ment of Television and Sound-broadcasting, PhD in Technical Science. Tel.: +74959577708. E-mail: andrey_sam@mail.ru

References

1. Smirnov A.V., Peskin A.E. Cifrovoe televidenie: ot teorii k praktike [Digital TV - from theory to practice]. Moscow, Goryachaya liniya – Telekom Publ., 2005. 352 p.
2. Preobrazovanie standartov. Primenenie texnicheskix reshenij [Convert standards. The use of engineering solutions]. «625», 2005, no.7, 79 p.
3. Bezrukov V.N., Balobanov V.G. Sposob peredachi dopolnitel'noj informacii v polose chastot televizionnogo signala [Method for transmitting additional information in the frequency band of the television signal]. Copyright certificate USSR, no. 586572, 1977.
4. Bezrukov V.N., Balobanov V.G. Sposob peredachi dvuh televizionnyh program po odnomu kanalu svyazi [Method for transmitting two television programs on one channel]. Copyright certificate USSR, no. 484655, 1975.
5. Bezrukov V.N., Balobanov V.G. Sistemy cifrovogo veshchaniya i prikladnogo televideniya [System's digital broadcasting and television application]. Moscow, Goryachaya liniya – Telecom Publ., 2015. 600 p.
6. Hu. S., Zhang. X., Yang.Z. Efficient Implementations of interpolation for AVS. Congress on image and signal processing, 2008, vol. 3, pp. 133-138. doi: 10.1109/CISP.2008.58.
7. Sullivan G.I. Thomas Wiegand Video compression- From Conserts to the H.264/AVC Standart. Proc. of the IEEE 2004, vol. 93, pp. 18-31. doi: 10.1109/JPROC.2004.839617.
8. Prett U. Metody peredachi izobrazhenij. Sokrashchenie izbytochnosti [Image transfer techniques. Reduced redundancy]. Moscow, Radio and Communications Publ. 1983. 264 p.
9. Verner M. Osnovy kodirovaniya: uchebnik dlya vuzov [Basics of coding: Textbook for Universities, Translated from the German Zigangirova D.K.] Moscow, Tehnosphere Publ., 2005. 320 p.
10. Selomon D. Szhatie dannyh, izobrazhenij i zvuka: uchebnoe posobie dlya vuzov [Data compression, image and sound]. Moscow, Tehnosphere Publ., 2004. 368 p.
11. Richardson Jan, Videokodirovanie. N. 264 i MPEG-4 – standarty novogo pokoleniya [Video coding H.264 and MPEG-4 next generation standards]. Moscow, Tehnosphere Publ., 2005. 368 p.
12. Morelos-Sarogossa R. Iskusstvo pomekhoustojchivogo kodirovanija. Metody, algoritmy, primenenie [Art error-correcting coding. The Methods, algorithms, applications] Moscow, Tehnosphere, 2005. 320 p.

Received 09.01.2017

ЭЛЕКТРОМАГНИТНАЯ СОВМЕСТИМОСТЬ И БЕЗОПАСНОСТЬ ОБОРУДОВАНИЯ

УДК 004.056.52+004.413.2

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И УПРАВЛЕНИЕ РАЗРЫВОМ КАНАЛА ПЕРЕДАЧИ В СЕАНСНОМ РЕЖИМЕ

Мостовой Я.А., Слепушов И.И.
Поволжский государственный университет телекоммуникаций и информатики, Самара, РФ
E-mail: slepushovii@gmail.com

Рассматривается метод противодействия угрозам информационной безопасности с автономным управлением физическим разрывом канала передачи данных по защищенному расписанию. Метод рассмотрен в рамках концепции эшелонированной обороны и подходит для многих компьютеризированных систем, для которых достаточно эпизодических связей с сетевыми структурными элементами или пользователями услуг. В этом случае доступ защищаемого узла к сети необходим и достаточен в сеансном режиме – в определенные и ограниченные интервалы времени, между которыми доступ может отсутствовать. Метод имеет самостоятельное значение как еще один эшелон обороны, но при этом повышает эффективность применения других методов эшелонированной обороны, вероятность преодоления которых зависит от времени нахождения защищаемого узла под возможными атаками или наблюдением. Проведена оценка эффективности рассматриваемого метода. Для реализации данного метода написано клиент-серверное программное обеспечение на C#.

