16. MathWorks. «MATLAB & Simulink Help Center» MathWorks, 2023. Available at: https://www.mathworks.com/help/index.html. Accessed 20 December 2023.
17. *Moler Cleve B.* Numerical Computing with Matlab. The MathWorks, Inc., Natik, 2004.
18. *Chapra Steven C*. Applied Numerical Methods with MATLAB for Engineers and Scientists. McGraw Hill Companies, Inc. 2nd ed. New York, 2008.
19. *Trench William F*. Elementary Differential Equations. Trench, 2013.
20. *Ukil A., Braendle H., Krippner P*. Distributed temperature sensing: Review of technology and applications, *IEEE Sens. J*., 2011, 12, pp. 885-892. DOI: 10.1109/JSEN.2011.2162060.
21. *Fawad Khan, Zhiguang Xu*, Recent Advances in Sensors for Fire Detection, PMID: 35590999, 2022 Apr 26, DOI: 10.3390/s22093310.

Статью рекомендовал к опубликованию д.т.н., профессор В.В. Курейчик.

Сингх Санни – Южный федеральный университет; e-mail: singkh@sfedu.ru; г. Таганрог, Россия; тел.: +79885751350; кафедра систем автоматического управления; аспирант.

Прибыльский Алексей Васильевич – e-mail: apribylsky@sfedu.ru; тел.: +79885619718; кафедра систем автоматического управления; к.т.н.; доцент.

Singh Sanni – Southern Federal University; e-mail: singkh@sfedu.ru; Taganrog, Russia; phone: +79885751350; the department of automatic control systems; graduate student.

Pribylskiy Alexey Vasilievich – e-mail: apribylsky@sfedu.ru; phone: +79885619718; the department of automatic control systems; cand. of eng. sc.; associate professor.

УДК 004.056.53+347.837+654.16 DOI 10.18522/2311-3103-2024-2-132-141

А.В. Дьяков, К.Е. Румянцев

АКТУАЛЬНЫЕ ПРОБЛЕМЫ РАДИОМОНИТОРИНГА В СИСТЕМЕ МЕРОПРИЯТИЙ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Беспроводные сети передачи данных порождают угрозы, от которых невозможно защититься традиционными для проводных сетей средствами, поскольку в таком случае невозможно обеспечить эквивалент безопасности проводных сетей в силу физических свойств канала связи. Целью статьи является определение актуальных проблем, существующих при обеспечении информационной безопасности (ИБ) в беспроводных сегментах сетей передачи данных. Для достижения поставленной цели из банка угроз безопасности информации ФСТЭК России осуществлена выборка угроз, потенциально реализуемых в беспроводных сетях. Установлено, что реализация таких угроз может приводить к полному набору нарушений состояния ИБ, а именно: к нарушению конфиденциальности, целостности и доступности информации. Рассмотрены существующие практические способы обеспечения ИБ в беспроводных сегментах сетей. Анализ этих способов указал на присутствующую при радиомонитроинге техническую возможность создания дополнительного рубежа в системе эшелонированной защиты информации. В свою очередь, это обеспечивает потенциал обнаружения уязвимостей и вторжений на канальном уровне сетевого взаимодействия как в локальных сетях предприятий, так и в крупномасштабных сетях общего пользования. В соответствии с целью сгруппированы аспекты построения такого рубежа защиты, связанные с контролем канального уровня сетевого взаимодействия беспроводных устройств, уменьшением размеров частотно-территориальных кластеров и правовым обеспечением. Обзором публикаций выявлен разрыв между существующими подходами к радиомонитроингу и обеспечению ИБ, также обнаружена слабая развитость направления, связанного с исследованиями в области обнаружения и предотвращения беспроводных вторжений. Полученный результат указывает на необходимость пересмотра сложившейся концепции радиомонитроинга и разработки соответствующих организационно-технических мер для его интеграции в систему мероприятий по обеспечению ИБ, что должно помочь решить проблему своевременного обнаружения и предотвращения вторжений в беспроводные сегменты сетей передачи данных, а также выявления уязвимых элементов инфраструктуры этих сетей.

Информационная безопасность; радиоконтроль; радиомониторинг; системы обнаружения вторжений; СОВ; беспроводные сети; Wi-Fi; WIDS; WIPS.

