S. V. Lebedev, M. G. Panteleyev
Saint Petersburg Electrotechnical University «LETI»

D. V. Skorikov
Research and Engineering Center of Saint Petersburg Electro-Technical University JSC (REC ETU SEC JSC)

CONSTRUCTION OF KNOWLEDGE BASES FOR ANALYTICAL WORK MAINTENANCE IN THE REALM OF INTERNATIONAL WEAPON REDUCTION TREATIES

A problem of developing the ontology-based approach for knowledge base maintenance in the realm of international weapon reduction treaties is discussed. Knowledge bases are used to support shared situation awareness that enables rational and coordinated decision making. Such knowledge bases are formalized with the help of ontology languages. Thanks to formalization such knowledge can be processed with machines and transmitted through a network. Knowledge bases are built continuously based on the incoming information. To support this process an ontology-based architecture is suggested. The architecture is evaluated on a Strategic Arms Reduction Treaty domain fragment. Examples of ontologies construction are shown. The usage of ontology-oriented instruments for building, storage, extraction and visualization of knowledge is demonstrated.

Weapon reduction treaties, unified information and analytical system, knowledge base, ontology

УДК 304.444

В. Гарате Гонзалес
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)

Применение передовой методологии безопасности в беспроводных сетях

Предложена методология по улучшению безопасности беспроводных сетей, сформированная на основе методологии непрерывного совершенствования и практического опыта в данной отрасли с целью обеспечения высокого уровня безопасности при проектировании и развертывании беспроводных сетей. Рассматриваются способы защиты от распределенных беспроводных компьютерных атак и подчеркивается важность наличия политики беспроводной безопасности организации, а также компетентность персонала. Методология способствует формированию процессного подхода к созданию, внедрению, эксплуатации, мониторингу, проверке, поддержанию и совершенствованию политики безопасности беспроводных сетей организаций. Методология обеспечивает надежную модель для реализации принципов безопасности, регулирующих оценку рисков, разработку и реализацию мер безопасности, управление безопасностью и переоценку. Информационная безопасность играет важную роль в выравнивании бизнеса компании со своей стратегией информационной технологии, и в этом контексте информационная безопасность имеет первостепенное значение, поскольку она помогает компаниям внедрять экономически эффективные меры безопасности.

Беспроводные сети, проектирование, моделирование, методология, шифрование, беспроводная инфраструктура

В настоящее время беспроводные сети (WLAN) в стандарте 802.11, который был опубликован в 1997 г. Институтом инженеров по электротехнике и электронике (IEEE), по-прежнему являются одной из технологий, широко используемых в любом сценарии, когда необходим обмен информацией (дома, на работе, в общественных и частных организациях, образовательных центрах) и можно воспользоваться предоставляемыми преимуществами (мобильность, масштабируе-

мость, гибкость, экономия средств, сокращение времени установки и т. д.). При этом существуют проблемы проектирования, внедрения и администрирования в отношении безопасности при использовании данной технологии.

В университете «Инка Гарсиласо де ла Вега» данную задачу решить сложнее, поскольку он предлагает услуги для разных типов пользователей, в отличие от бизнес-компаний, для передачи академической информации как студентов, преподавателей, факультетов, так и исследователей. Отсутствие учета требований безопасности при внедрении беспроводной технологии WLAN в локальной сети привело к проблемам безопасности, которые влияют не только на технологию WLAN, но и на проводную локальную сеть (IEEE 802.3).

Как указано в OSSTMM [1], «The information to be found within the wireless spectrum is not limited to product specifications». («Информация, содержащаяся в беспроводном спектре, не ограничивается спецификациями продукта».) Возникающие при этом проблемы безопасности связаны:

– с отсутствием или низкой политикой безопасности в беспроводных средах;

– отсутствием физической безопасности периметра беспроводных устройств (AP – точки доступа, контроллеров и т. д.);

– интерференцией электромагнитных сигналов при использовании общих устройств (принтеры, микроволны и т. д.);

– плохой практикой поддержания стандартной конфигурации продуктов или услуг;

– устаревшими системами, программным обеспечением, прошивками и приложениями, необходимыми для работы;

– недостатком знаний технического персонала и пользователей беспроводных сетей;

– использованием недостаточных протоколов аутентификации и авторизации;

– использованием слабых протоколов шифрования, легко настраиваемых, для удобства техников.