Ключевые слова: защита информации, эшелонированная оборона, вероятность преодоления защиты, закрытое расписание, время нахождения под наблюдением

Введение

В связи со стремительным ростом угроз информационной безопасности улучшение защиты информации является актуальной и важной задачей для обеспечения беспроблемной производственной деятельности любой компании, обеспечения безопасной работы любой системы, управляемой от компьютера.

Для защиты от этих угроз разработано и применяется много эффективных методов и средств: идентификация и аутентификация, управление доступом, шифрование и экранирование, антивирусное программное обеспечение (ПО), межсетевые экраны, IDS (системы обнаружения вторжений), пакетные фильтры, прокси-серверы и т.п. [1]. Каждый из этих методов защиты имеет свои уязвимости и может быть взломан с течением времени.

В мире ИТ не существует «главного» и непреодолимого средства защиты, и стратегия обеспечения информационной безопасности – стратегия эшелонированной обороны [2]. Эшелонированная защита - эффективный способ борьбы с многонаправленными постоянно меняющимися опасностями в современной информационной среде, а также с неуверенностью в достаточной эффективности средств защиты через некоторое время их эксплуатации.

Эшелонированная защита – концепция, предназначение которой предоставлять «избыточную» многоуровневую защиту компьютерной системы для сохранения безопасности в случае неисправности, или преодолении одного или нескольких из эшелонов системы защиты, или при предположении наличия в одном или нескольких из эшелонов некой уязвимости, которая может быть использована злоумышленником [3].

Большинство из рассмотренных угроз безопасности идет из сети Internet. Угрозы, идущие из Internet, связаны с утратой конфиденциальности важной информации, возможностями ее зловредного искажения и воровства, прекращением нормального функционирования систем. Реализация этих угроз требует во многих случаях доступа злоумышленника в течение достаточно длительного интервала времени к атакуемому узлу для подбора паролей, сканирования жестких дисков с целью поиска плохо защищенных файлов и каталогов, для внедрения и запуска троянских программ, вирусов и т.п. атак на уровне ОС, сетевого и прикладного ПО.

Самый радикальный способ защиты от этих угроз – отключить защищаемые компьютеры от сети. Однако это сразу уменьшает возможности системы, в которой установлен компьютер, так как для большинства систем необходим для функционирования сетевой обмен информацией с удаленными и структурными элементами систем, респондентами и пользователями услуг.

Разрыв сетевого канала передачи информации по защищенному расписанию

Исходя из вышеизложенного, в работе рассмотрен универсальный и кардинальный метод защиты информации с автономным управлением физическим разрывом канала передачи данных по защищенному расписанию в качестве еще одного из эшелонов защиты.

Для функционирования многих компьютеризированных систем достаточно эпизодических связей со структурными элементами по сети или пользователями услуг. В этом случае доступ узла к сети необходим и достаточен в сеансном режиме – в определенные и ограниченные интервалы времени, между которыми связь может отсутствовать. Для таких систем в те моменты времени, когда нужды в связи нет, защищаемый узел может быть физически оторван от сети.

Для сохранения возможности полудуплексной связи абонентов с использованием Internet разрыв и подключение сетевого канала абонентом предлагается проводить по расписанию, уменьшая шансы злоумышленника на несанкционированный доступ к информации. Еще большей защищенности можно добиться, сделав это расписание секретом, известным только взаимодействующим абонентам или абоненту, который хочет подключаться к Интернет в моменты времени, неизвестные потенциальным злоумышленникам.

Этот доступ можно автоматизировать, разработав соответствующее программное обеспечение для передачи по закрытому каналу расписания сеансов связи данного узла с Internet и управления подключением к сети в соответствии с данным расписанием. Эффективность данного способа защиты будет тем выше, чем меньше время нахождения защищаемого узла в состоянии подключения к среде Internet. Будучи самостоятельным средством защиты, данное средство увеличивает эффективность уже существующих средств защиты от угроз, зависящих от времени пребывания защищаемого узла в доступном для

атак состоянии под наблюдением возможных злоумышленников.

Классификация этих угроз может быть проведена. Примеры угроз, реализация которых зависит от времени доступа (наблюдения) к объекту:

1. Перебор пароля (bruteforce). Вероятность реализации данной атаки зависит не только от сложности используемого пароля, но и от времени, в течении которого злоумышленник будет иметь доступ к взламываемому объекту, для подстановки различных комбинаций пароля [4-8].

