На правах рукописи

Иващук Ирина Юрьевна

Модель и метод построения семейства профилей защиты для беспроводной сети

Специальность 05.13.19.
Методы и системы защиты информации,
информационная безопасность

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Санкт-Петербург
2010

Работа выполнена в Санкт-Петербургском Государственном университете информационных технологий, механики и оптики на кафедре “Безопасные информационные технологии”

Научный руководитель: кандидат технических наук, доцент
Птицын Алексей Владимирович

Официальные оппоненты: доктор технических наук, профессор,
Гольдштейн Борис Соломонович

доктор технических наук, профессор,
Воробьев Владимир Иванович

Ведущая организация: Закрытое акционерное общество «Эврика»

Защита диссертации состоится « » 2010 г. в 15 часов 50 минут на заседании диссертационного совета Д.212.227.05 в Санкт-Петербургском государственном университете информационных технологий, механики и оптики
Адрес: 197101, г. Санкт-Петербург, Кронверкский пр., д. 49.

С диссертацией можно ознакомиться в библиотеке Санкт-Петербургского государственного университета информационных технологий, механики и оптики.

Автореферат разослан « » 2010 г.

Учёный секретарь
диссертационного совета
Д.212.227.05
к.т.н., доцент
_____В.И.Поляков

Общая характеристика работы

Актуальность темы исследования

Актуальность настоящего исследования подтверждается тем, что стандартизация требований безопасности является одной из важных и трудных задач, стоящих перед специалистами по информационной безопасности.

Беспроводные технологии с каждый годом становятся все более незаменимы в современной жизни человека. В первую очередь это связано с все возрастающими требованиями к мобильности сотрудников, которая непосредственно влияет на скорость принятия решений по важным для компании вопросам. Но при множестве плюсов беспроводных технологий передачи данных, имеется один существенный минус: открытая среда передачи информации, которая ведет к возможности беспрепятственного перехвата кодированных потоков, передающихся по сети. Увеличение доли информации, передаваемой по беспроводным каналам, влечет за собой и увеличение доли атак на беспроводные сети. Именно по этой причине столь важен вопрос защиты информации при ее передаче по радиоканалам.

Но зачастую, учитывая жесткую конкуренцию между компаниями на внутреннем и внешнем рынках страны, одной защиты информации оказывается недостаточно. Необходимо еще документально подтвердить, что беспроводная сеть, посредством которой осуществляется передача данных, на самом деле безопасна и отвечает предъявляемым к ней требованиям безопасности. Именно в этот момент возникает следующий вопрос: сертификация сети в соответствии с необходимым классом защищенности.

Создание модели семейства профилей защиты для беспроводной сети позволит значительно упростить и ускорить процесс сертификации данного вида сетей, что влечет за собой увеличение доверия к самой сети со стороны как внешних, так и внутренних пользователей.

Разработка метода определения уровня доверия к беспроводной сети на основе реализованных в ней механизмов защиты информации также является актуальной задачей, так как позволит оценить защищенность сети, как на этапе ее построения, так и в ходе проведения аудита защищенности сети.

Цели и задачи диссертации

Целью диссертационной работы является разработка модели семейства профилей защиты и метода построения семейства профилей защиты для беспроводной сети.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Провести обзор существующих стандартов семейства IEEE 802.11 и описанных в них механизмов защиты информации;
2. Построить модель семейства профилей защиты для беспроводной сети;
3. Разработать систему критериев оценки защищенности беспроводной сети, основывающуюся на реализованных в ней механизмах защиты согласно семейству стандартов IEEE 802.11, с учетом специфики ее построения;
4. Разработать новую систему уровней доверия к беспроводной сети, основанную на системе оценочных уровней доверия ГОСТ Р ИСО/МЭК 15408;
5. Разработать метод построения семейства профилей защиты для беспроводной сети на основе модели семейства профилей защиты для нее с целью последующей ее сертификации согласно требованиям безопасности ГОСТ Р ИСО/МЭК 15408;

Предмет исследования

Предметом исследования является комплекс вопросов обеспечения информационной безопасности данных при их передаче по радиоканалам в рамках структуры беспроводной сети.

Объект исследования

Объектом исследования являются модель семейства профилей защиты для беспроводной сети и метод построения семейства профилей защиты для беспроводной сети, исходя из реализованных в ней механизмов защиты согласно семейству стандартов 802.11 и с учетом требований безопасности ГОСТ Р ИСО/МЭК 15408.

Методы исследования

При решении поставленных задач были использованы: методы теории графов, теории множеств, математической индукции, теории интегрального исчисления, статистические и графические методы.

Основные научные положения, выносимые на защиту

1. Модель семейства профилей защиты для беспроводной сети;
2. Методика построения профиля защиты для беспроводной сети на основе метода построения семейства профилей защиты для данного вида сетей;
3. Методика проведения аудита защищенности беспроводной сети.

Основные результаты работы

Проведен обзор существующих стандартов семейства IEEE 802.11 и реализованных в них механизмов защиты информации.

Построена модель семейства профилей защиты для беспроводной сети на основе реализованных в ней механизмов защиты информации, а также разработан метод построения семейства профилей защиты для беспроводной сети базирующийся на этой модели.

Разработана методика аудита защищенности беспроводной сети и присвоения ей соответствующего уровня доверия, исходя из требований безопасности ГОСТ Р ИСО/МЭК 15408.

Предложены варианты использования разработанных модели и метода для сертификации беспроводной сети и разработанной системы уровней доверия для проведения аудита защищенности беспроводной сети.