A.V. Dyakov, K.E. Rumyantsev

CURRENT PROBLEMS OF RADIOMONITORING IN THE SYSTEM OF ACTIONS TO ENSURE INFORMATION SECURITY

Wireless data transmission networks generate threats that cannot be protected against by means traditional for wired networks, because in this case it is impossible to provide equivalent security of wired networks due to the physical properties of the communication channel. The purpose of the article is to determine the actual problems that exist in ensuring information security (IS) in wireless segments of data networks. To achieve this goal, a selection of threats potentially realizable in wireless networks has been made from the information security threat bank of FSTEC of Russia. It is established that the realization of such threats can lead to a full set of violations of the state of IS, namely: violation of confidentiality, integrity and availability of information. The existing practical ways of providing IS in wireless segments of networks are considered. The analysis of these methods pointed out the technical possibility of creating an additional boundary in the system of echeloned information protection. In turn, this provides the potential to detect vulnerabilities and intrusions at the link layer of network communication both in local networks of enterprises and in large-scale public networks. In accordance with the goal, aspects of building such a defense frontier are grouped, related to control of the link layer of network interaction of wireless devices, reduction of frequency-territorial clusters and legal support. The review of publications reveals a gap between the existing approaches to radio monitoring and IS provision, and also reveals poor development of the direction related to research in the field of detection and prevention of wireless intrusions. The obtained result indicates the need to revise the existing concept of radio monitoring and develop appropriate organizational and technical measures for its integration into the system of measures to ensure IS, which should help to solve the problem of timely detection and prevention of intrusions into wireless segments of data networks, as well as the identification of vulnerable elements of the infrastructure of these networks.

Information security; radiocontrol; radiomonitoring; intrusion detection systems; wireless networks; Wi-Fi; WIDS; WIPS.

Введение. Беспроводная передача информации, не ограничивающая абонентов определенной точкой пространства, всегда вызывала большой интерес. Сегодня с уверенностью можно сказать о том, что беспроводная техника буквально завоевывает мир. Среди причин такой популярности можно отметить мобильность и эстетическую привлекательность: помимо свободы передвижения отсутствие проводов делает интерьер опрятным, исчезают трудности, связанные с распутыванием кабелей и механической надёжностью соединений. Рост популярности беспроводных технологий объясняется также развитием самой инфраструктуры: появляются новые стандарты передачи данных, обеспечивающие высокую скорость передачи информации, увеличивается количество базовых станций и, как следствие, расширяется зона покрытия. Встроенное программное обеспечение устройств существенно сокращает время на настройку соединения: пользователю достаточно всего один раз подключиться к защищённой сети, после чего повторные подключения к ней будут осуществляться устройством автоматически. В случае мобильной связи с использованием SIM-карт, средств бесконтактной оплаты с технологией NFC, а также устройств радиочастотной идентификации (RFID) у пользователя принципиально отсутствует необходимость в каких-либо настройках и получении для этого специальных знаний.

Вместе с тем каждый новый этап распространения беспроводных технологий создаёт такие угрозы, которые зачастую трудно спрогнозировать, не говоря уже о разработке и внедрении контрмер для предотвращения реализации этих угроз. С позиции возможного нарушения состояния информационной безопасности (ИБ) беспроводной сегмент телекоммуникационной сети является самым уязвимым звеном по ряду причин. Во-первых, в реальных условиях радиоэлектронные средства (РЭС), действующие в беспроводной сети, всегда будут подвержены непреднамеренному интерференционному воздействию других РЭС и излучений иных источников электромагнитных помех. Нарушение электромагнитной совместимости приводит не только к снижению скорости передачи данных по радиоканалу, но и вовсе к потере связи и приведению информационной системы в состояние «отказ в обслуживании» (англ. Denial of Service, DoS). Во-вторых, между конечными точками беспроводного сегмента сети находится неограниченная область – ра-

диоэфир, в связи с чем у злоумышленника появляется возможность не преодолевать физическую защиту и не контактировать с аппаратными средствами информационной системы. Анонимность беспроводных вторжений [1] делает для нарушителя эту возможность ещё более привлекательной. Воздействия, при которых беспроводные сети становятся уязвимыми для несанкционированного доступа, с точки зрения обеспечения ИБ представляют гораздо большую опасность по сравнению с DoS-атаками.

Для оценки негативных последствий реализации угроз в беспроводных сетях можно воспользоваться банком данных угроз безопасности информации ФСТЭК России [2], выбрав из него угрозы, потенциально реализуемые в этих сетях. Полученные таким образом данные консолидированы в табл. 1 и визуализированы на диаграмме (рис. 1).

Таблица 1

Последствия реализации угроз в беспроводных сетях

Идентификатор угрозы	Последствия реализации угрозы		
	нарушение конфиденциальности	нарушение целостности	нарушение доступности
УБИ.011			+
УБИ.030	+	+	+
УБИ.069	+	+	
УБИ.083	+	+	+
УБИ.116		+	
УБИ.125	+	+	+
УБИ.126	+		+
УБИ.133	+		
УБИ.139	+	+	+
УБИ.140			+

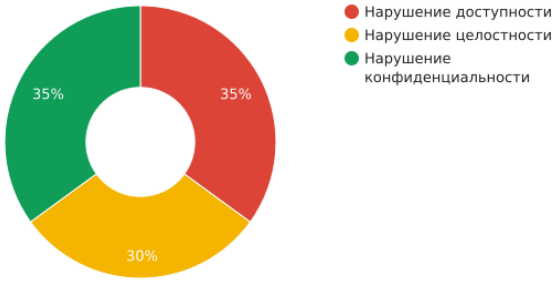

Рис. 1. Диаграмма распределения последствий реализации угроз в беспроводных сетях

Распределение последствий реализации угроз в беспроводных сетях указывает на то, что нарушения доступности, целостности и конфиденциальности информации возможны и находятся приблизительно в одинаковых пропорциях относительно друг друга.