На основе критерия ISO/IEC 27001: 2013 [2] «Система управления информационной безопасностью сохраняет конфиденциальность, целостность и доступность информации путем применения процесса управления рисками и дает уверенность заинтересованным сторонам в том, что риски адекватно управляются» важно защитить важнейшие активы организации, такие, как служебная информация организации и персональные данные, созданные в среде высшего учебного заведения техническими методами защиты информации от следующих действий со стороны злоумышленников:

– получение личной информации, поскольку в беспроводной сети есть сведения о приложениях, банковской и финансовой информации, ноу-хау и т. д.;

– использование беспроводной сети для совершения компьютерных преступлений или противоправных действий, оставляя ложный след;

– выполнение маскированных атак с помощью интернета вещей (IoT);

– удаленный контроль компьютеров с помощью вредоносных программ, а также через социальную инженерию;

– сканирование сетевых ресурсов в поисках информации, которая ставит под угрозу организацию (патенты, расследования, привилегированные обращения, секретные документы и т. д.).

Техническая база. Беспроводная локальная сеть (WLAN) – это сеть, в которой ряд устройств (ПК, рабочие станции, принтеры, серверы, ноутбуки и т. д.) обмениваются данными друг с другом посредством радиосигналов, распространяющихся через воздух, без необходимости прокладки кабелей» [3]. К этому надо добавить IoT – сеть физических объектов, транспортных средств, машин, бытовой техники и т. д., которые используют датчики и API для подключения и обмена данными через Интернет.

Собранная статистика показывает аспекты внедрения беспроводных технологий, которые каким-то образом влияют на вопросы информационной безопасности:

– большинство компаний планирует увеличить пропускную способность Wi-Fi не менее чем на 20 % в 2019 г.;

– 2/3 компаний позволяют своим сотрудникам сегодня приносить свои устройства в компанию;

– атака Wi-Fi в открытой сети может занять менее 2 с;

– в ближайшие годы будет создано более 7 млрд новых устройств с Wi-Fi;

– 11ac / Wave2 настроен на скорость беспроводной связи в несколько гигабайт;

– 90 % всех смартфонов оснащены возможностями Wi-Fi;

– 71 % всех потоков мобильной связи осуществляется через Wi-Fi;

– 90 % людей перемещаются между устройствами для достижения цели;

– 79 % пользователей смартфонов используют телефон по 22 ч в день;

– 90 % сотрудников (в развитых странах) используют свое оборудование (BYOD) каким-то образом для доступа к информации о компании;

– 80 % компаний не предоставляют образование/обучение в BYOD;

60 % компаний не имеют письменной политики BYOD;

– 80 % операционных систем на рынке смартфонов – Android;

– 79 % всех вредоносных программ для смартфонов – в приложениях Android.

К 2020 г. ожидается, что к Интернету подключится 24 млрд устройств. Подавляющее большинство будет использовать некоторую форму беспроводного доступа.

Топологии. Режим ***AD HOC*** – это набор независимых базовых услуг, когда связь между двумя беспроводными устройствами не требуется, при этом нет необходимости в промежуточном сетевом оборудовании (рис. 1). Вариант сетей ad hoc – это тот, который обеспечивается смартфоном, способным предлагать временную зону беспроводной связи для доступа к Интернету [3].