2. Сетевая разведка – получение и обработка данных об информационной системе, ресурсов информационной системы, используемых устройств и программного обеспечения и их уязвимости, средств защиты, а также о границе проникновения в информационную систему. Чем меньше время доступа к объекту, тем труднее собрать информацию о нем [4-8].

3. Сетевой червь. Вероятность заражения (скорость распространения) данной вредоносной программой также может быть уменьшена за счет сокращения времени подключения компьютера к сети передачи данных [4-8].

4. DoS и DDoS - это атаки на вычислительную систему, основной целью которой является невозможность получить доступ к предоставляемым системным ресурсам (серверам). В связи с тем, что расписание подключения узла к сети передачи данных злоумышленнику не известно, совершение такого вида атаки на узел сети может быть затруднено [4-8].

Определение эффективности предлагаемого метода

Будем оценивать эффективность защиты вероятностью ее непреодоления P за заданное время. В случае эшелонированной обороны обозначим P_i – вероятность непреодоления i-го эшелона защиты, тогда вероятность преодоления i-го защитного барьера:

$$Q_i = 1 - P_i. \qquad (1)$$

Составим схему эшелонированной обороны (рис. 1).

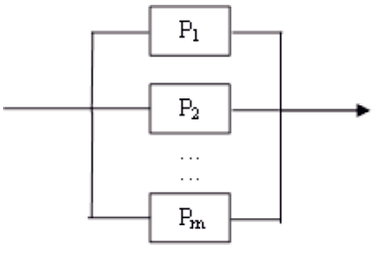

Рис. 1. Схема эшелонированной обороны

Защита будет преодолена, если будут преодолены все m параллельные защитные барьеры (i = 1…m):

$$Q_\Sigma = \prod_{i=1}^{m} Q_i = \prod_{i=1}^{m} (1 - P_i). \qquad (2)$$

Надежность обороны – вероятность ее непреодоления P_Σ:

$$P_\Sigma = 1 - \prod_{i=1}^{m} (1 - P_i). \qquad (3)$$

Рассмотрим три вида защитных барьеров:

1) Защитные барьеры, вероятность неопреодоления (преодоление) которых не зависит от t - времени нахождения компьютера в подключенном состоянии к сети (времени нахождения под возможными атаками или временем наблюдения). Пусть таких барьеров всего n.

2) Защитные барьеры, вероятность преодоления которых зависит от времени нахождения в подключенном состоянии компьютера к сети (времени нахождения под возможными атаками или временем наблюдения). Пусть таких барьеров всего k.

3) Дополнительный защитный барьер, связанный с отключением компьютера от сети передачи данных и подключении его в сеансе связи по закрытому расписанию. Характеристика этого расписания – относительное время подключенного к сети состояния

$$\gamma = \frac{t_{подкл.сост.}}{t}. \qquad (4)$$

Это же значение γ есть не что иное, как вероятность преодоления данного дополнительного защитного барьера Q_3.

Здесь (4) $t_{подкл.\ сост.}$ – время нахождения компьютера в подключенном состоянии к сети (времени нахождения под возможными атаками или временем наблюдения).

Тогда схема эшелонированной обороны примет вид рис. 2.

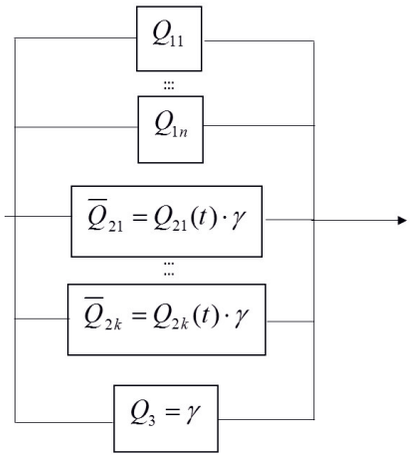

Рис. 2. Схема эшелонированной обороны с временным отключением узла от сети

С учетом влияния времени отключения узла от сети на эшелоны защиты вида 2 имеем:

$$Q_{\Sigma} = \prod_{i=1}^{n} Q_{1i} \cdot \prod_{i=1}^{k} (Q_{2i} \cdot \gamma) \cdot \gamma = \prod_{i=1}^{n+k} Q_i \cdot \gamma^{k+1} \quad (5)$$

$$P_{\Sigma} = 1 - (\prod_{i=1}^{n+k} Q_i) \cdot \gamma^{k+1}. \quad (6)$$

Отсюда видно, что, выбирая γ достаточно малым, порядка γ = 0,001, можно достаточно сильно увеличить P_{Σ} (уменьшить Q_{Σ}), особенно в случаях, когда $k > 2$.

