УДК 004.056

Зарешин С.В., Сильнов Д.С.

Национальный исследовательский ядерный университет «МИФИ», г. Москва, Россия

КОМПЛЕКСНЫЙ АНАЛИЗ ЗАЩИЩЕННОСТИ БЕСПРОВОДНЫХ СЕТЕЙ НИЯУ МИФИ

АННОТАЦИЯ

В статье обсуждается проблематика незащищенности данных, передаваемых по беспроводным сетям, использующих технологию wi-fi. Анализируется безопасность беспроводных точек доступа на территории НИЯУ МИФИ, также анализируются wi-fi точки с признаками уязвимости, доступные за пределами территории университета. Иллюстрируются зоны покрытия беспроводных сетей, принадлежащие НИЯУ МИФИ.

КЛЮЧЕВЫЕ СЛОВА

Wi-fi сеть; сканирование беспроводных точек; несанкционированный доступ; WEP; WPA; WPA2; защищенность wi-fi сетей; НИЯУ МИФИ; безопасность.

Zareshin S.V., Silnov D.S.

National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Moscow, Russia

COMPREHENSIVE ANALYSIS OF THE SECURITY OF WIRELESS NETWORKS NRNU MEPHI

ABSTRACT

In article the issue of vulnerability of the data transferred on wireless networks using wi-fi technology is discussed. Safety of wireless access points in the territory of the NRNU MEPhI is analyzed, wi-fi access points with signs of vulnerability available outside the university territory are also analyzed. The cover zones of wireless networks belonging to NRNU MEPhI are illustrated.

KEYWORDS

Wi-fi network; scan for wireless points; unauthorized access; WEP; WPA; WPA2; security of wi-fi networks; NRNU MEPhI; safety.

Мировые реалии диктуют свои требования к информационному обеспечению человечества. Получить доступ к глобальной сети Интернет порой не столько прихоть, а жизненно важная необходимость. Одним из самых популярных способов получения заветного доступа – это использования Wi-fi точек доступа.

Современный человек, погруженный в информационное поле, постоянно с ним взаимодействует, и нуждается в нём, будь то работа, учёба или хобби. Учитывая уникальное свойство информации, что это реплицируемый ресурс, и при информационном обмене каждая сторона получает свою собственную копию информации, крайне важно знать кто участвует в информационном обмене. Университеты – это не только образовательные учреждения, где огромное количество студентов пользуются интернетом для выполнения разнообразных задач [2-6], но и организации проводящие различные, зачастую уникальные и инновационные исследования, информация о которых является частной. Невозможно не упомянуть, что информационная безопасность таких исследований, как и других частных информационных ресурсов, крайне важна, так как несанкционированное получения копии информации может привести к неприятным последствиям и потерям, в том числе и финансовым.

Однако сейчас сложно говорить о полной защищённости информации, именно поэтому авторы изучили вопрос защищённости Wi-Fi точек доступа, поскольку потенциально, любая из них может стать точкой входа злоумышленника во внутреннюю сеть университета, не имея физического контакта с сетевым оборудованием, с вытекающими из этого последствиями, такими как организация ботнетов[7] и спам-рассылок[1,7]. А поскольку далеко не все протоколы защиты для беспроводных сетей позволяют обеспечить безопасность точки доступа, то необходимо не только проверить точку доступа на наличие протокола защиты, но и определить какой именно протокол используется.

В современном городе почти каждый метр пространства пронизан волнами беспроводных сетей. НИЯУ МИФИ аналогично пронизан множеством беспроводных сетей, от множества Wi-fi точек доступа. Для их анализа, использовалось программное обеспечение Vistumbler [8]. Данное программное обеспечение позволяет из беспроводных сетей получить следующую информацию о точке доступа: SSID, MAC-адрес, уровень сигнала в дБм, производителя сетевого оборудования, способ аутентификации и способ шифрования трафика пользователей беспроводной сети. Vistumbler позволяет взаимодействовать

с GPS-адаптером, для получения дополнительных метрик, таких как GPS-координаты, для фиксации wi-fi точки в пространстве.