Для всестороннего рассмотрения проблемы вторжений в системы беспроводной передачи данных помимо определения угроз и последствий их реализации необходимо также установить категории нарушителей. Модель нарушителя, построенная согласно нормативным документам [3], будет носит весьма общий характер. Основными факторами, которые окажутся неучтенными, являются цели и мотивация нарушителя. В некоторых случаях эти факторы являются решающими [4]. В оценке потенциала нарушителя, даже при учете его компетенции, основополагающую роль играет мотивация [5]: так, в отсутствии необходимой компетенции именно мотивация толкает злоумышленника на совершение нарушения.

Проблема контроля канального уровня сетевого взаимодействия. Арсенал средств защиты информации в телекоммуникационных каналах традиционно представляет собой межсетевые экраны, а также может включать в себя средства криптографиче-

ского шифрования и системы обнаружения и предотвращения вторжений (англ. Intrusion Detection and Prevention System, IDS/IPS). Последние в качестве входной информации используют поток пакетов сетевого трафика [6–8]. Рассматривая перечисленные средства в иерархии семиуровневой модели сетевого взаимодействия OSI [9], можно сделать вывод от том, что действуют они в подавляющем большинстве на сетевом уровне модели OSI. Работа с канальным уровнем модели OSI зачастую сводится лишь к ограничительным мерам, правила которых задаются вручную и являются по сути статическими, например: фильтрация адресов устройств в управляемых коммутаторах и настройка паролей беспроводных интерфейсов. При этом, в соответствии с принципом декапсуляции, подробности взаимодействия, происходящего на канальном уровне, при движении к более высшим уровням утрачиваются и уже на сетевом уровне отсутствуют. Таким образом, доступ к канальному уровню сетевого взаимодействия возможен только лишь с низшего слоя модели OSI – физического уровня, что для беспроводных сетей является радиоэфиром.

Идея контроля активности на канальном уровне посредством специализированных радиоприёмных устройств не нова: беспроводные IDS/IPS (англ. Wireless IDS/IPS, WIDS/WIPS) существуют и представляют собой системы, которые осуществляют мониторинг радиоэфира, анализируют полученную информацию об источниках радиосигнала, их взаимодействиях и аномальных активностях, а также предотвращают действия, противоречащие настроенной политике предотвращения вторжений.

Преимущества построения IDS/IPS на более низких уровнях сетевой модели OSI очевидны: эшелонированная защита обеспечивает собственные меры безопасности на каждом уровне, если нарушитель сумеет преодолеть один рубеж безопасности, то он столкнется со следующим, что значительно затруднит проникновение в информационную систему через периметр сети.

Необходимо отметить, что научное направление построения WIDS/WIPS развито слабо. В русскоязычных публикациях упоминания таких систем встречаются нечасто и преимущественно в рекламных брошюрах ведущих иностранных производителей сетевого оборудования. В зарубежных публикациях научный интерес представляет эксплуатационная документация к оборудованию WIDS/WIPS, из которой можно сложить некоторое представление об алгоритмах действия этих устройств. По существу, упомянутые WIDS/WIPS являются дополнительным функционалом сетевого оборудования семейства стандартов IEEE 802.11 и позволяют организовывать ещё один рубеж безопасности беспроводного сегмента телекоммуникационной корпоративной сети, состоящей из одной или нескольких точек доступа Wi-Fi, находящихся в ограниченном пространстве. Такие WIDS и WIPS предназначены для защиты интересов именно владельца базовой станции (точки доступа) и находящейся за ней информационной системы, при этом у абонентов нет возможности удостовериться в надёжности сети, к которой они производят подключение. Кроме того, контроль телекоммуникационных сетей других стандартов и масштабирование таких WIDS/WIPS до уровня сетей общего пользования не представляется возможным.

Доступ к канальному уровню модели OSI также может быть получен через физический уровень посредством техники, предназначенной для контроля за излучениями РЭС и стоящей на вооружении у специальных служб, осуществляющих радиоконтроль и радиомонитроинг. Специфика данных мероприятий, заключающаяся в закрытости указанных служб, накладывает существенный отпечаток на направленность публикаций: подавляющее большинство из них посвящены решению широко известных научных и технических проблем, совершенствованию существующих методов и их программно-аппаратных реализаций. Так, наиболее полно типовые задачи радиомониторинга, аспекты построения и функционирования систем радиоконтроля, а также опыт осуществления мероприятий радиоконтроля в сложной помеховой обстановке в промышленных центрах, внутри зданий и на открытой местности освещены в [10, 11]. Благодаря высокой концентрации теоретической и практической информации книги по существу являются настольными справочниками и высоко востребованы специалистами в области радиомониторинга, руководителями радиоконтрольных служб, сотрудниками силовых ведомств и служб безопасности государственных и коммерческих структур.