Научная новизна

Научная новизна данной диссертационной работы обусловлена:

1. разработкой новой системы критериев оценки защищенности беспроводной сети на основе реализованных в ней механизмов защиты в соответствии с семейством стандартов 802.11;
2. разработкой новой системы уровней доверия к беспроводной сети, основывающейся на оценочных уровнях доверия ГОСТ Р ИСО/МЭК 15408;
3. построением модели семейства профилей защиты для беспроводной сети;
4. разработкой метода построения семейства профилей защиты для беспроводной сети;
5. разработкой методики проведения аудита защищенности беспроводной сети.

Практическая ценность

Практическая ценность данной диссертационной работы заключается в том, что на основании описанной в ней модели семейства профилей защиты для беспроводной сети возможна разработка специализированных руководящих документов для сертификации беспроводных сетей по требованиям безопасности. Также разработанная в ней методика аудита защищенности беспроводной сети позволит значительно сократить затраченные временные и трудовые ресурсы при его проведении и в процессе сертификации данного вида сетей.

Апробация работы

Основные положения и результаты диссертационной работы докладывались и обсуждались на семинарах кафедры БИТ и конференциях:

- на XI Научно-практической конференции «Теория и технология программирования и защиты информации» (Санкт-Петербург, май 2007)
- на научно-технической конференции «День антивирусной безопасности» (Санкт-Петербург, октябрь 2007)
- на V Межвузовской конференции молодых ученых (Санкт-Петербург, апрель 2008)
- на XXXVIII научной и учебно-методической конференции СПбГУ ИТМО (Санкт-Петербург, февраль 2009)
- на VI Межвузовской конференции молодых ученых (Санкт-Петербург, апрель 2009)
- на XIV Научно-практической конференции «Теория и технология программирования и защиты информации» (Санкт-Петербург, май 2009)
- на VI Межрегиональной конференции «Информационная безопасность регионов России» (Санкт-Петербург, октябрь 2009)
- на VII Межвузовской конференции молодых ученых (Санкт-Петербург, апрель 2010)

Внедрение результатов

Разработанные модель и метод построения семейства профилей защиты для беспроводной сети использованы при проведении исследования безопасности беспроводной сети ООО «ГК «Рубеж 92» и построения для нее профиля защиты, при проведении исследования безопасности беспроводной сети ОАО «Завод железобетонных изделий №1», в учебном процессе кафедры «Безопасные информационные технологии» СПбГУ ИТМО по специальности 090103 в лекционных и практических курсах «Технология сертификации средств защиты информации» и «Телекоммуникационные технологии».

Публикации по теме диссертации

По материалам диссертации опубликовано восемь печатных работ.

Структура и объем диссертации

Диссертация состоит из введения, четырех глав, заключения и списка литературы. Материал изложен на 133 страницах машинописного текста, содержит 22 рисунка и 22 таблицы, список литературы состоит из 70 наименований.

Содержание работы

Во введении обосновывается актуальность темы исследования и научная новизна работы, обозначены цели и задачи диссертации, определены основные положения, выносимые на защиту.

В первой главе проведен обзор существующих стандартов семейства IEEE 802.11 и описанных в них механизмов защиты информации, также обозначены основные виды угроз для беспроводных сетей (БС).

В первом разделе дан обзор процесса развития технологий беспроводной связи, рассмотрены основные этапы ратификации стандартов IEEE 802.11. Также приводятся основные режимы работы сети.

Во втором разделе рассматриваются официально принятые механизмы аутентификации в беспроводных сетях и закрепленные посредством семейства стандартов 802.11.

Изначально стандарт IEEE 802.11 предусматривал два механизма аутентификации беспроводных абонентов: открытую аутентификацию и аутентификацию с общим ключом.

В дальнейшем для аутентификации в сети используется протокол EAP. Различные производители создали свои реализации протокола EAP для обеспечения безопасности беспроводных сетей (табл.1).

Табл.1 Реализации протокола EAP

Протокол	Аутенти-фикация по паролю	Сертификат клиента	Сертификат сервера	Динами-ческий обмен ключами	Взаимная аутенти-фикация
EAP-MD5	√				
LEAP	√			√	√
EAP-TLS		√	√	√	√
PEAP	√		√	√	√
EAP-TTLS	√		√	√	√

В третьем разделе рассматриваются основные криптографические алгоритмы, обеспечивающие конфиденциальность и целостность данных при их передаче по беспроводным каналам.

Первоначально широкое распространение в различных системах обеспечения беспроводного доступа к цифровым сетям получил алгоритм WEP, с помощью которого осуществляется шифрование трафика, затрудняющее анализ последнего сканирующей аппаратурой. Для кодирования данных стандарт предоставляет возможности шифрования с использованием алгоритма RC-4 с 40-битным разделяемым ключом.

Но впоследствии было выяснено, что система защиты беспроводной сети, основанная на WEP со статическими ключами и аутентификацией по MAC-адресу устройства, не соответствует условиям безопасной эксплуатации. Это потребовало усовершенствования процедур аутентификации и работы WEP.

Версия WEP2 защищена надежнее своей предшественницы благодаря 128-разрядному вектору инициализации IV и 128-разрядным ключам. В то же время в ней применены прежние алгоритм шифрования RC-4 и схема контроля целостности.

Следующим шагом на пути увеличения безопасности беспроводных сетей является применение нового алгоритма шифрования AES.

AES – это симметричный итерационный блочный шифр, оперирующий блоками данных размером 128 и длинной ключа 128, 192 или 256 бит.