В качестве GPS-адаптера использовался G-STAR IV, выбор был сделан в сторону данного адаптера, благодаря относительно высокой мощности, что позволило устанавливать связь со спутниками внутри зданий. Для проведения сканирования использовалось два Wi-Fi-адаптера: встроенный и внешний. Внешний – TP-LINK AC 1200 (стандарт: 802.11ac, частоты: 2.4Гц и 5Гц), который позволил обнаружить все современные Wi-fi точки доступа. Встроенный – Wi-fi-адаптер планшета Microsoft Surface Pro 3, с аналогичными свойствами, но меньшей мощностью. Внешний вид используемого стенда для сканирования можно увидеть на рисунке 1.

Рисунок 1 – Изображение стенда

Для получения полной картины распределения, уровня сигнала и количества wi-fi точек на территории университета, необходимо было произвести сбор информации со всего пространства института, путём последовательного сканирования каждого этажа, каждого корпуса, после чего обеспечить запись и хранение всех необходимых метрик.

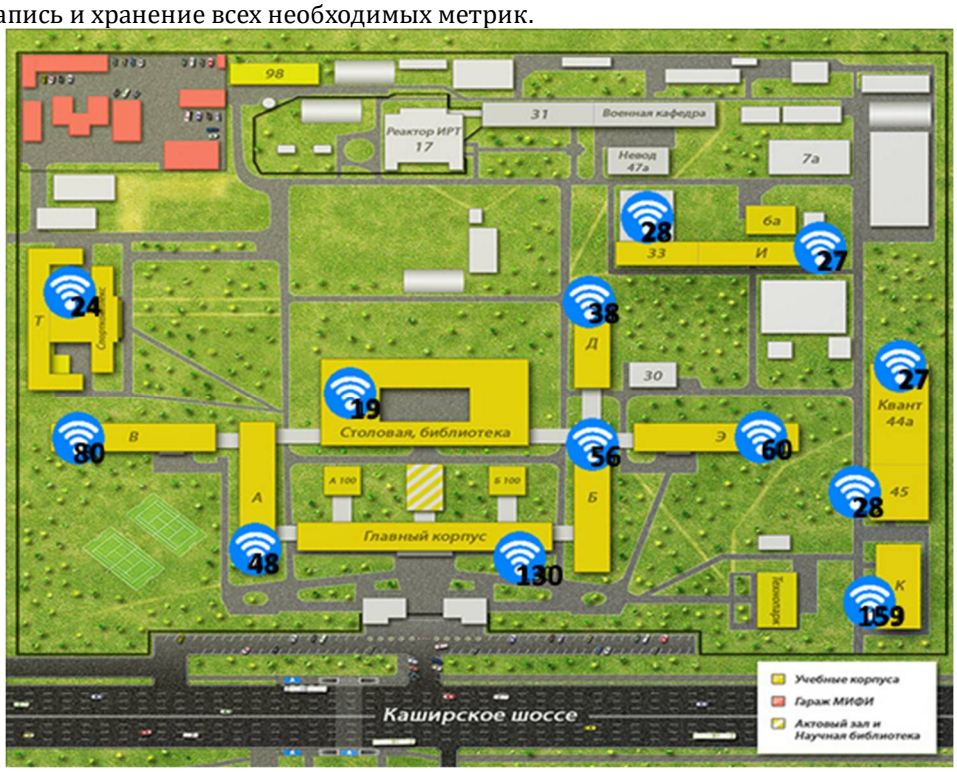

Рисунок 2 – Схема НИЯУ «МИФИ»

Для более наглядного отображения статистики будем использовать схему НИЯУ «МИФИ» приведённую на рисунке 2. В соответствии с полученными экспериментальными данными на изображении подписано количество различных сетевых устройств, работающих в качестве точки доступа в Интернет. Согласно собранной статистике наибольшее количество точек доступа находится в корпусах Г и К. Что обусловлено тем, что Г – является главным корпусом университета, и большую его часть занимают административные работники, которым необходим удобный доступ в интернет, с различных устройств, а К – корпус с наибольшей площадью среди всех остальных корпусов университета. Более подробная сводная статистика по доступным wifi-точкам на территории «МИФИ» представлена в таблице 1.