Вместе с тем, несмотря на глубокое и многогранное изложение материала в указанных источниках, а также немалое количество обзорных и рационализаторских публикаций, основанных на данных источниках, о существовании острых и актуальных практических трудностей применения существующего радиоконтрольного оборудования можно судить лишь по единичным публикациям. Так, наличие серьёзных пробелов, вызванных формальным подходом к радиоконтролю, открыто заявлено лишь в [12]. Авторы недвусмысленно и эмоционально указывают на то, что современный (по состоянию на 2017 год) радиоконтроль невозможен без анализа трафика цифровых каналов связи, причём извлекаемая информация носит не второстепенный характер, а должна являться приоритетным фактором принятия решений. Также авторами показаны простые и одновременно яркие примеры абсурдности формального подхода в интересах обеспечения защиты информации, заключающегося в анализе амплитудно-частотных характеристик излучений «классическим радиоконтролем». Повсеместное внедрение беспроводной цифровой связи привело к тому, что эта проблема за считанные годы распространилась из отдельных защищаемых помещений на масштабные территории мегаполисов и государств в целом.

Невозможность осуществления полноценного радиоконтроля без вскрытия передаваемой информации подтверждается также и в [13], где коллектив авторов (сотрудников одной из ведущих организаций-производителей российского радиоконтрольного оборудования) предлагает способ адресного пеленгования базовых станций GSM, UMTS, LTE сетей сотовой связи. При этом авторы также заявляют о том, что «в большинстве сотовых систем связи, в частности, UMTS и LTE, множество базовых станций, характеризующихся своими идентификационными параметрами, осуществляют одновременную передачу в одном частотном диапазоне. Это делает принципиально невозможным применение фазоразностного метода пеленгования с непосредственным вычислением пеленга и требует выделения сигнала каждой обнаруженной БС из суммарного группового сигнала». Вводится понятие «тонкой структуры» сигналов базовых станций.

Проблема уменьшения размеров частотно-территориальных кластеров. Поскольку радиочастотный спектр как ресурс ограничен, увеличение пропускной способности каналов (и, как следствие, их широкополосности) становится возможным путём увеличения плотности размещения РЭС с одновременным уменьшением зон обслуживания каждого средства. Таким образом, доля аппаратуры стандартов и технологий беспроводной связи на коротких расстояниях с каждым годом будет увеличиваться вместе с ростом широкополосной такой аппаратуры. Приведённая тенденция развития беспроводных сетей связи свидетельствует о том, что всё большее количество РЭС будет одновременно использовать одни и те же радиочастотные каналы. Начиная с технологий связи третьего поколения (3G, UMTS), стало возможным развёртывать масштабные одночастотные беспроводные сети. Такая особенность делает традиционные амплитудно-частотные методы радиоконтроля неэффективными, поскольку стационарные комплексы радиоконтроля в таком случае смогут обнаруживать лишь один ближайший передатчик, под мощным излучением которого будут маскированы излучения от других передатчиков, находящихся на большем удалении и работающих в том же частотном канале. Уменьшение размеров частотно-территориальных кластеров приводит к тому, что развитие сети дорогостоящих стационарных комплексов радиоконтроля в перспективе не приведёт к сколь-нибудь значимому увеличению охвата территории радиоконтролем. С этой проблемой уже сталкиваются службы ИБ, обеспечивающие защиту информации в рамках даже относительно небольшого ограниченного пространства предприятий, применяя пространственно-распределённые системы радиоконтроля (TORNADO-RxMTCA, RS1000, АРК-АБС и прочие).

В случае контроля сетей общего пользования, развёрнутых на масштабных территориях, стратегия увеличения количества стационарных мониторинговых комплексов невозможна, поскольку количество последних должно будет расти соразмерно с количеством базовых станций (точек беспроводного доступа). В настоящее время единственной «панацеей» для решения подобных задач являются мобильные комплексы радиоконтроля. Двигаясь по установленному маршруту, они позволяют обнаруживать большее количество РЭС по сравнению со стационарными изделиями. Вместе с тем возникает пробле-

ма идентификации РЭС, поскольку помимо обнаружения самого факта излучения необходимо вскрыть содержимое передаваемой информации и выделить уникальные идентификаторы-позывные, позволяющие указать на присутствие излучения от конкретных РЭС в электромагнитном групповом «смоге». Так, поиски незаконно-действующих РЭС превращаются в «поиск иголки в стоге сена»: априори неизвестно, существуют ли такие средства, а обнаружить их становится возможным лишь оказавшись в непосредственной близости, при этом размер зоны обнаружения неуклонно сокращается из-за ввода в эксплуатацию новых средств. В результате, вместе с постоянным ростом трудозатрат на осуществление мероприятий радиомониторинга, также растёт и нагрузка на специалистов, быстрее вырабатывается ресурс дорогостоящего радиоконтрольного оборудования, увеличиваются расходы на горюче-смазочные материалы и на поддержание в надлежащем состоянии автомобильного парка. Кроме того, подобная тактика поиска вторжений в сети и уязвимых элементов её инфраструктуры не обеспечивает непрерывности контроля.