Недостатком алгоритма можно считать лишь примененную в нем нетрадиционную схему - теоретически она может содержать скрытые уязвимости, обнаруживаемые только спустя достаточное количество времени после широкого использования данного алгоритма.

В четвертом разделе рассматриваются основные виды угроз для беспроводных сетей, приводится их классификация.

Анализ существующего положения показывает, что основной причиной нерешительности перехода на беспроводные сети являются проблемы информационной безопасности, уровень которой как для отдельных линий, так и для системы в целом, пока не определен.

Принято считать, что безопасности беспроводных сетей угрожают:

- нарушение физической целостности сети;
- подслушивание трафика;
- вторжение в сеть.

При рассмотрении уязвимостей сетей стандарта 802.11 можно выделить 2 группы угроз: угрозы на сигнальном уровне и угрозы на информационном уровне. Наличие

уязвимостей на сигнальном уровне делает весьма проблематичной защиту информационного уровня, на котором должны быть предотвращены:

- целенаправленное искажение передаваемых и получаемых данных;
- перехват информации, которая может быть использована во вред пользователю;
- перехват управления системой связи или информационной системой.

Во второй главе описана модель построения семейства профилей защиты для беспроводной сети, рассмотрены вопросы моделирования и классификации компонент, учитываемых при создании системы защиты информации в беспроводной сети, проведено математическое моделирование описанной модели. Также разработана система критериев оценки защищенности беспроводной сети.

В первом разделе описывается специфика построения семейства профилей защиты (ПЗ) для сетей стандарта 802.11.

Специфика создания ПЗ для беспроводных сетей базируется на специфике их построения, особенностях конфигурации и технологии обработки и передачи информации. За счет открытой среды передачи данных в БС должны быть усилены требования безопасности, выдвигаемые к объекту оценки (ОО) на этапах аутентификации, контроля доступа и шифрования передаваемой информации (табл. 2).

Табл. 2 Специфика БС в соответствии с требованиями безопасности к ним

Требования к безопасности	**Специфика беспроводных сетей**
Нормативно-правовое обеспечение	Использование беспроводных сетей попадает под действие как российских, так и международных нормативных актов. Кроме того, поскольку в беспроводных сетях интенсивно используется шифрование, а применение криптографических средств защиты в ряде случаев попадает под довольно жесткие законодательные ограничения, необходимо заранее определить категорию информации, с которой предполагается работать по средствам БС и те механизмы защиты, которые предполагается использовать для ее защиты.
Безопасность среды	В связи с отрытой природой каналов передачи данных БС накладывается ряд ограничений на передаваемую информацию в зависимости от ее ценности и на допустимую дальность ее распространения.
Разделение сетей	В связи со спецификой БС желательно выделять точки беспроводного доступа в отдельный сетевой сегмент с помощью межсетевого экрана, особенно когда речь касается гостевого доступа.
Использование криптографических средств защиты	Должны быть определены используемые протоколы и алгоритмы шифрования трафика в беспроводной сети (WEP или AES). Также должны быть определены требования к протоколам ЭЦП и длине ключа подписи сертификатов, используемых для различных целей.
Аутентификация	Должны быть определены требования к хранению данных аутентификации, их смене, сложности, безопасности при передаче по сети. Могут быть явно определены используемые методы EAP, методы защиты общего ключа сервера RADIUS.

Продолжение табл. 2

Требования к безопасности	Специфика беспроводных сетей
Допустимость использования программного и аппаратного обеспечения	Должны быть отдельно специфицированы требования к точкам доступа, беспроводным коммутаторам и клиентам беспроводной сети.
Обнаружение атак	Должны быть определены требования к системам обнаружения беспроводных атак, закреплена ответственность за анализ событий.
Удаленный доступ к сети	В большинстве случаев пользователей беспроводной сети логично относить к пользователям систем удаленного доступа. Это обусловлено аналогичными угрозами и как следствие - контрмерами, характерными для данных компонентов ИС.

Во втором разделе происходит построение графо-аналитической модели структуры семейства профилей защиты в соответствии с ГОСТ Р ИСО/МЭК 15408.

В Руководящем документе Гостехкомиссии РФ «Безопасность информационных технологий. Руководство по формированию семейств профилей защиты» от 2003 года семейство ПЗ определяется как совокупность упорядоченных взаимосвязанных ПЗ, которые относятся к определенному типу изделий ИТ.

Все ПЗ в семействе связаны иерархическими связями, т.е. каждый последующий наследует все компоненты предыдущего, усиливая их.

Первоочередной задачей для получения базового функционального пакета (БФП) семейства ПЗ является исследование множества ОО и получение общего для него набора функциональных требований безопасности (ФТБ).

В качестве ОО при разработке ПЗ для БС рассматривается вся сеть, а не отдельные ее сегменты или рабочие места с интегрированными беспроводными адаптерами.

Объединив понятия ПЗ и БФП семейства ПЗ, построим схему формирования ПЗ на основе выработанного для семейства БФП (рис. 1).