Таблица 1. – Распределённая по корпусам статистика по доступным wifi-точкам на территории НИЯУ «МИФИ»

Корпус	Всего точек доступа	Из них скрытых	Открытые	Защищённых WEP	WPA	WPA2-P	WPA2-E
33	28	1	9	1	0	18	0
44а	27	0	7	0	0	20	0
45	28	0	7	0	1	20	0
А	48	3	22	2	1	19	5
Б	56	0	28	0	5	23	0
Д	38	3	16	1	3	18	0
Э	60	1	27	0	4	28	1
Г	130	1	85	1	2	36	6
И	27	0	8	0	4	15	0
К	159	3	55	1	1	85	17
Столовая	19	0	12	0	1	6	0
Т	24	2	6	0	2	15	1
В	80	12	20	4	3	43	12
Итого:	724	26	302	10	27	346	42
Относительный показатель определённого вида точек к общему количеству точек %		3,59	41,71	1,38	3,73	47,79	5,80

Некоторые точки доступа могут сочетать в себе несколько способов авторизации пользователя, именно поэтому суммарное количество точек доступа может отличаться от общего количества точек доступа.

В соответствии с относительным показателем, который отображает процентное отношение количества определённого вида точек к общему количеству рассматриваемых wi-fi точек, почти 42% от общего количества точек являются открытые точки доступа без шифрования трафика, и около 1,5% точек используют слабый протокол защиты WEP [9]. 3,5% процента от общего количества являются точки, которые не рассылают пакеты анонсов. Почти 54% сетей используют WPA2 авторизацию пользователей, которая на данный момент является наиболее надёжной среди существующих на данный момент [10].

Однако достаточно всего одной открытой и доступной точки доступа для проникновения злоумышленника во внутреннюю инфраструктуру, не имея физического контакта с сетевым оборудованием, а на территории НИЯУ «МИФИ» имеется порядка 300 таких точек. Но они доступны на территории университета, на которую невозможно попасть без специального пропуска. Какое же количество точек доступа доступно извне НИЯУ «МИФИ». На рисунке 3 отражены точки доступа, которые можно поймать за территорией университета, а в таблице 2 указаны их названия и в каких корпусах они располагаются.

Таблица 2 – Точки доступа НИЯУ «МИФИ», которые можно найти за территорией университета

SSID	Корпус	Шифрование
Без анонса	К	None
A-206	А	WEP
ASUS	Э	None
Department12-Guest	В	None
Dlink	А	WEP
DOZEN	В	WPA
Hpsetup	В	None
Kaf44.WiFi.Free	Т	None
MEPhI	Г	None
MEPhI	Б	None