Проблема правового обеспечения. Действующий в настоящее время на территории Российской Федерации порядок радиоконтроля РЭС гражданского назначения основан на том, что в ходе мероприятий радиоконтроля его объектами главным образом являются параметры излучений РЭС с привязкой к местам их установки. Сами РЭС и их взаимодействие между собой представляют интерес лишь в экстраординарных случаях [14], например при установлении причин нарушений связи в цифровых системах и локализации источников DoS-атак, при этом специалисты радиоконтроля де-факто вынуждены действовать за пределами руководящих документов [15], то есть заниматься «самодеятельностью» со всеми вытекающими отсюда последствиями. В таких случаях успех мероприятия не гарантирован даже при наличии у специалиста соответствующего оборудования, опыта и некоторых других сопутствующих факторов, включая аналитические способности, физическую силу, артистизм, способность пойти на риск, и даже интуицию, поэтому проведение подобных операций является своего рода искусством.

Таким образом, при радиоконтроле анализу подлежит именно физический уровень модели сетевого взаимодействия OSI; требования к обязательному контролю канального уровня и тем более руководящие документы отсутствуют, несмотря на наличие соответствующих технических возможностей. Кроме того, подавляющее большинство РЭС, являющихся абонентскими станциями (стационарными, носимыми и возимыми), не представляют интерес у надзорных органов и оказываются неохваченными радиоконтролем.

Ранее упомянутая проблема, заключающаяся в уменьшении размеров частотно-территориальных кластеров, хорошо известна специалистам радиоконтроля и вынуждает их применять совместно со средствами измерения так-называемые «индикаторы» [16]. Данное вспомогательное оборудование позволяет получать с канального уровня модели OSI не только сведения о передаваемой в эфир идентификационной информации (MAC-адреса устройств, CID, LAC, MCC, MNC базовых станций сотовой связи и т.п.), но и о подробностях сетевого взаимодействия, что даёт возможность строить топологии сетей. В качестве примера таких индикаторов можно привести носимые изделия отечественного производства RAD-001 (ООО НПФ «Радиан-М»), Барс-GSM (ООО «ТАиП»), Барс-У-мини (ООО «СТЦ»). Широчайшим спектром возможностей подобного рода обладают и мобильные комплексы на основе радиоприёмного устройства Аргамак-ИС (АО «ИРКОС»). Однако, нормативно-правовой статус у таких средств в настоящее время отсутствует, что стало возможным после череды законодательных новшеств. В действующем законодательстве [17] определено, что в качестве доказательств правонарушений могут рассматриваться показания специальных технических средств, под которыми понимаются приборы, утверждённые в установленном порядке в качестве средств измерения, имеющие соответствующие сертификаты и метрологическую поверку. Индикаторы (вспомогательное оборудование) не являются средствами измерения и не могут обладать метрологическими характеристиками в принципе. Кроме того, формируемые индикаторными средствами отчёты, могут быть свободно отредактированы, то есть сфальсифицированы. Таким образом, полученные при помощи индикаторов сведения невозможно использовать в качестве доказательства факта нарушения. По этим причинам, при от-

сутствии у владельца РЭС действий, направленных на устранение нарушения в добровольном порядке, возникают прецеденты невозможности принуждения владельца РЭС к устранению нарушений.

Вместе с тем, сама процедура установления юридического владельца РЭС зачастую сопряжена со значительными трудностями процессуального характера: нередки случаи, когда, несмотря на совокупность прямых и косвенных признаков, нарушитель отрицает факт владения неразрешённым РЭС [18]. При контроле соблюдения требований об обязательной идентификации абонентов при подключении к сети «Интернет» [19] Роскомнадзор, в чьём ведении находится осуществление соответствующего контроля, не имеет полномочий на проведение проверок в отношении физических и юридических лиц, не являющихся операторами связи. Данные о таких случаях передаются в правоохранительные органы (МВД, ФСБ, прокуратуру РФ), однако дальнейшее движение материалов нередко останавливается из-за ряда иных вполне очевидных причин, включающих малозначительность гипотетического правонарушения и несоразмерность сил и средств, необходимых для установления всех обстоятельств, возможному размеру вреда и тяжести последствий. Также отсутствует механизм установления факта организации физическим лицам публичных сетей с использованием точек доступа, закрытых паролем [20].