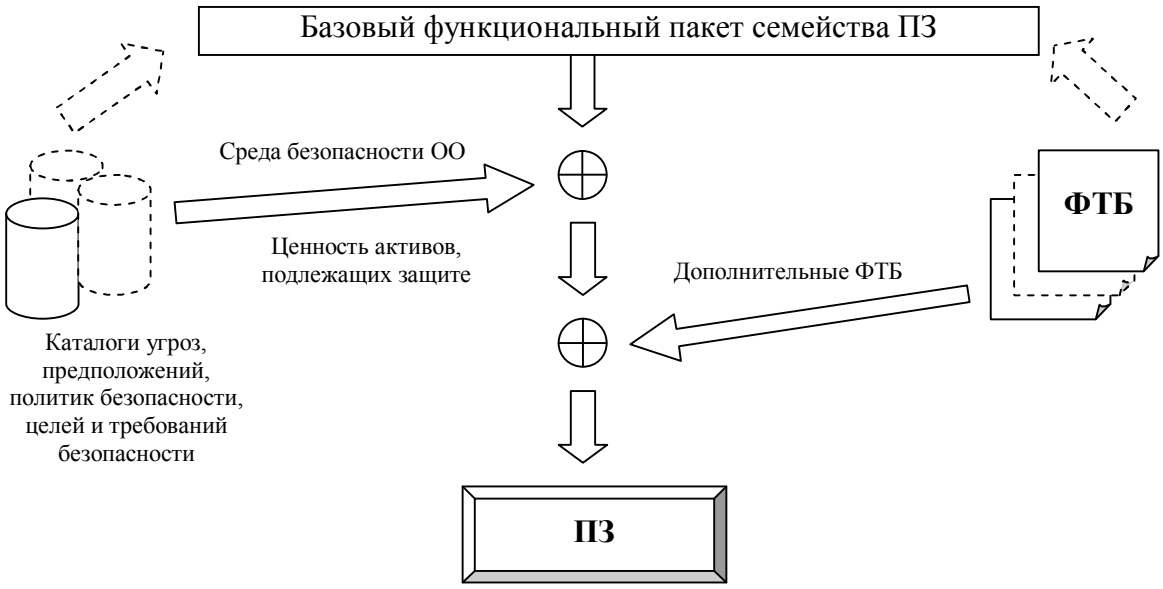

Рис. 1 Схема формирования профиля защиты

Исходя из приведенной выше структуры типового ПЗ и прибегая к теории графов, построим в общем виде модель данной структуры:

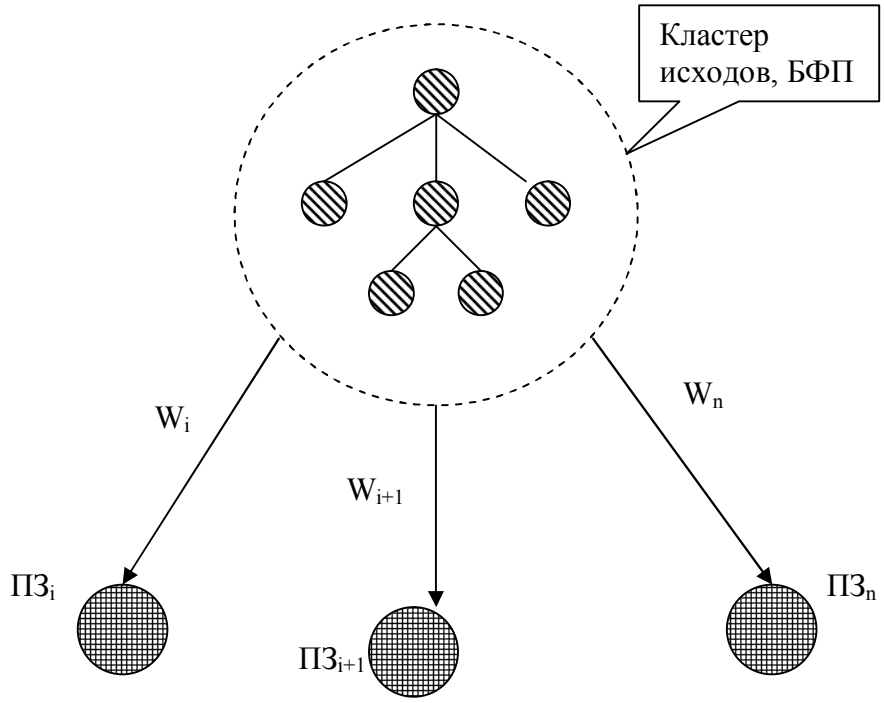

Рис. 2 Модель структуры семейства профилей защиты

Кластер исходов представляет собой вершину графа. В нашем случае вершиной графа является БФП ПЗ, состоящий из множества базовых ФТБ:

$$\text{БФП} = \{W_б\} = \{У_б, \text{ЦБ}_б\}, \quad (1)$$

где $\{W_б\}$ – множество, представляющее набор базовых ФТБ;

$\{У_б, \text{ЦБ}_б\}$ – множество базовых угроз для ОО и противопоставляемых им базовых ЦБ.

В зависимости от среды безопасности ОО на БФП накладывается ряд дополнительных ФТБ, исходя из которых и строится ПЗ для определенного класса защищенности ОО:

$$\{W_d\} = \{У_d, \text{ЦБ}_d\}. \quad (2)$$

Таким образом, суммируя все вышесказанное, получаем, что ПЗ для определенного класса защищенности ОО представляет собой сумму двух множеств: множества базовых ФТБ, представляющих собой БФП семейства ПЗ, и множества дополнительных ФТБ, добавляемых к первому множеству исходя среды безопасности ОО и ценности его информационных активов:

$$\text{ПЗ}_i = \text{БФП} + \{W_d\} = \{W_б\} + \{W_d\} = \{У_б, ЦБ_б\} \cup \{У_d, ЦБ_d\}. \quad (3)$$

Для построения графо-аналитической модели структуры ПЗ введем следующее его определение: совокупность агентов защиты, расположенных в узлах коммутации, и соединений защиты, организационно реализованных в отдельных выделенных виртуальных каналах.