В предельном случае, когда k=0 (нет барьеров, вероятность преодоления которых зависит от времени нахождения под возможными атаками):

$$P_{\Sigma} = 1 - (\prod_{i=1}^{n} Q_i) \ \gamma. \quad (7)$$

Если обозначить α повышение эффективности защиты всей системы от использования дополнительного эшелона защиты через управляемое автономное отключение узла от сетевого канала как отношение вероятности преодоления защиты после применения метода к вероятности преодоления защиты до применения метода, то получим:

$$\alpha = \frac{\prod_{i=1}^{n} Q_{1i} \ \prod_{i=1}^{k} Q_{2i} \ \gamma^{k+1}}{\prod_{i=1}^{n} Q_{1i} \ \prod_{i=1}^{k} Q_{2i}} = \gamma^{k+1}. \quad (8)$$

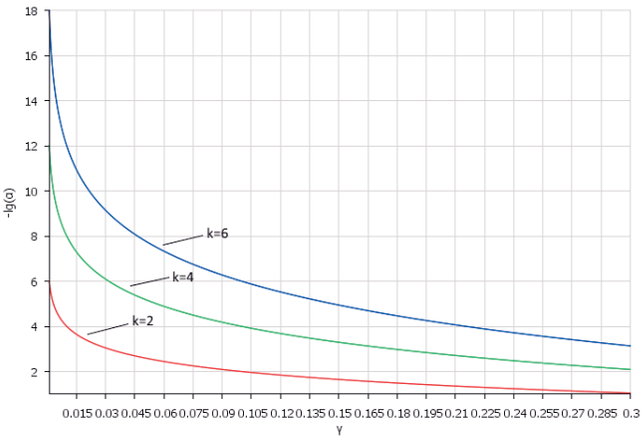

Рис. 3. Изменение эффективности защиты в зависимости от относительного времени нахождения компьютера в подключенном к сети состоянии γ

Например, для $\gamma = 0{,}1$ и $k = 4$ вероятность преодоления защиты уменьшится в 10^5.

Можно полагать, что, когда система имеет доступ к сети Internet, можно пытаться взломать и данный уровень защиты, взлом которого примерно такой же сложности, как и для остальных эшелонов защиты. Но время доступа к нему, для изучения его работы гораздо меньше, чем для других методов.

Программная реализация и аварийная защита

Разработано клиент-серверное программное обеспечение, реализующее данный метод [9]. Данное ПО функционирует автономно, создавая препятствие, преодоление которого сопряжено с возникновением сложностей для злоумышленника или дестабилизирующего фактора (рис 4).