Кроме того, в соответствии с постановлением [21] у органов радиочастотной службы существует ряд задач, которые невозможно выполнить качественно без применения индикаторных средств, позволяющих анализировать канальный уровень сетевого взаимодействия [16]. Наиболее ответственными среди этих задач можно отметить радиоконтроль базовых станций сотовой связи в пограничной зоне (вблизи государственной границы) при международной правовой защите частотных присвоений, работы по оценке выполнения операторами связи требований к защите сетей связи от несанкционированного доступа к ним и передаваемой по ним информации, а также проведение мониторинга в целях выявления угроз устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования.

Сложившаяся ситуация, связанная с несовершенством правового обеспечения, нередко приводит к абсурдности радиомониторинга в системе мероприятий по обеспечению ИБ вследствие того, что получаемые данные не имеют юридической силы и не могут служить основанием для нейтрализации возникающих угроз. В свою очередь, количественное накопление проблем приводит к качественным изменениям в обществе: наблюдая за неспособностью государства дать ответы на возникающие вызовы и угрозы, граждане утрачивают доверие к власти, что в конечном итоге вынуждает их решать возникающие проблемы способами, лежащими вне правового поля.

Выводы. В настоящее время сложилась парадоксальная ситуация, когда между защитой информации и радиомониторингом образовалась своеобразная техническая, методологическая и нормативно-правовая пустота. Такое положение является существенным препятствием как для эффективного осуществления мероприятий по обеспечению ИБ, так и надзорной деятельности за излучениями РЭС и регулирования использования радиочастотного спектра. Разработка и внедрение организационно-технических мер, позволяющих преодолеть проблему контроля беспроводных сетей на канальном уровне сетевого взаимодействия, проблему уменьшения размеров частотно-территориальных кластеров и проблему правового обеспечения, должны создать благоприятные условия для качественного социально-экономического развития общества.

Данные, получаемые в ходе радиомониторинга беспроводных сетей с подробностями взаимодействия на канальном уровне, могут быть востребованы не только в целях предотвращения вторжений в такие сети, но и в иных задачах, например:

- получение дополнительного фактора идентификации личности (владельца устройства) в системах распознавания клиентов (в банках, клубах, библиотеках и иных общественных местах);
- решение широкого спектра оперативно-разыскных задач, включая поиск похищенного имущества и пропавших без вести лиц;

♦ установление личности граждан, поступающих в лечебные учреждения в состоянии нарушенного сознания;

♦ контроль за соблюдением ИБ в части ограничений на внос техники в режимные зоны;

♦ выявление базовых станций, позволяющих подключаться к сети «Интернет» без идентификации (в нарушение требований [19]);

♦ выявление беспроводного сегмента сетей, не ограничивающих доступ к запрещённой информации (нарушение требований [22]).

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Меррит М., Поллино Д.* Безопасность беспроводных сетей / пер. с англ. Семенова А.В. – М.: Компания АйТи; ДМК Пресс, 2004. – 288 с.
2. Банк данных угроз безопасности информации // ФСТЭК России. – URL: https://bdu.fstec.ru/threat (дата обращения: 27.01.2024).
3. Методический документ «Методика оценки угроз безопасности информации» (утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г.).
4. *Голембиовская О.М., Рытов М.Ю., Шинаков К.Е., Горлов А.П., Губсков Ю.А., Голембиовский М.М., Кондрашова Е.В.* Этапы формирования модели угроз и модели нарушителя информационной безопасности с учетом изменений законодательства Российской Федерации. – 2-е изд. – Саратов: Вузовское образование, 2024. – 265 с.
5. *Голембиовская О.М., Рытов М.Ю., Шинаков К.Е., Голембиовский М.М., Кондрашова Е.В.* Формализация подхода к определению степени ущерба и потенциала нарушителя. – 2-е изд. – Саратов: Вузовское образование, 2024. – 75 с.
6. *Полтавцева М.А., Лаврова Д.С.* Высокопроизводительные системы обнаружения вторжений: учеб. пособие. – 2-е изд. – М.; Вологда: Инфра-Инженерия, 2023. – 152 с. – ISBN 978-5-9729-1213-1.
7. *Шелухин О.И., Руднев А.Н., Савелов А.В*. Системы обнаружения вторжений в компьютерные сети: учеб. пособие. – М.: Московский технический университет связи и информатики, 2013. – 88 с.
8. *Басыня Е.А.* Сетевая информационная безопасность: учебник. – М.: Национальный исследовательский ядерный университет «МИФИ», 2023. – 224 с. – ISBN 978-5-7262-2949-2.
9. *Таненбаум Э., Фимстер Н., Уэзеролл Д.* Компьютерные сети. – 6-е изд. – СПб.: Питер, 2023. – 992 с.
10. *Рембовский А.М., Ашихмин А.В., Козьмин В.А.* Радиомониторинг: задачи, методы, средства. – 3-е изд. – М.: Горячая линия – Телеком, 2012. – 640 с.
11. *Слободянюк П.В., Благодарный В.Г.* Радиомониторинг. Вчера, сегодня, завтра (Теория и практика построения системы радиомониторинга). – Прилуки: ООО «Издательство «Аір-Поліграф», 2010. – 296 с.
12. *Захаров А.В., Кривцун А.В.* Имитация бурной деятельности, или каким не должен быть радиоконтроль в XXI веке // Информационно-методический журнал «Защита информации. Инсайд». – 2017. – № 1.
13. *Манелис В.Б., Сладких В.А., Козьмин В.А., Бизюков П.Е.* Адресное пеленгование базовых станций GSM, UMTS, LTE сетей сотовой связи // Системы управления, связи и безопасности. – 2021. – № 2.
14. *Карш А., Симонов Д.* Каждый инспектор желает знать. Причины возникновения радиопомех // Радиочастотный спектр. – 2013. – № 10. – С. 38-42.
15. Приказ Роскомнадзора от 02.02.2010 №78 «Об утверждении Инструкции по поиску и обнаружению источников радиопомех».
16. *Курков А., Пулин А.* Ловись, РЭС, большое и маленькое. Радиоконтроль сетей беспроводного доступа не дремлет // Радиочастотный спектр. – 2013. – № 12. – С. 34-37.
17. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 №195-ФЗ (ред. от 25.12.2023).
18. *Бикшанов П.* Маскировочная ШБД-сеть. Как владельцы неразрешённых беспроводных РЭС скрывают свои устройства // Радиочастотный спектр. – 2017. – № 8. – С. 44-46.
19. Постановление Правительства Российской Федерации от 31.12.2021 № 2607 «Об утверждении Правил оказания телематических услуг связи».
20. *Жаров А.А.* Публичный Wi-Fi выходит из тени // Радиочастотный спектр. – 2016. – № 10. – С. 15-16.
21. Постановление Правительства РФ от 14 мая 2014 г. № 434 «О радиочастотной службе».
22. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