Обозначим ПЗ как следующее множество – совокупность четырех сервисных служб защиты – аутентификации, конфиденциальности, достоверности и контроля доступа, которые и реализуются агентами защиты:

$$\text{ПЗ} = \{G_А, G_К, G_Д, G_Ц\}, \quad (4)$$

где G_A [S_A (M), X_A] – граф аутентификации,
G_K [S_K (M), X_K] – граф конфиденциальности,
$G_Д$ [$S_Д$ (M), $X_Д$] – граф достоверности,
$G_Ц$ [$S_Ц$ (M), $X_Ц$] – граф контроля доступа,
где S_i (M) – множество вершин (агентов защиты),
X_i; i = А, К, Д, Ц – множество ребер (соединений защиты).

Таким образом, при изменении хотя бы одного из параметров множества меняется соответственно и сам ПЗ, но его основа, в качестве которой выступает БФП, остается неизменной.

Исходя из построенной нами модели семейства ПЗ, его можно определить с помощью равенств (3) и (4). Приравняв их, получаем следующее:

$$\{У_б, ЦБ_б\} \cup \{У_д, ЦБ_д\} = \{G_A, G_K, G_Д, G_Ц\}. \quad (5)$$

После анализа полученного равенства становится очевидным, что объединенное множество базовых и дополнительных ФТБ, по сути, представляет нам множество агентов защиты четырех сервисных служб. Очевидным является тот факт, что множество агентов защиты в свою очередь представляет собой объединенное множество базовых и дополнительных агентов защиты, которые реализуются при построении ОО в зависимости от класса его защищенности:

$$ПЗ = \{G_{Аб}, G_{Кб}, G_{Дб}, G_{Цб}\} + \{G_{Ад}, G_{Кд}, G_{Дд}, G_{Цд}\}. \quad (6)$$

Проинтегрируем равенство (6):

$$ПЗ = \sum_x \int_{i=1}^{n} G_{x_{б_i}} dM + \sum_x \int_{j=1}^{m} G_{x_{д_j}} dM, \quad (7)$$

где $x = \{А, К, Д, Ц\}$, т.е. совокупность четырех сервисных служб защиты;
n, m - количество ФТБ, которые противопоставляются основным и дополнительным механизмам защиты соответственно.

Так как значения множеств $i = \{1, n\}$ и $j = \{1, m\}$ не пересекаются по определению, то в своей сумме они составляют общее количество ФТБ, которые можно включить в ПЗ:

$$\{i + j\} \subseteq \{W\}. \quad (8)$$

Из этого следует, что ПЗ представляет собой множество ФТБ по каждому аспекту защиты информации в БС:

$$ПЗ = \sum_x \int_{z=1}^{n+m} G_{x_z} dM. \quad (9)$$

Таким образом, исходя из полученных равенств (6) и (9), для построения семейства ПЗ первоначально необходимо определить множество базовых агентов защиты беспроводной сети, другими словами определить ее защищенность.

Для того, чтобы оценить защищенность БС, а впоследствии проанализировать полученные результаты, необходимо выработать ряд критериев оценки защищенности, исходя из которых будет представляться возможным произвести оценку сети.

В третьем разделе разрабатывается новая система критериев оценки защищенности беспроводной сети на основе механизмов защиты, описанных в рамках семейства стандартов 802.11.

Проводится исследование семейства стандартов IEEE 802.11 на предмет описанных в нем механизмов защиты информации. В рамках данной работы не затрагиваются средства защиты передаваемых по радиоканалам данных, направленные на предотвращение конкретных видов атак или угроз.

Суммируя знания по существующим ныне стандартам в мире беспроводных технологий, был выделен ряд критериев для проведения анализа, а впоследствии и оценки защищенности БС.

Было получено две основные группы критериев, в соответствии с которыми и происходит оценка сети:

1. Криптографические критерии;
2. Критерии аутентификации.

Каждая группа включает в себя ряд компонентов.

Криптографические критерии:

1. криптографические алгоритмы;
2. длина используемого ключа;
3. использование динамических или статических ключей;
4. технология проверки целостности сообщений (MIC, CCMP).

Критерии аутентификации:

1. протокол;
2. наличие сервера аутентификации;
   a. взаимная аутентификация;
3. использование цифровых сертификатов.

В четвертом разделе осуществляется анализ функциональных требований безопасности второй части ГОСТ Р ИМО/МЭК 15408, происходит их противопоставление разработанным критериям оценки защищенности БС.

Для каждого выделенного критерия ставится в соответствии определенный класс или семейство ФТБ ГОСТ Р ИСО/МЭК 15408.

Первой группе критериев полностью соответствует класс функциональных требований FCS. Данный класс используется для содействия достижению некоторых, наиболее важных целей безопасности, к ним относятся: идентификация и аутентификация, неотказуемость, доверенный маршрут, доверенный канал, разделение данных.

Теперь перейдем ко второй группе критериев, а именно критериям аутентификации.

Семейство FIA_UAU определяет типы механизмов аутентификации пользователя, предоставляемые ФБО. Оно также определяет те атрибуты, на которых необходимо базировать механизмы аутентификации пользователя.

Любые протоколы аутентификации, используемые в БС можно описать с использованием компонент этого семейства, поэтому критерию протокол из группы критериев аутентификации противопоставим сразу же все семейство FIA_UAU.