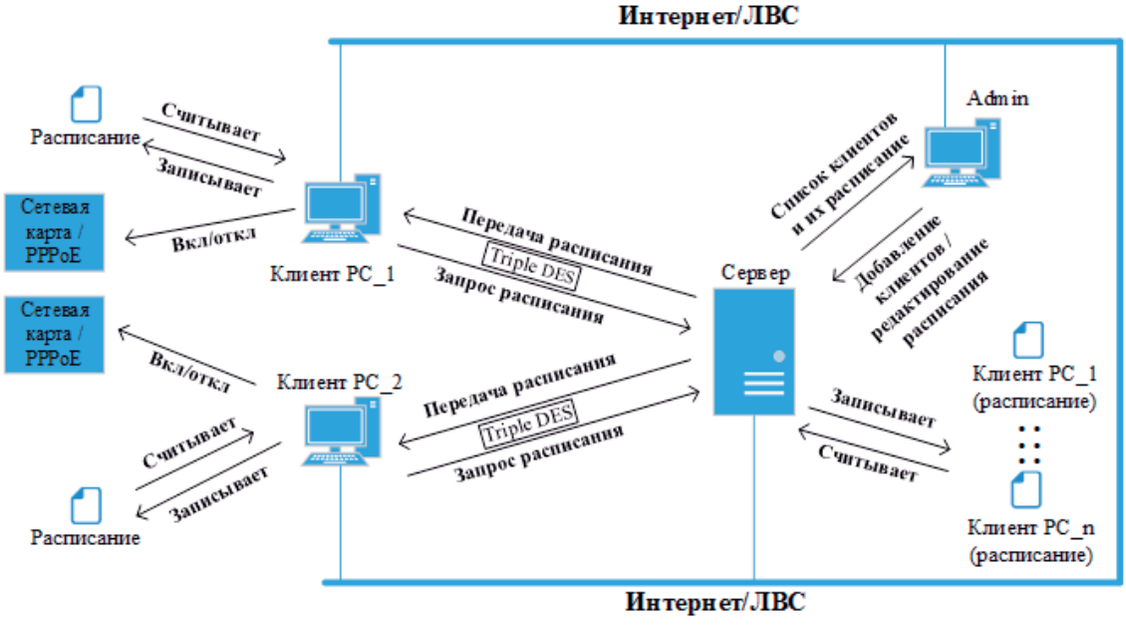

Рис. 4. Схема работы ПО, реализующего рассмотренный метод

Клиент при подключении к серверу получает расписание $t_{обнов}$, по которому он будет осуществлять переключение сетевой карты. Расписание клиента на сервере хранится в файле с «уникальным» именем. Для каждого клиента свой файл.

Хранение расписания и передача информации между всеми сетевыми компонентами предлагается осуществлять в зашифрованном виде по алгоритму Triple DES [10].

Все манипуляции с клиентами, а также редактирование их расписания работы осуществляется из отдельного программного модуля администратора.

У клиента предполагается разработка необходимого функционала по восстановлению связи с сервером в случае отсутствия связи в установленное по расписанию время с таковым по каким-либо техническим причинам.

Также планируется добавление поддержки отключения и включения не только сетевой карты, но и PPPoE соединения с помощью библиотеки DotRas.

Для аварийного включения сетевой карты, в случае когда основная программа-клиент не включила ее по расписанию, предусмотрена специальная служба. Если по истечении заданного времени $t_{авар}$ ($t_{авар} > t_{обнов}$) сетевая карта не включится, служба сама ее включит и удалит расписание клиента. Счетчик времени $t_{авар}$ восстанавливает свое исходное значение каждый раз при переключении сетевого адаптера.

Заключение

1. Для функционирования многих компьютеризированных систем достаточно эпизодических связей компьютера со структурными элементами или пользователями услуг по сети Интернет. В этом случае доступ рабочей станции к сети возможен в сеансном режиме – в определенные и ограниченные интервалы времени, между которыми связь может отсутствовать.

2. Для улучшения защиты информации и сохранения возможности полудуплексной связи абонентов с использованием Internet разрыв и подключение сетевого канала абонентом предлагается проводить по внутреннему расписанию, являющимся секретом, известным только взаимодействующим абонентам.

3. Разработано соответствующее программное обеспечение для передачи по закрытому каналу расписания сеансов связи данного узла с Интернет и управления подключением к сети в соответствии с данным расписанием.

4. Будучи самостоятельным средством защиты, данный метод одновременно увеличивает эффективность уже существующих средств защиты от угроз, зависящих от времени пребывания защищаемого узла под наблюдением возможных злоумышленников.

Литература

1. Хорев А.А. Угрозы безопасности информации // Специальная техника. – М.: 2010. – № 1(67) – С. 50 - 63.
2. Мостовой Я.А., Слепушов И.И. Повышение информационной безопасности путем управления физическим разрывом канала передачи // Материалы XXIII Российской научн. конф. ППС, НС и аспирантов. ПГУТИ, 2016. – С. 264 - 265.
3. Исаев А.Б. Современные технические методы и средства защиты информации: учебное пособие – М., РУДН, 2008. - С. 258.
4. Барышников А.А., Исаев И.А. Моделирование вероятности взлома системы информационной безопасности // Горный информационно-аналитический бюллетень. – М.: 2010. – № 5 – С. 152 - 155.
5. Mark Rhodes-Ousley. Information Security The Complete Reference, Second Edition. McGraw-Hill Education, 2013. – 306 p.
6. P.W. Singer, Allan Friedman. Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press, 2014. – 101 p.
7. John Fay. Contemporary Security Management, Third Edition. Butterworth-Heinemann, 2010. – 56 p.
8. Загинайлов Ю.Н. Теория информационной безопасности и методология защиты информации: учебное пособие / Ю. Н. Загинайлов. – М.-Берлин: Директ-Медиа, 2015. - С. 124-170.
9. Мостовой Я.А., Слепушов И.И. Программа управления доступом компьютеров к сети в сеансах связи по изменяемому закрытому расписанию // Свидетельство о регистрации программы на ЭВМ. № 2016662289, 2016.
10. Купцевич Ю.Е. Альманах программиста: Безопасность в .NET, Шифрование, Защита кода и данных. / Ю. Е. Купцевич – М.-Русская редакция, 2004. – С. 174 – 261.