REFERENCES

1. *Merrit M., Pollino D.* Bezopasnost' besprovodnykh setey [Security of wireless networks], transl. from engl. by Semenova A.V. Moscow: Kompaniya AyTi; DMK Press, 2004, 288 p.
2. Bank dannykh ugroz bezopasnosti informatsii [Information security threats data bank], *FSTEK Rossii* [FSTEC of Russia]. Available at: https://bdu.fstec.ru/threat (data obrashcheniya: 27 January 2024).
3. Metodicheskiy dokument «Metodika otsenki ugroz bezopasnosti informatsii» (utv. Federal'noy sluzhboy po tekhnicheskomu i eksportnomu kontrolyu 5 fevralya 2021 g.) [Methodological document «Methodology for Assessing Information Security Threats» (approved by the Federal Service for Technical and Export Control on February 5, 2021)].
4. *Golembiovskaya O.M., Rytov M.Yu., Shinakov K.E., Gorlov A.P., Gubskov Yu.A., Golembiovskiy M.M., Kondrashova E.V.* Etapy formirovaniya modeli ugroz i modeli narushitelya informatsionnoy bezopasnosti s uchetom izmeneniy zakonodatel'stva Rossiyskoy Federatsii [Stages of formation of the threat model and the model of the information security intruder taking into account changes in the legislation of the Russian Federation]. 2nd ed. Saratov: Vuzovskoe obrazovanie, 2024, 265 p.
5. *Golembiovskaya O.M., Rytov M.Yu., Shinakov K.E., Golembiovskiy M.M., Kondrashova E.V.* Formalizatsiya podkhoda k opredeleniyu stepeni ushcherba i potentsiala narushitelya [Formalization of the approach to determining the degree of damage and potential of the intruder]. 2nd ed. Saratov: Vuzovskoe obrazovanie, 2024, 75 p.
6. *Poltavtseva M.A., Lavrova D.S.* Vysokoproizvoditel'nye sistemy obnaruzheniya vtorzheniy: ucheb. posobie [High-performance intrusion detection systems: a textbook]. 2nd ed. Moscow; Vologda: Infra-Inzheneriya, 2023, 152 c. ISBN 978-5-9729-1213-1.
7. *Shelukhin O.I., Rudnev A.N., Savelov A.V.* Sistemy obnaruzheniya vtorzheniy v komp'yuternye seti: ucheb. posobie [Intrusion detection systems in computer networks: a textbook]. Moscow: Moskovskiy tekhnicheskiy universitet svyazi i informatiki, 2013, 88 p.
8. *Basynya E.A.* Setevaya informatsionnaya bezopasnost': uchebnik [Network information security: textbook]. Moscow: Natsional'nyy issledovatel'skiy yadernyy universitet «MIFI», 2023, 224 p. ISBN 978-5-7262-2949-2.
9. *Tanenbaum E., Fimster N., Uezeroll D.* Komp'yuternye seti [Computer Networks]. 6th ed. –Saint Petersburg.: Piter, 2023, 992 p.
10. *Rembovskiy A.M., Ashikhmin A.V., Koz'min V.A.* Radiomonitoring: zadachi, metody, sredstva [Radio monitoring: tasks, methods, means]. 3rd ed. Moscow: Goryachaya liniya – Telekom, 2012, 640 p.
11. *Slobodyanyuk P.V., Blagodarnyy V.G.* Radiomonitoring. Vchera, segodnya, zavtra (Teoriya i praktika postroeniya sistemy radiomonitoringa) [Radiomonitoring. Yesterday, today, tomorrow (Theory and practice of building a radio monitoring system)]. Priluki: OOO «Izdatel'stvo «Aip- Poligraf», 2010, 296 p.
12. *Zakharov A.V., Krivtsun A.V.* Imitatsiya burnoy deyatel'nosti, ili kakim ne dolzhen byt' radiokontrol' v XXI veke [Imitation of stormy activity, or what should not be radio monitoring in the XXI century], *Informatsionno-metodicheskiy zhurnal «Zashchita informatsii. Insayd»* [Information-methodical journal "Information Protection. Inside"], 2017, No. 1.