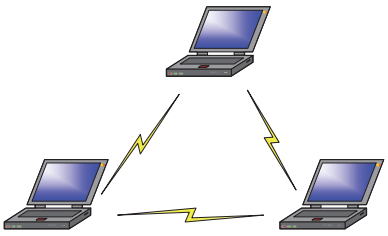

Рис. 1

В режиме ***инфраструктуры*** с точкой доступа (AP) связь между устройствами происходит только через AP. Через нее осуществляется выход во внешние проводные сети. Такой режим позволяет транслировать мультимедийную информацию для работы в Интернете, и может быть создано несколько точек доступа, объединенных проводной сетью Ethernet (рис. 2). Фактически такая сеть представляет набор базовых станций с перекрывающимися зонами охвата. AP могут иметь доступ к Интернету также через беспроводную сеть WiMAX [3].

Риски безопасности. В настоящее время все больше беспроводных сетей 802.11 (WLAN) реализуются для удовлетворения потребностей каких-либо организаций, когда необходимо и важно понимать различные типы угроз и уязвимостей, которые эта технология влечет за собой, с целью реализации контроля или соответствующих мер безопасности в соответствии с передовой практикой и отраслевыми стандартами. Большинство из этих проблем безопасности являются «врожденными» для стандарта 802.11 и влияют на конфиденциальность, целостность и доступность информации [4].

Отсутствие конфиденциальности. Из-за использования радиоволн для передачи данных в общедоступных средствах трудно гарантировать конфиденциальность, так как этот канал облегчает несанкционированный доступ к сети, являясь шлюзом в локальную вычислительную сеть (ЛВС) организации, благодаря чему возможна утечка информации, находящейся в ней.

Одна из атак, ставящих под угрозу конфиденциальность, – «**Подслушивание**», которое является перехватом в режиме реального времени неавторизованного частного сообщения (телефонный звонок, мгновенное сообщение, видеоконференция, просмотр в Интернете или использование веб-приложений).

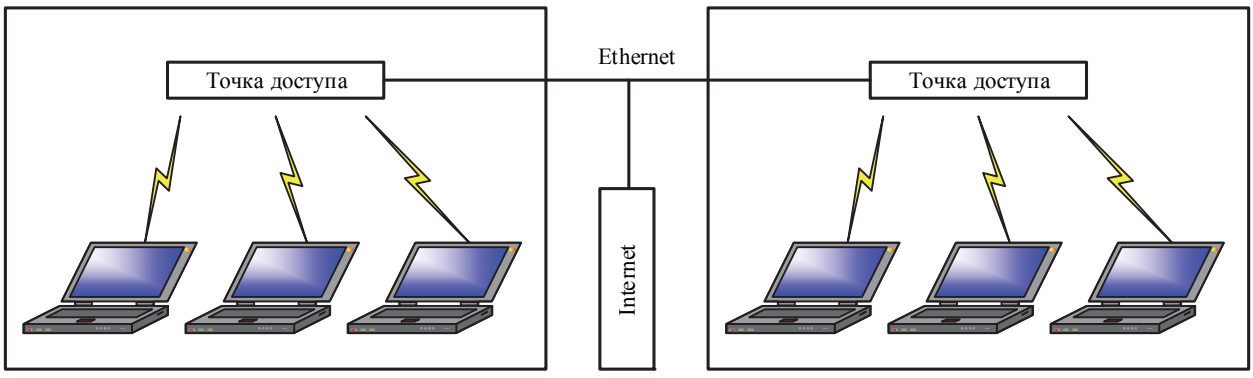

Рис. 2

Контроль	Описание
OWISAM-TR-001	Открытая сеть связи Wi-Fi
OWISAM-TR-002	Наличие WEP-шифрования в сетях связи
OWISAM-TR-003	Алгоритм генерации небезопасных ключей устройства (пароли и WPS)
OWISAM-TR-004	Ключи WEP/WPA/WPA2 на основе словаря
OWISAM-TR-005	Небезопасные механизмы аутентификации (LEAP, PEAP-MD5, …
OWISAM-TR-006	Устройство с поддержкой Wi-Fi защищенной установки Active PIN (WPS)
OWISAM-TR-007	Сеть Wi-Fi, не уполномоченная организацией
OWISAM-TR-008	Небезопасный портал горячих точек
OWISAM-TR-009	Клиент пытается подключиться к небезопасной сети
OWISAM-TR-010	Диапазон охвата сети слишком обширен