Семейство FIA_SOS определяет требования к механизмам, которые реализуют определенную метрику качества для предоставляемых секретов и генерируют секреты, удовлетворяющие определенной метрике.

Секреты, рассматриваемые в данном семействе, содержат аутентификационные данные, предъявляемые пользователем механизму аутентификации, основанному на сведениях, которыми располагает пользователь. Данному семейству соответствует критерий 2.2 (использование сервера аутентификации).

Семейство FPT_SSP устанавливает требование использования надежных протоколов некоторыми критичными по безопасности функциями из числа ФБО. Компонент FPT_SSP.2 соответствующего семейства содержит требование, что в дополнение к предоставлению подтверждения получения передаваемых данных принимающей части ФБО необходимо обратиться к передающей за уведомлением о получении подтверждения. Этот механизм с полной уверенностью можно противопоставить критерию 2.2.1(использование взаимной аутентификации).

При использовании в сети цифровых сертификатов для аутентификации пользователей (критерий 2.3) дополнительно рассматривается класс функциональных

требований FDP (Защита данных пользователей), а именно семейство FDP_DAU (Аутентификация данных).

Суммируя все вышесказанное, мы получаем соответствие критериев для оценки защищенности БС ФТБ, описанным в ГОСТ Р ИСО/МЭК 15408. Результаты представлены в таблице 3.

Табл. 3 Соответствие критериев оценки защищенности беспроводной сети ФТБ

Критерии	**ФТБ**
1. *Криптографические критерии*	
1.1 Алгоритм	FCS_COP.1.1
1.2 Длина ключа	FCS_CKM.1.1
1.3 Динам./стат. Ключ	FCS_CKM.2.1
1.4 Проверка целостности	FCS_COP.1.1
2. *Критерии аутентификации*	
2.1 Протокол	FIA_UAU
2.2 Сервер аутентификации	FIA_SOS
2.2.1 Взаимная аутентификация	FPT_SSP.2
2.3 Цифровые сертификаты	FDP_DAU

В третьей главе разрабатывается метод построения семейства профилей защиты для беспроводных сетей с учетом специфики их функционирования. Также разрабатывается система уровней доверия к беспроводной сети, базирующаяся на оценочных уровнях доверия, описанных в ГОСТ Р ИСО/МЭК 15408.

В первом разделе разрабатывается система уровней доверия (УД) к беспроводной сети основанная на системе оценочных уровней доверия третьей части ГОСТ Р ИСО/МЭК 15408.

Для дальнейшего ранжирования критериев безопасности БС по УД характеризуем каждый из них.

- УД1 включает в себя минимально возможный набор компонентов для удовлетворения минимальных требований безопасности сети. Подобные механизмы защиты использовались в основном в начале развития беспроводных технологий, когда пропускная способность сети оставляла желать много лучшего и мощные методики не могли быть реализованы в связи со значительными затратами на аппаратные ресурсы;
- УД2 характеризуется усилением применяемых механизмов на УД1, т.е. в основе лежат все те же малозащищенные протоколы и алгоритмы, на которые накладываются дополнительные «заплатки». Также к этому уровню можно отнести появившиеся средства защиты информации с минимальным набором компонентов;
- УД3 изначально использует новое поколение алгоритмов и механизмов, усиленных за счет возможностей, лежащих в их основе (например, увеличение длины ключа) либо введением дополнительных мер безопасности (использование цифровых сертификатов);
- УД4 представляет максимально возможный в рамках стандарта 802.11 уровень безопасности БС за счет использования механизмов защиты информации с максимально надежным набором компонентов;
- УД5 внедряет дополнительные механизмы защиты информации, которые не описываются в рамках семейства стандартов 802.11 и в своем большинстве представляют защиту от конкретного вида атак или угроз.

Во втором разделе проводится исследование логических связей в структуре механизмов защиты информации в беспроводных сетях.

Для ранжирования механизмов защиты беспроводной сети по выработанным уровням доверия необходимо проанализировать семейство стандартов 802.11 по критериям оценки защищенности, полученным в предыдущей главе. В результате анализа получаем полный структурированный набор механизмов защиты, которые описываются в семействе стандартов IEEE 802.11 для БС (рис. 3).