13. *Manelis V.B., Sladkikh V.A., Koz'min V.A., Bizyukov P.E.* Adresnoe pelengovanie bazovykh stantsiy GSM, UMTS, LTE setey sotovoy svyazi [Address direction finding of GSM, UMTS, LTE base stations of cellular communication networks], *Sistemy upravleniya, svyazi i bezopasnosti* [Control, Communication and Security Systems], 2021, No. 2.
14. *Karsh A., Simonov D.* Kazhdyy inspektor zhelaet znat'. Prichiny vozniknoveniya radio-pomekh [Every inspector wants to know. Causes of radio interference], *Radiochastotnyy spektr* [Radio Frequency Spectrum], 2013, No. 10, pp. 38-42.
15. Prikaz Roskomnadzora ot 02.02.2010 №78 «Ob utverzhdenii Instruktsii po poisku i obnaruzheniyu istochnikov radiopomekh» [Order of Roskomnadzor from 02.02.2010 № 78 "On approval of the Instruction on search and detection of radio interference sources"].
16. *Kurkov A., Pulin A.* Lovis', RES, bol'shoe i malen'koe. Radiokontrol' setey besprovodnogo dostupa ne dremlet [Catch, RPS, big and small. Radio control of wireless access networks does not slumber], *Radiochastotnyy spektr* [Radio Frequency Spectrum], 2013, No. 12, pp. 34-37.
17. Kodeks Rossiyskoy Federatsii ob administrativnykh pravonarusheniyakh ot 30.12.2001 №195-FZ (red. ot 25.12.2023) [Code of the Russian Federation on Administrative Offenses of 30.12.2001 №195-FL (ed. of 25.12.2023)].
18. *Bikshanov P.* Maskirovochnaya SHBD-set'. Kak vladel'tsy nerazreshennykh besprovodnykh RES skryvayut svoi ustroystva [Masking SHBD network. How owners of unauthorized wireless RPS hide their devices], *Radiochastotnyy spektr* [Radio Frequency Spectrum], 2017, No. 8, pp. 44-46.

19. Postanovlenie Pravitel'stva Rossiyskoy Federatsii ot 31.12.2021 № 2607 «Ob utverzhdenii Pravil okazaniya telematicheskikh uslug svyazi» [Resolution of the Government of the Russian Federation No. 2607 dated 31.12.2021 "On Approval of the Rules for the Provision of Telematic Communication Services"].
20. *Zharov A.A.* Publichnyy Wi-Fi vykhodit iz teni [Public Wi-Fi comes out of the shadows], *Radiochastotnyy spektr* [Radio Frequency Spectrum], 2016, No. 10, pp. 15-16.
21. Postanovlenie Pravitel'stva RF ot 14 maya 2014 g. № 434 «O radiochastotnoy sluzhbe» [Resolution of the Government of the Russian Federation of May 14, 2014, No. 434 "On Radio Frequency Service"].
22. Federal'nyy zakon ot 27.07.2006 № 149-FZ «Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii» [Federal Law No. 149-FL dated 27.07.2006 "On Information, Information Technologies and Information Protection"].

Статью рекомендовал к опубликованию д.т.н., профессор В.В. Курейчик.

Дьяков Антон Владимирович – Южный федеральный университет; e-mail: adyakov@sfedu.ru; г. Таганрог, Россия; аспирант.

Румянцев Константин Евгеньевич – e-mail: rke 2004@mail.ru; тел.: +78634371902; кафедра информационной безопасности телекоммуникационных систем; зав. кафедрой; д.т.н.; профессор.

Dyakov Anton Vladimirovich – Southern Federal University; e-mail: adyakov@sfedu.ru; Taganrog, Russia; graduate student.

Rumyantsev Konstantin Evgenyevich – e-mail: rke2004@mail.ru; phone: +78634371902; the department of information security of telecommunication systems; head of department; dr. of eng.sc.; professor.