Отсутствие целостности. Атака, которая нарушает целостность, – это изменение содержания данных в сообщении, благодаря чему возникает отличие его от первоначально отправленного сообщения [4]. Например, злоумышленник может изменить последовательность проверки кадров (FCS), пересчитав значение захваченного сообщения и изменив его для повторной передачи. FCS помогает проверять ошибки во время передачи сообщения посредством вычисления хеш-функции всего сообщения на основании известных алгоритмов.

Отсутствие доступности. Оно часто связано с DoS-атакой на отказ в обслуживании. Известные методы атаки: блокировка и флудинг делают беспроводную сеть не пригодной для использования законными клиентами, которым требуются предлагаемые услуги или ресурсы. Преднамеренное вмешательство вызывает интерференцию спектра за счет внешнего излучения сигналов высокой мощности, а флудинг насыщает точки доступа или беспроводного клиента большим количеством сообщений, вызывающим деградацию или полное прерывание связи в сети.

OWISAM 2013 (Открытая методология оценки безопасности беспроводной сети) находится в черновом варианте, она основана на структуре проекта OWASP (Открытый проект безопасности веб-приложений) и CVSS (Общая система подсчета уязвимостей). Это открытая методология, созданная для стандартизации процессов анализа беспроводной сети, объективного оценивания рисков и защиты корпоративных сетей.

В [5] приведена ТОП-10 угроз безопасности, наиболее часто встречающихся в организациях, где ЛВС являются беспроводными сетями WLAN, которые должны быть приоритетными и подлежат устранению. Далее перечислены 10 основных угроз безопасности (таблица).

Идентификация требований. Для идентификации технологий, архитектуры, ролей и необходимого содержимого беспроводных сетей WLAN в университетском городке вуза, согласно своей организационной модели, реализовано 3 разных типа беспроводных сетей с доступом к Интернету:

1. Академическая сеть. Эта сеть была создана для академического и исследовательского сообщества и позволяет пользователям данных учреждений поддерживать подключение к Интернету из своего собственного кампуса или других учреждений с их институциональными полномочиями пользователей. При аутентификации и авторизации используют протокол RADIUS, который был внедрен каждым учреждением. Аутентификация достигается за счет использования доменов, например user1@uigv.edu.pe, user2@instb.edu.pe, user3@instc.edu.pe, которые через прокси-сервер высокого уровня RADIUS перенаправляют запросы на различные учреждения в зависимости от домена. Безопасность находится в соответствии с протоколом 802.11i с WPA2 типа инфраструктуры EAP-TLS на рис. 3.

2. Сеть с порталом. Эта сеть использует следующий метод проверки подлинности. Клиент использует сертификат безопасности сервера (SSL), где пользователь обычно будет обращаться к беспроводной сети. Как только соединение будет установлено, оно будет перенаправлено на страницу аутентификации. После ввода учетных данных пользователя беспроводной контроллер (WLC) через протокол RADIUS запросит проверку учетных данных на сервере Active Directory (AD), где расположены все профили пользователей. Активный каталог после проверки подлинности пользователя отправит маркер авторизации на RADIUS-сервер или укажет, что учетные данные недействительны. Безопасность предоставляется в соответствии с протоколом 802.11i с