Получено 21.12.2016

Мостовой Яков Анатольевич, проф., д.т.н., профессор Кафедры программного обеспечения и управления в технических системах (ПОУТС) Поволжского государственного университета телекоммуникаций и информатики (ПГУТИ). Тел. 8 (846) 228-00-13; E-mail: jakob.mostovoi@yandex.ru

Слепушов Илья Игоревич, магистрант Кафедры ПОУТС ПГУТИ. Тел.: 89277552321; E-mail: slepushovii@gmail.com

INFORMATION SECURITY AND CONTROL OF TRANSMISSION CHANNEL BREAKING IN THE SESSION MODE

Mostovoi J.A., Slepushov I.I.
Povolzhskiy State University of Telecommunication and Informatics, Samara, Russian Federation
E-mail: slepushovii@gmail.com

A countermeasure for information security threats with autonomous controlling of physical disruption of data transmission channel is considered, according to a secure schedule. The method is effective within a concept of the defense in depth and is suitable for many computerized systems, which have sufficient amount of episodic communications with network structural elements or service users. In this case, the protected node access to the network is necessary and sufficient in the session mode in specific and limited intervals of time, between which access may be absent. The method has an independent significance, as another level of defense, but in these conditions, it increases the effectiveness of other methods of the defense in depth, the probability of overcoming them depends on the time of finding the protected node under possible attacks or surveillance. The efficiency of the method is estimated. Client-server software was written on C# to implement this method.

Keywords: information security, defense in depth, probability of overcoming protection, closed schedule, time spent under observation

DOI: 10.18469/ikt.2017.15.1.12

Mostovoj Jakov Anatolevich, Povolzhskiy State University of Telecommunication and Informatics, 77, Moscovskoe shosse, Samara, 443090, Russian Federation; Professor of the Department of Software and Management in Technical Systems; Doctor of Technical Science; Professor. Tel.: +78462280013. E-mail: jakob.mostovoi@yandex.ru

Slepushov Ilya Igorevich, Povolzhskiy State University of Telecommunication and Informatics, 77, Moscovskoe shosse, Samara 443090, Russian Federation; Master Student of the Department of Software and Management in Technical Systems. Tel.: +79277552321. E-mail: slepusho-vii@gmail.com

References

1. Horev A.A. *Ugrozy bezopasnosti informacii* [Threats to information security]. Special'naja tehnika Publ., 2010, no. 1, pp. 50-63.
2. Mostovoi J.A., Slepushov I.I. [Increased information security by managing the physical rupture of the transmission channel]. *XXIII Rossijskaja nauchnaja konferencija professorsko-prepodavatel'skogo sostava, nauchnyh sotrudnikov i aspirantov* [Proc. HHIII Russian scientific conference of the faculty, researchers and graduate students]. Samara, 2016, pp. 264-265. (In Russian).
3. Isaev A.B. *Sovremennye tehnicheskie metody i sredstva zashhity informacii* [Modern technical methods and means of protection of information]. Moscow, RYDN Publ., 2008. 258 p.
4. Baryshnikov A.A., Isaev I.A. Modelirovanie verojatnosti vzloma sistemy informacionnoj bezopasnosti [Modeling the probability of breaking the information security system]. *Gornyj informacionno-analiticheskij bjulleten*, 2010, no. 5, pp. 152-155.
5. Mark Rhodes-Ousley. *Information Security The Complete Reference, Second Edition*. McGraw-Hill Education, 2013. 306 p.
6. Singer P.W., Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press, 2014. 101 p.
7. John Fay. *Contemporary Security Management, Third Edition*. Butterworth-Heinemann, 2010. 56 p.
8. Zaginajlov Ju.N. *Teorija informacionnoj bezopasnosti i metodologija zashhity informacii* [Theory of information security and methodology of information security]. Moscow, Direkt-Media Publ, 2015, pp. 124-170.

