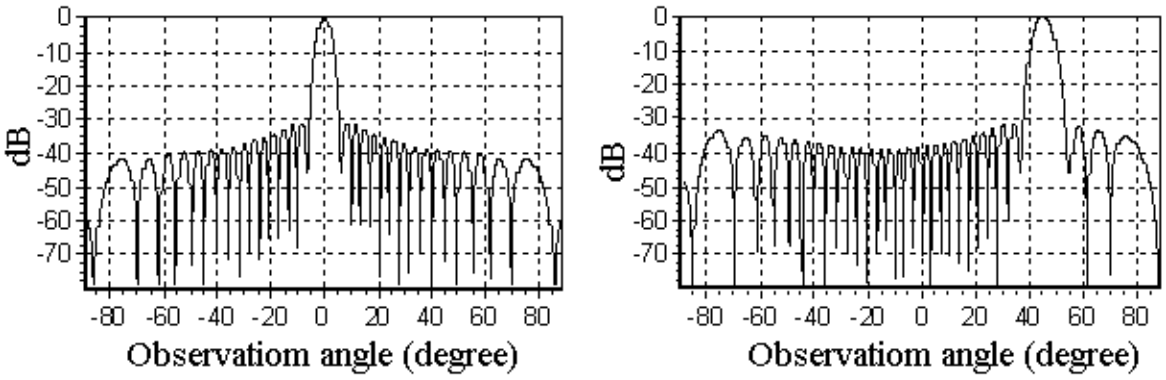


Fig. 10. Plane array AP in the E-plane

The side lobes level in the array substantially depends on random errors of radiators excitation in amplitude and phase. This pattern is illustrated in Fig.11, which shows the random realization of the same AP (see Figure 10), but with a maximum error of rows excitation at 20 % amplitude and phase of 20°.

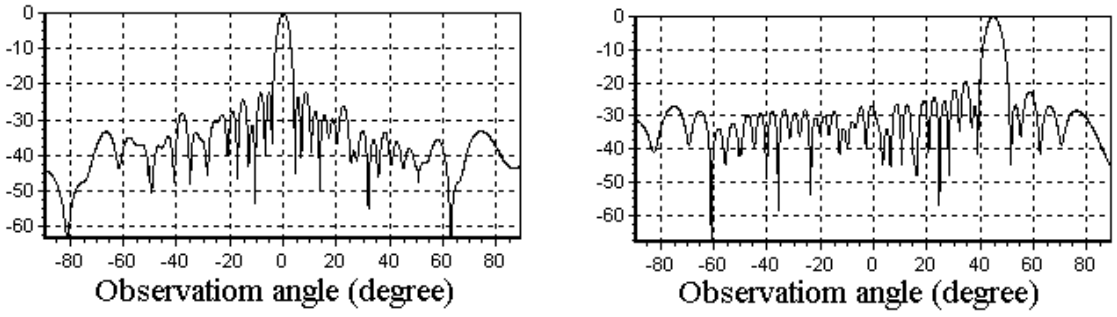


Fig. 11. Random AP implementation at two scanning angles with respect to rows random excitation errors in amplitude (20 %) and phase (20°)

As can be seen, the side lobes increased by almost 10 dB. The requirements for the side lobes level in the scanning plane accuracy requirements and implementation of the array structure and amplitude-phase distribution of radiators excitation in the scanning plane arise.

3. Conclusion

A numerical simulation of planar array in which rows are linear array of rectangular microstrip radiators excited sequentially from the microstrip line. Moreover, the case of polarization when the electric field vector is perpendicular to the line location radiators is studied.

Numerical simulation of a linear array (rows) showed that when the excitation of the array in the center can provide a VSWR < 2 in the frequency band of about 15%. In a somewhat narrow bandwidth (approximately 10 %) angular pattern in the plane of the radiators location retains its shape: the main lobe is perpendicular to the axis of the array, the side lobes do not exceed the values of –13 dB. If in such an array plane of polarization is perpendicular to the line location of microstrip radiators field level by cross-polarization in the E-plane is very low (–50...–70 dB). Angular pattern in this plane substantially depends on the number of rows (linear arrays) in a planar array. When the number of rows is more than 8-9 and the distance between lines is about 0,5 λ, than field in the main lobe in the sector of angles 45° varies slightly, allowing the possibility of wider scanning in this plane. In the H-plane field level in the cross-polarization is (–20...–24) dB side lobes level is (–13...–14) dB. Angular pattern in this plane is almost independent of the number of rows in the array.

Studied linear microstrip radiators antenna array with sequence power supply circuit is convenient as it combines radiators system itself and their excitation system. This allows simplifying the overall structure of the planar array with the one-dimensional scanning and lowering its cost. In particular, there is no need to make a linear microstrip array (planar array radiator) two-layered with placing radiators system at one layer and a feed net system on a different layer.

Numerical simulations of other variants of microstrip linear antenna arrays with consistent power supply circuit, used in planar antenna array with one-dimensional scanning were conducted. Variants in which the electric field vector is oriented along the line of radiators location and dual-polarization array were also included and discussed. The main problem in all the versions is the problem of the side lobes in the plane of the radiators location and the relatively high field level of cross-polarization in this plane. Side-lobe level less than (14...15) dB in said plane cannot be received.

References

1. *Ямайкин В.Е., Северьянов В.Ф., Кишкунов В.К., Рунов А.В.* Антенные устройства. Мн.: МВИРТУ, 1965, 529 с.