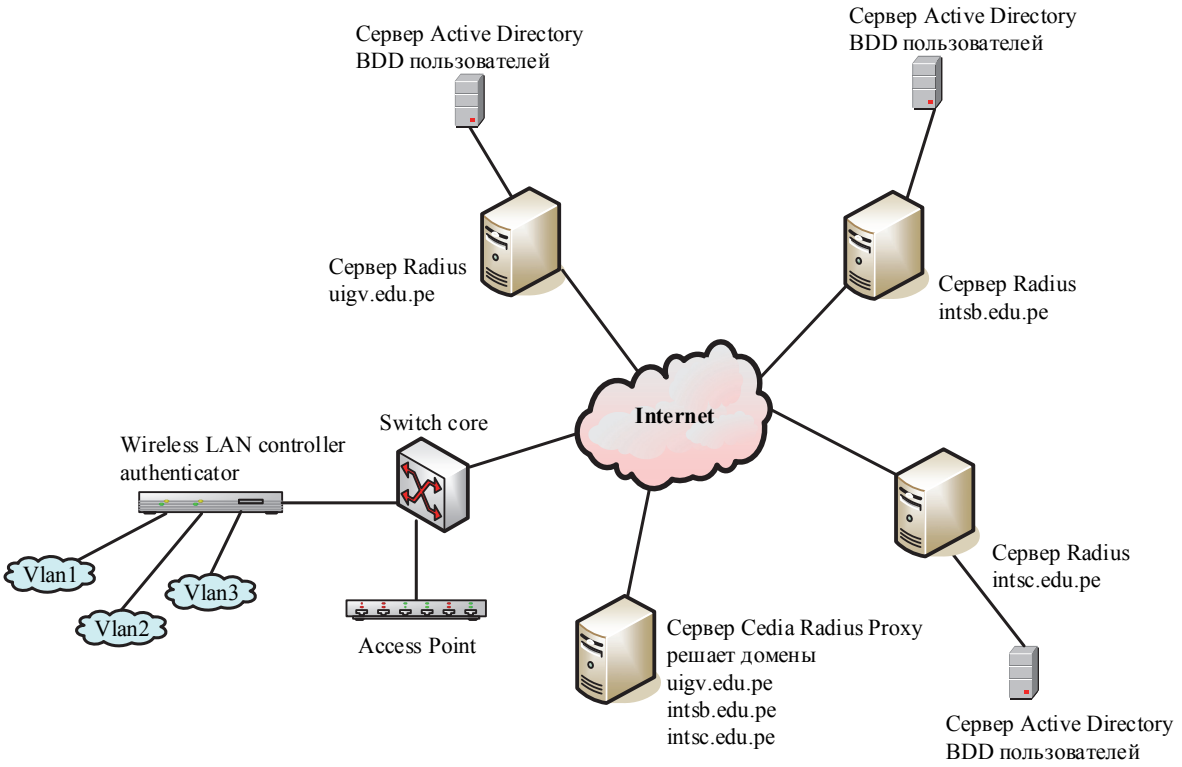

Рис. 3

WPA2 режимом инфраструктуры со специальным порталом.

3. Классные сети. Эта сеть эксплуатируется преподавателями на компьютерах в классах всех специальностей, она использует фильтрацию MAC-адресов с предварительно открытым ключом TKIP и протоколом безопасности WPA2-Personal.

Предлагаемая методология. При проектировании беспроводных сетей необходимо создавать меры безопасности совместно с уровнями безопасности проводной сети 802.3. В случае сбоя безопасности другие уровни стратегии защиты должны обеспечивать защиту сети. Следующий подход не описывает подробно все возможные соображения проектирования и реализации для развертывания беспроводной сети. Однако эта методология пытается дать ссылку на основные соображения для разработки и внедрения защищенной корпоративной WLAN.

Эта методология основана на модели непрерывного совершенствования Деминга, называемой Plan-Do-Check-Act, циклом PDCA, которая помогает генерировать базовую линию с инкрементной характеристикой качества (рис. 4). Критерий информационной безопасности реализуется на основе создания политики безопасности на базе общих сценариев реализации беспроводной сети, которые обеспечат основные элементы безопасности: конфиденциальность, целостность и доступность. Анализ рисков помогает определить правильность использования элементов управления и смягчить инциденты, которые могут поставить под угрозу ключевые элементы безопасности. Компоненты системы безопасности показаны на рис. 4.