9. Mostovoi J.A., Slepushov I.I. *Programma upravlenija dostupom komp'juterov k seti v seansah svjazi po izmenjaemomu zakrytomu raspisaniju.* [The program of access control of computers to a network in communication sessions according to the changeable closed schedule]. Svidetel'stvo ob ofitsialnoi registratsii programm dlya EVM. No 2016662289, 2016.
10. Kupcevich Ju.E. *Al'manah programmista: Bezopasnost' v .NET, Shifrovanie, Zashhita koda i dannyh* [Almanac of the programmer: Safety in .NET, Encoding, Protection of a code and data]. Moscow, Russkaja redakcija Publ., 2004. pp. 174-261.

Received 21.12.2016

УДК 621.396.67

ЭЛЕКТРОДИНАМИЧЕСКАЯ МОДЕЛЬ ОЦЕНКИ ЭЛЕКТРОМАГНИТНОЙ БЕЗОПАСНОСТИ ПОЛЯ ИЗЛУЧЕНИЯ КОНИЧЕСКОГО РУПОРА

Кубанов В.П.[1], Ружников В.А.[1], Сподобаев М.Ю.[2]
[1]Поволжский государственный университет телекоммуникаций и информатики, Самара, РФ
[2] Научно-исследовательский институт радио, Москва, РФ
E-mail: kubanov@psati.ru

В статье приведены результаты исследований и разработки методологии расчетного мониторинга поля, создаваемого одним из элементов телекоммуникационных технических средств СВЧ-диапазона – коническим рупором. Была поставлена и решена задача уточнения физически обоснованной математической модели для расчета значений плотности потока энергии вблизи апертуры конического рупора. Модель ориентирована на применение в практике прогнозирования электромагнитной безопасности на соответствующих объектах.

Ключевые слова: электромагнитная безопасность, плотность потока энергии, электродинамическая модель, конический рупор, диаграмма направленности

Введение

Основой решения задач электромагнитной (ЭМ) экологии является разработка универсальных подходов к расчету полей в зонах, прилегающих к излучающему объекту. В числе первых значимых работ этого направления следует назвать [1-3]. Проблемы ЭМ-экологии в систематическом виде впервые были сформулированы в [4-5].

Излучение ЭМ-полей коническими рупорами рассматривались многими авторами, например [6-10]. Анализ результатов этих работ показал, что для их применения в моделях прогнозирования ЭМ-обстановки необходимы дополнительные исследования по расчету коэффициента направленного действия (КНД) в зоне Френеля с учетом расфазировки апертуры рупора.

Методика расчета

Ключевым моментом при решении задач оценки ЭМ-безопасности является расчет плотности потока энергии (ППЭ) ЭМ-излучения. В свою очередь, расчет ППЭ требует предварительных вычислений двух параметров излучателя – нормированной характеристики направленности и КНД. Ниже приводится подробное изложение методики расчета этих параметров и ППЭ конического рупора с прямолинейной образующей, показанного на рис. 1.

Геометрию рупора зададим параметрами: a – радиус апертуры (раскрыва); l – длина рупора. В большинстве случаев конический рупор возбуждается круглым волноводом с волной типа H_{11}. Примем, что плоскости H соответствует угол $\varphi = 0$, а плоскости E – угол $\varphi = \pi/2$.

Для зоны Френеля, представляющей особый интерес при оценке электромагнитной безопасности конического рупора, поле в точке наблюдения может быть представлено в виде [11-12]:

$$E(\theta,\varphi) = -i\frac{E_0 a^2}{2R\lambda}\left(1+\cos\theta\right)e^{-ikR}f(\theta,\varphi), \quad (1)$$

где

$$f(\theta,\varphi) = \\ = \int_0^{2\pi}\int_0^{1} f(\rho,\phi)\, e^{-i\gamma\rho^2 - i\delta\rho\cos(\varphi-\phi)}\rho d\rho d\phi. \quad (2)$$

Функция, аппроксимирующая распределение амплитуд в плоскости раскрыва рупора при его возбуждении волной H_{11}:

$$f(\rho,\phi) = (1 - 0{,}37\rho^2 + (-0{,}845 + \\ + 0{,}215\rho^2\,\rho^2\cos^2\phi. \quad (3)$$