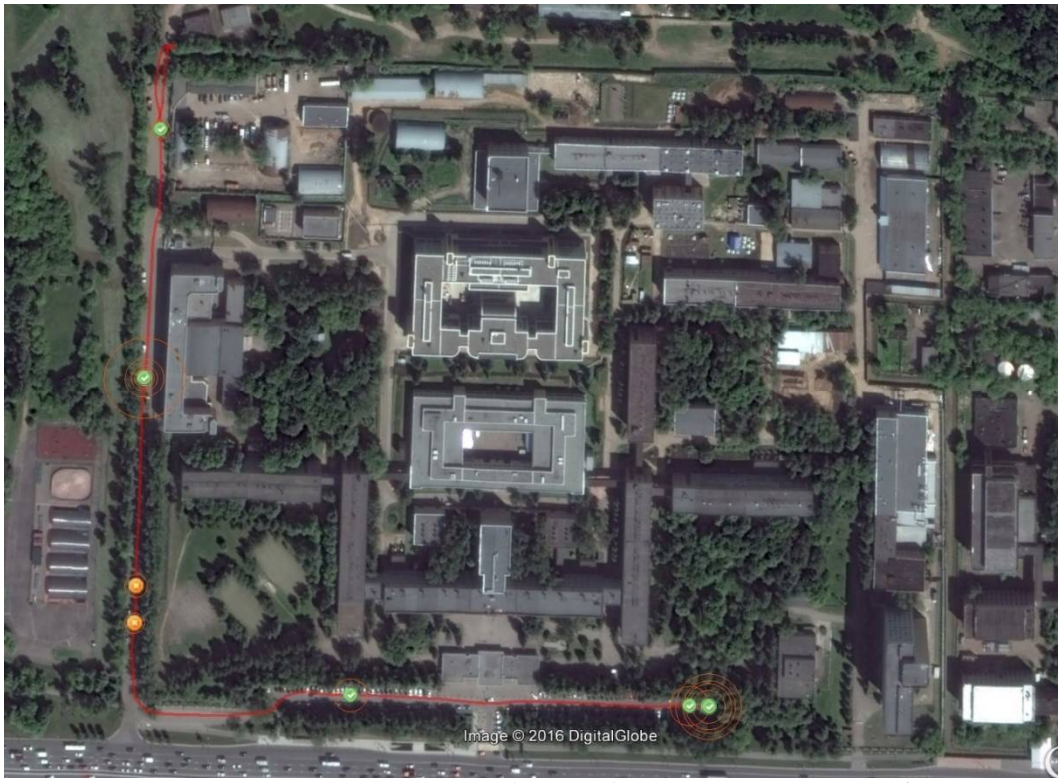

Рисунок 3 – Карта покрытия открытых точек доступа, доступных за территорией НИЯУ «МИФИ»

Особое место в сетевой архитектуре университета занимает сеть с SSID «MEPhI» она обеспечивает доступ профессорско-преподавательского состава и студентов к сети Интернет. И непосредственно связана с многими информационными сервисами университета. Но тем не менее является открытой точкой доступа и является потенциальной дырой в безопасности. Ведь радиус сигнала некоторых точек, входящих в беспроводную сеть «MEPhI», распространяется за территорию НИЯУ «МИФИ» и для подключения к этим точкам, злоумышленнику достаточно находится недалеко от территории университета, к примеру, он может с комфортом расположиться в автомобиле, стоящим за внешним периметром университета, и подключившись к беспроводной точке доступа, вмешаться во внутреннюю работу сети и/или университета.

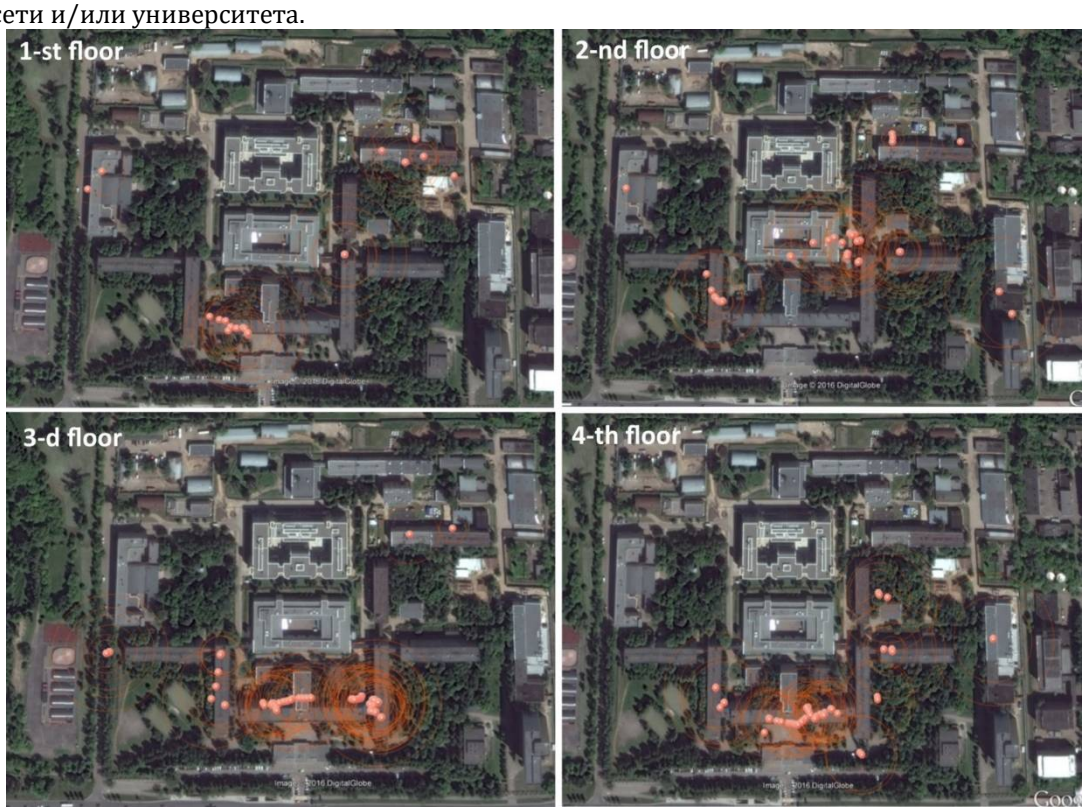

Рисунок 4 – Расположение точек доступа сети «MEPhI»