Политика. Необходимо создать корпоративную политику по внедрению и использованию беспроводной сети [6]. Чрезмерные правила безопасности могут привести к снижению полезности и скорости работы сети.

1. Планирование. Внутри организации важно разумно управлять информационными ресурсами (аппаратное обеспечение, программное обеспечение, прошивка, службы, приложения, связь, персонал и т. д.), которые соответствуют технологии WLAN. Организация должна определить методологию, позволяющую оценивать риски, определять их, анализировать и обрабатывать, а также выделять ресурсы, которые считаются критическими для организации. Организация должна выявлять потенциальные угрозы для активов в отношении элементов безопасности: конфиденциальности, целостности, доступности и аутентичности, которые могут привести к повреждению или потере информации при возникновении события. Согласно NIST типы источников угрозы следующее:

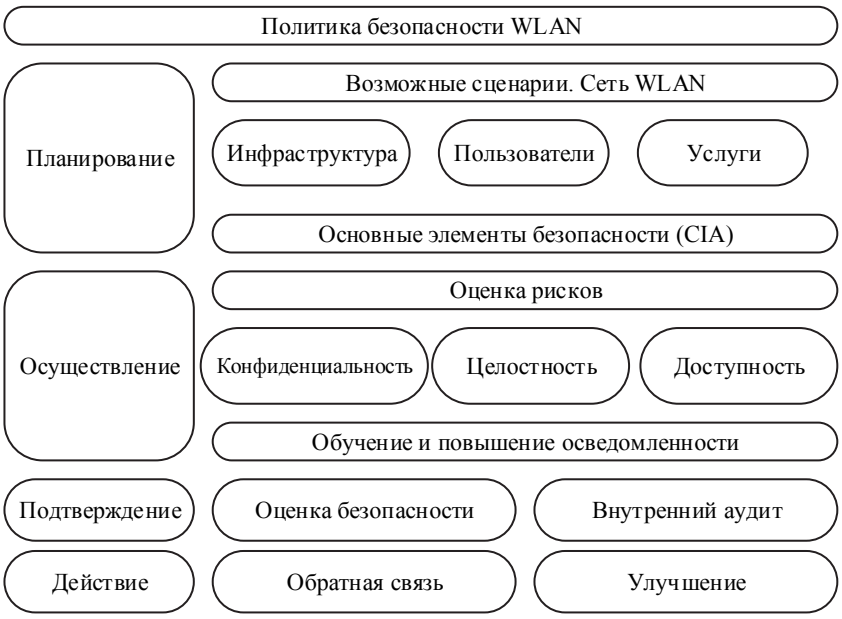

Рис. 4

– кибер-вымогательство или физические атаки;

– человеческие ошибки;

– структурные сбои ресурсов, контролируемых организацией (например, аппаратное обеспечение, программное обеспечение и экологический контроль);

– стихийные бедствия, а также несчастные случаи и неудачи, не зависящие от организации.

2. Осуществление. Организация должна определить, какие риски существуют или могут произойти со всеми возможными характеристиками, временем, продолжительностью и возможными положительными или отрицательными результатами. Анализ рисков позволяет обеспечить входные данные для оценки риска, и организация может принимать соответствующие меры. Кроме того, предоставляются критерии принятия решений, связанных с различными видами риска. Этот шаг состоит в определении и принятии решений, основанных на идентификации и анализе рисков, для смягчения рисков и определения приоритета в реализации их устранения.

Для реализации элементов управления рассматривается методология OWISAM, о которой упоминалось ранее в соответствии с возможными сценариями беспроводных сетей.