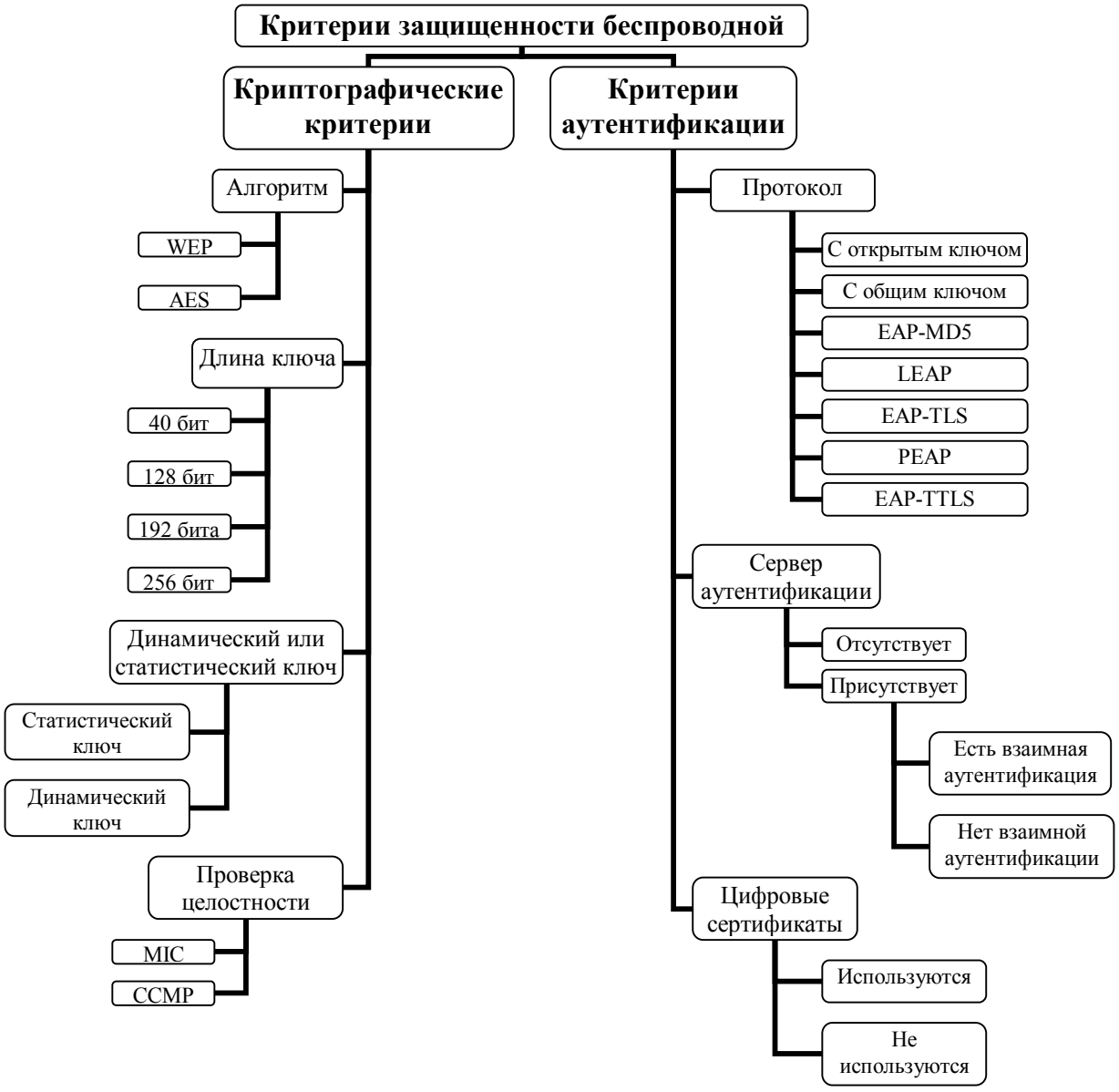

Рис. 3 Классификация механизмов защиты в БС

В третьем разделе осуществляется ранжирование полученных совокупностей механизмов защиты БС по разработанной ранее системе УД к ней (табл. 4).

Табл. 4 Соответствие механизмов защиты беспроводной сети уровням доверия

УД	Критерии	Механизмы защиты
1	Криптографические	WEP-40
		WEP-128 +[1] СК[2] -[3] ПЦ[4]
	Аутентификации	Аутентификация с открытым ключом
		Аутентификация с общим ключом
2	Криптографические	WEP-128 + СК + ПЦ
		WEP-128 + ДК[5] - ПЦ
		WEP-128 + ДК+ ПЦ
		AES-128 + СК - ПЦ
	Аутентификации	EAP-MD5-ВА[6]-ЦС[7]
		LEAP-ВА
		LEAP+ВА
3	Криптографические	AES-128 + СК + ПЦ
		AES-128 + ДК - ПЦ
		AES-128 + ДК + ПЦ
		AES-192 + СК - ПЦ
	Аутентификации	EAP-TLS-ВА+ЦС
		EAP-TLS+ВА+ЦС
		PEAP-ВА-ЦС
		PEAP-ВА+ЦС
		PEAP+ВА-ЦС
4	Криптографические	AES-192 + СК + ПЦ
		AES-192 + ДК - ПЦ
		AES-192 + ДК + ПЦ
		AES-256 + СК - ПЦ
		AES-256 + СК + ПЦ
		AES-256 + ДК - ПЦ
		AES-256 + ДК + ПЦ
	Аутентификации	PEAP+ВА+ЦС
		EAP-TTLS-ВА-ЦС
		EAP-TTLS-ВА+ЦС
		EAP-TTLS+ВА-ЦС
		EAP-TTLS+ВА+ЦС

1) - использование механизма защиты;
2) - статистический ключ;
3) - отсутствие механизма защиты;
4) - проверка целостности;
5) - динамический ключ;
6) - взаимная аутентификация;
7) – цифровые сертификаты.

В четвертом разделе происходит построение семейства базовых функциональных пакетов для беспроводной сети.

Используя полученные данные о соответствии критериев оценки защищенности ФТБ, противопоставим каждому механизму защиты информации в БС соответствующий ему компонент ФТБ.