Рассмотрим расположение устройства, которых на территории университета расположилось 182 штуки, и которые в совокупности являются сетью «MEPhI». На рисунке 4 представлены все точки с областями доступности точки и распределением по этажам. То есть на рисунке представлены изображения, для 4 этажей, на каждый этаж своё изображения, подписанное в левом верхнем углу. Оранжевые точки показывают точки доступа из сети «MEPhI», а окружности вокруг них отображают область, в рамках которой эти точки доступны. Поскольку точки, входящие в беспроводную сеть «MEPhI», не применяют шифрование трафика, то злоумышленник может анализировать трафик и получить доступ к личной информации сотрудников или студентов университета, таким как логины/пароли от учётных записей различных интернет ресурсов, отправляемые сообщения и т.п.

Отдельного рассмотрения заслуживают открытые точки доступа и точки, использующие слабое шифрование. В таблице 3 приведено распределение точек доступа по корпусам университета. По-прежнему наибольшая часть точек приходится на корпуса Г и К, как самые крупные в университете. Последняя колонка отражает количество сетевых устройств, предназначенных для печати. На рисунке 5 приведена страница настроек одного из таких сетевых МФУ. Показывающая, что для доступа к сетевому печатающему устройству можно относительно просто получить доступ. Открытые сетевые МФУ так же являются потенциальным каналом утечки информации, ведь на таких принтерах печатаются различные приказы, результаты исследований и многое другое. А поскольку злоумышленник имеет доступ к устройству, то он потенциально может получить доступ к распечатываемой информации без ведома пользователя. Сетевые МФУ зачастую имеют usb-порт для работы с flash-носителями пользователей, и МФУ имеют право производить на этих накопителях запись. Что может привести к заражению flash-накопителя вирусом или любой другой разрушающей программой, при наличии у злоумышленника контроля над сетевым МФУ, что в свою очередь потенциально позволит злоумышленнику получить доступ к устройствам, которые не подключены к беспроводной сети и/или к Интернету вообще. И заполучить необходимую информацию с таких устройств. Так же доступ к настройкам сетевых устройств позволит при необходимости саботировать образовательный/исследовательский процесс.

Таблица 3 – Распределение открытых точек доступа по корпусам

Корпус	Открытые точки	Слабое шифрование	Сетевые МФУ
33	10	1	0
44а	7	0	1
45	7	0	0
А	24	2	0
Б	28	0	4
Д	17	1	0
Э	27	0	5
Г	86	1	2
И	8	0	3
К	56	1	1
Столовая	12	0	0
Т	6	0	1
В	24	4	3
Всего:	312	10	25

В целом открытые точки доступа, не имеющие шифрования или имеющие слабое шифрование, являются дырами безопасности, поскольку злоумышленник может снифить, т.е. перехватывать сетевой трафик без ведома владельца, заниматься фишингом учётных записей, добывать информацию с локальных компьютеров сети и заниматься другими противозаконными действиями, с прицелом на собственную выгоду и/или на внесение разрушающего воздействия в работу университета. Как видно проблема информационной безопасности беспроводных систем актуальна как никогда.

Подводя итог, хотелось бы отметить, что, несмотря на кажущуюся безопасность режимных объектов, которые ограничивают физический доступ к себе, не так безопасны, как хотелось бы. Современные технологии с одной стороны помогают всем в повседневной жизни, но с другой являются потенциальной угрозой безопасности и/или потенциальным каналом утечки информации. Ведь как показал анализ, что университет мирового уровня имеет порядка 40% открытых точек доступа.