3. Подтверждение. На этом этапе важно рассмотреть вопрос о найме профессионального персонала в области компьютерной безопасности (pentester), чтобы провести тест вторжений с конфигурацией инфраструктуры беспроводной сети для определения и смягчения потенциальных уязвимостей и рисков. Этот тест на проникновение должен применяться с помощью метода тестирования с использованием серого ящика, который позволяет профессионалу по безопасности начинать с технической информации о инфраструктуре WLAN и смоделировать реальную атаку, причем этот тест считается наиболее эффективным при определении большого количества угроз. В качестве последующей или оценочной практики важно провести внутренний или внешний аудит, предпочтительно для архитектуры и беспроводной инфраструктуры. Для этого важно, чтобы он был смоделирован в руководстве по методам тестирования безопасности с открытым исходным кодом (OSSTMM 3) в его разделе «Тест безопасности беспроводной сети» или методологии открытой оценки безопасности беспроводной сети OWISAM.

4. Действие. Этот этап заключается в том, что все найденные или реальные и потенциальные несоответствия, которые могут повлиять на функционирование, должны быть обработаны как в тесте вторжения, так и в отчетах об аудите или инцидентах по областям организации, пользователям, сотрудникам и т. д. Важно, чтобы требования (средства контроля, процессы, клиенты, юридические и т. д.) были указаны явно в количественном, временном, выборочном соотношении и на основании доказательной базы для исключения всех неясностей.

В настоящее время сети WLAN сталкиваются с различными типами угроз высокого уровня, которые включают атаки по анализу трафика, маскировки, человека посредине, отказа в обслуживании, подслушивания, модификации сообщений и т. д. Эти инциденты в основном происходят между рабочей станцией и точкой доступа. Внедрение этой методологии послужит руководством для развертывания новых WLAN или улучшения существующих, обеспечивая ключевые элементы безопасности и поддерживая приемлемую безопасность в организации, что позволяет противостоять большинству существующих угроз.

Руководство организаций должно пересматривать политику беспроводной безопасности организации не реже одного раза в год, чтобы обеспечить ее постоянную готовность, адекватность и эффективность реакции на постоянно увеличивающееся количество внешних угроз. Подходы к пересмотру включают в себя оценку возможностей для дальнейшего улучшения и внесения изменений в политику безопасности беспроводной связи для обеспечения и поддержания высокого уровня информационной безопасности организации. Политика обеспечения безопасности и результаты проверок беспроводной связи должны быть четко прописаны и задокументированы.

Цель данной статьи – помочь администраторам безопасности, специалистам служб безопасности и другим лучше понять важность компьютерной безопасности и обязанностей, которые она предполагает.

СПИСОК ЛИТЕРАТУРЫ

1. OSSTMM 3. URL: (http://www.isecom.org/mirror/OSSTMM.3.pdf/ (дата обращения 24.01.2019).

2. ISO/IEC 27001:2013(en). URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en/ (дата обращения 24.01.2019).

3. IEEE 802.11. URL: https://ru.bmstu.wiki/IEEE_802.11.https://ru.bmstu.wiki/IEEE_802.11/ (дата обращения 24.01.2019).

4. Best Practices for Enterprise Security. URL: https://msdn.microsoft.com/es-es/cc750076/ (дата обращения 24.01.2019).

W. Garate Gonzales
Saint Petersburg Electrotechnical University «LETI»

APPROACH OF THE ADVANCED METHODOLOGY OF SECURITY IN WIRELESS NETWORKS

Proposes a methodology for improving the information security process of wireless data networks based on a continuous improvement methodology and industry best practices in order to provide a chain of information security recommendations for designing and possible deploying of wireless data networks. It discusses the ways of protection against distributed wireless computer attacks, internal and external attacks, and stresses the importance of the organization's wireless security policy, as well as staff training. This approach promotes the adoption of a process approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's wireless data security policy. This methodology provides a robust model for implementing the security guidelines governing risk assessment, information security design and implementation, information security management and reassessment. Information security has an important role in aligning the company's business with its information technology strategy, and in this context, information security is paramount, as it helps companies implement cost-effective information security measures.

Wireless networks, design, modeling, methodology, encryption, wireless infrastructure