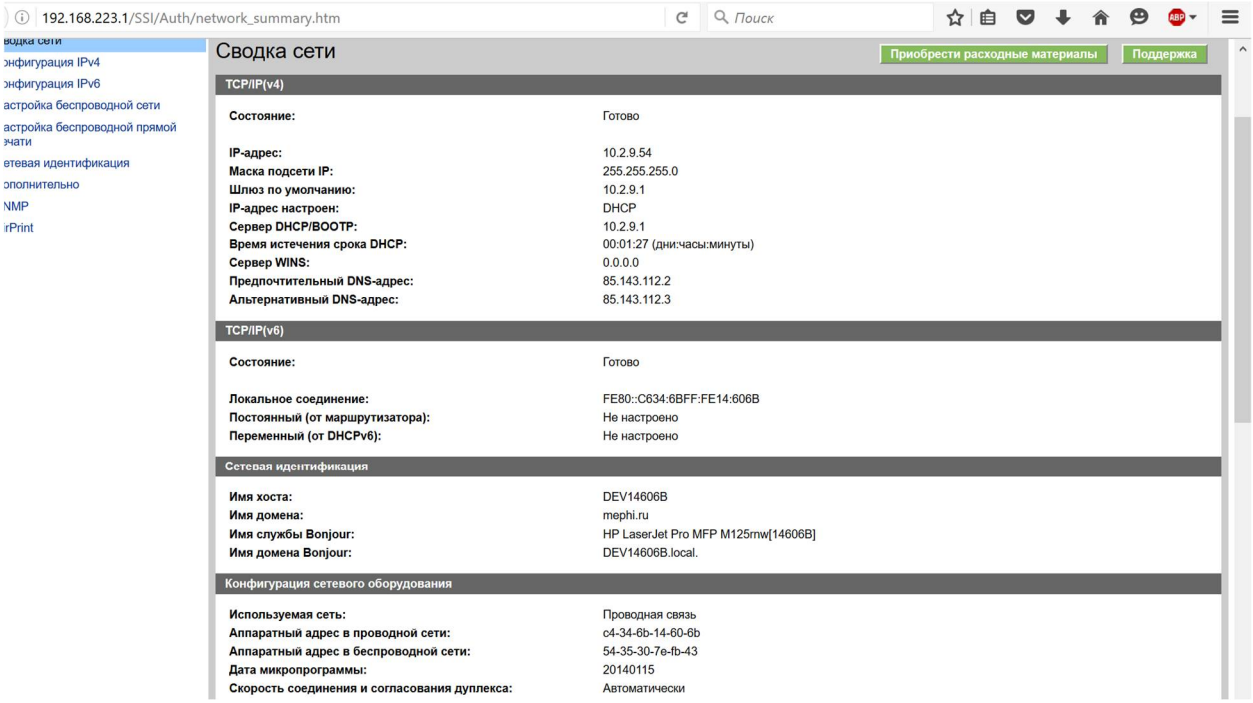

Рисунок 6 – Страница настроек сетевого МФУ

Литература

1. Makneil P. Web-dizain. Idei, secrety, sovety. – P.: «Piter», 2011. – 272s.
2. W3C Markup Validation Service. URL: http://validator.w3.org/.
3. W3C CSS Validation Service/. URL http://jigsaw.w3.org/css-validator/.
4. Ritchie S. King «The Top 10 Programming Languages» // IEEE Spectrum. – 2011. URL: http://spectrum.ieee.org/at-work/tech-careers/the-top-10-programming-languages.
5. D. S. Silnov An Analysis of Modern Approaches to the Delivery of Unwanted Emails (Spam). Indian Journal of Science and Technology, Vol 9(4), DOI: 10.17485/ijst/2016/v9i4/84803, January 2016
6. Devjatykh, D., Gerget, O., Berestneva, O.G. Sleep Apnea Detection Based on Dynamic Neural Networks (2014) Communications in Computer and Information Science, 466 CCIS, pp. 556-567.
7. Berestneva, O.G., Volovodenko, V.A., Gerget, O., Sharopin, K., Osadchaya, I.A. Multidimensional medical data visualization methods based on generalized graphic images (2013) World Applied Sciences Journal, 24 (24), pp. 18-23.
8. Belashenkova N.N., Cherepovskaya E.N., Lyamin A.V., Skshidlevsky A.A. Protection Methods of Assessment Procedures Used in e-Learning // 13th International Conference on Emerging eLearning Technologies and Applications. – 2015. – P. 27-32.
9. Uskov, V., Lyamin, A., Lisitsyna, L., Sekar, B. (2014) Smart e-Learning as a Student-Centered Biotechnical System, In: E-Learning, E-Education, and Online-Training, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Vol. 138, Eds.: Vincenti, G., Bucciero, A., Vaz de Carvalho, C. , Springer, 200 p., ISBN 978-3-319-13292-1. pp. 167-176.
10. Arzhakov, A.V., Silnov, D.S. New approach to designing an educational automated test generation system based on text analysis (2016) ARPN Journal of Engineering and Applied Sciences, 11 (5), pp. 2993-2997
11. Arzhakov A. V., Silnov D. S. Analysis of Brute Force Attacks with Ylmf-pc Signature //International Journal of Electrical and Computer Engineering (IJECE). – 2016. – Т. 6. – №. 4.
12. Zikrillah M. Analisa Wardriving Scanning dan Maping Pada Wilayah Unsri Menggunakan Software Vistumbler v10. 6, Wigle Wifi Android, dan Google Earth //Buletin Inovasi ICT & Ilmu Komputer. – 2016.
13. Tews E. Attacks on the WEP protocol //IACR Cryptology ePrint Archive. – 2007. – Т. 2007. – С. 471.
14. Lashkari A. H., Danesh M. M. S., Samadi B. A survey on wireless security protocols (WEP, WPA and WPA2/802.11 i) //Computer Science and Information Technology, 2009. ICCSIT 2009. 2nd IEEE International Conference on. – IEEE, 2009. – С. 48-52.

References

1. Makneil P. Web-dizain. Idei, secrety, sovety. – P.: «Piter», 2011. – 272s.
2. W3C Markup Validation Service. URL: http://validator.w3.org/.
3. W3C CSS Validation Service/. URL http://jigsaw.w3.org/css-validator/.
4. Ritchie S. King «The Top 10 Programming Languages» // IEEE Spectrum. – 2011. URL: http://spectrum.ieee.org/at-work/tech-careers/the-top-10-programming-languages.
5. D. S. Silnov An Analysis of Modern Approaches to the Delivery of Unwanted Emails (Spam). Indian Journal of Science and Technology, Vol 9(4), DOI: 10.17485/ijst/2016/v9i4/84803, January 2016
6. Devjatykh, D., Gerget, O., Berestneva, O.G. Sleep Apnea Detection Based on Dynamic Neural Networks (2014) Communications in Computer and Information Science, 466 CCIS, pp. 556-567.
7. Berestneva, O.G., Volovodenko, V.A., Gerget, O., Sharopin, K., Osadchaya, I.A. Multidimensional medical data visualization methods based on generalized graphic images (2013) World Applied Sciences Journal, 24 (24), pp. 18-23.
8. Belashenkova N.N., Cherepovskaya E.N., Lyamin A.V., Skshidlevsky A.A. Protection Methods of Assessment Procedures Used in e-Learning // 13th International Conference on Emerging eLearning Technologies and Applications. – 2015. – P. 27-32.
9. Uskov, V., Lyamin, A., Lisitsyna, L., Sekar, B. (2014) Smart e-Learning as a Student-Centered Biotechnical System, In: E-Learning, E-Education, and Online-Training, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Vol. 138, Eds.: Vincenti, G., Bucciero, A., Vaz de Carvalho, C. , Springer, 200 p., ISBN 978-3-319-13292-1. pp. 167-176.

10. Arzhakov, A.V., Silnov, D.S. New approach to designing an educational automated test generation system based on text analysis (2016) ARPN Journal of Engineering and Applied Sciences, 11 (5), pp. 2993-2997
11. Arzhakov A. V., Silnov D. S. Analysis of Brute Force Attacks with Ylmf-pc Signature //International Journal of Electrical and Computer Engineering (IJECE). – 2016. – Т. 6. – №. 4.
12. Zikrillah M. Analisa Wardriving Scanning dan Maping Pada Wilayah Unsri Menggunakan Software Vistumbler v10. 6, Wigle Wifi Android, dan Google Earth //Buletin Inovasi ICT & Ilmu Komputer. – 2016.
13. Tews E. Attacks on the WEP protocol //IACR Cryptology ePrint Archive. – 2007. – Т. 2007. – С. 471.
14. Lashkari A. H., Danesh M. M. S., Samadi B. A survey on wireless security protocols (WEP, WPA and WPA2/802.11 i) //Computer Science and Information Technology, 2009. ICCSIT 2009. 2nd IEEE International Conference on. – IEEE, 2009. – С. 48-52.

Поступила 11.09.2016

Об авторах:

Зарешин Сергей Владимирович, магистрант кафедры компьютерных систем и технологий Национального Исследовательского Ядерного Университета «МИФИ», svzareshin@gmail.com;

Сильнов Дмитрий Сергеевич, кандидат технических наук, доцент кафедры компьютерных систем и технологий, Национального Исследовательского Ядерного университета «МИФИ», ds@silnov.pro.