Исходя из полученных данных, найдем общие ФТБ для каждого уровня доверия и составим для них БФП ПЗ (табл.5):

Табл. 5 Семейство БФП для БС

Уровень доверия	**Функциональные требования безопасности**
УД 1	FCS_COP.1.1
	FCS_CKM.1.1
	FIA_UAU.2
	FIA_UAU.5.1
УД 2	FCS_COP.1.1
	FCS_CKM.1.1
	FCS_CKM.2.1
	FIA_UAU.2
	FIA_UAU.3.1
	FIA_UAU.5.1
	FIA_SOS.2.2
УД 3	FCS_COP.1.1
	FCS_CKM.1.1
	FCS_CKM.2.1
	FIA_UAU.2
	FIA_UAU.3.1
	FIA_UAU.5.1
	FIA_UAU.5.2
	FIA_UAU.7.1
	FIA_SOS.2.2
УД 4	FCS_COP.1.1
	FCS_CKM.1.1
	FCS_CKM.2.1
	FIA_UAU.2
	FIA_UAU.3.1
	FIA_UAU.5.1
	FIA_UAU.5.2
	FIA_UAU.7.1
	FIA_SOS.2.2
	FDP_DAU.2.1
	FDP_DAU.2.2
	FPT_SSP.2

В четвертой главе описывается методика построения ПЗ для БС, рассматриваются аспекты экономической целесообразности реализации системы защиты. Также на базе построенной ранее модели и предложенного на ее основе метода разрабатывается методика проведения аудита защищенности БС по требованиям безопасности ГОСТ Р ИСО/МЭК 15408, приводятся рекомендации по практическому применению методики.

В первом разделе описывается методика построения ПЗ для БС на основе построенного семейства ПЗ для нее. Всю процедуру формирования ПЗ можно разделить на несколько этапов:

- анализ ОО на соответствие его системы защиты стандартам 802.11 с использованием критериев оценки защищенности;
- нахождение уровня доверия к ОО;
- формирование ПЗ с использованием БФП для соответствующего уровня.

Рассмотрим каждым этап более подробно.

Процесс анализа БС можно изначально разбить на два подпроцесса:

- анализ в соответствии с криптографическими критериями;
- анализ в соответствии с критериями аутентификации.

Такое разделение узко специализирует каждый подпроцесс, что оказывает положительное влияние на точность и корректность конечных результатов. Также выявление механизмов защиты по каждому аспекту системы защиты значительно снижает фактор человеческой ошибки с точки зрения взаимной консолидации их между собой.

Результатом данного анализа является совокупность базовых механизмов защиты информации в беспроводных сетях, структурированная строго в соответствии с критериями оценки.

На следующем этапе проводится исследование полученной совокупности реализованных в БС механизмов защиты. Итогом данного процесса является совокупность двух чисел, определяющих уровень доверия к сети с точки зрения криптографических алгоритмов либо алгоритмов аутентификации.

УД к БС должен быть определен как наименьшее число из полученной совокупности. Обозначим его как промежуточный уровень доверия - $УД_{пр}$.

$$УД_{пр} = \min\{УД_{кр}, УД_{ау}\}, \quad (10)$$

где $УД_{пр}$ - промежуточный УД;

$УД_{кр}$ - УД с точки зрения реализованных криптографических функций:

$УД_{ау}$ - УД с точки зрения реализованных функций аутентификации.

Но построение системы защиты беспроводной сети строго согласно семейству стандартов 802.11 является неким идеальным процессом, который не имеет место быть в условиях современного информационного пространства. Зачастую механизмов защиты, определенных в стандартах 802.11 оказывается недостаточно для обеспечения требуемого уровня безопасности при передаче данных по радиоканалам. Для получения достоверных данных об истинном УД к сети необходимо также рассмотреть и совокупность дополнительных механизмов защиты.

Процесс включения в ПЗ требований безопасности по дополнительным механизмам защиты, отраженных в ФТБ ГОСТ Р ИСО/МЭК 15408, является очень трудоемким, поскольку включает в себя исследование по каждой реализованной контрмере в отдельности.

Результатом данного сравнительного анализа является дополнительная совокупность ФТБ $D_{ФТБ}$. Ее необходимо исследовать на наличие таких ФТБ, которые входят в БФП для УД, следующего за промежуточным.

$$D_{ФТБ} \cap (БФП_{пр+1} \setminus БФП_{пр}) = \begin{cases} \varnothing \\ Z \end{cases}, \quad (11)$$

где $БФП_{пр+1}$ - БФП для $УД_{пр+1}$;

$БФП_{пр}$ - БФП для $УД_{пр}$;

$Z \subset БФП_{пр+1} \setminus БФП_{пр}$.

Причем если

$$БФП_{пр} \cup Z = БФП_{пр+1}, \quad (12)$$

то в таком случае конечный УД к БС будет равен $УД_{пр+1}$.

Если же

$$БФП_{пр} \cup Z \subset БФП_{пр+1}, \quad (13)$$

то конечный УД к БС будет равен $УД_{пр}$.

Стоит отдельно оговорить ситуацию, когда $УД_{пр}=УД4$ и вместе с этим в ОО реализованы дополнительные механизмы защиты информации.

Следуя определению УД5, приведенному в третье главе, к данному УД могут быть отнесены такие ОО, в которых в дополнение к основным механизмам защиты, относящимся к УД4, добавляются также дополнительные. Данное утверждение логически обосновано, но не так уж незыблемо, так как Z представляет собой разницу двух множеств, одно из которых неизвестно. Совокупность дополнительных механизмов защиты может состоять только из таких элементов, которые в разрезе ФТБ будут соответствовать только нижестоящим по сравнению с $УД_{пр}$ уровням доверия либо самому $УД_{пр}$. По сути, принятие верных оценок по требованиям безопасности отдается на откуп эксперту или группе экспертов, которые в итоге определяют можно ли отнести подобный ОО к УД5 либо все-таки присвоить ему УД4.

Таким образом, итогом второго этапа формирования ПЗ для БС является УД к ней, полученный в результате исследования основных и дополнительных механизмов защиты и сопоставления их с ФТБ второй части ГОСТ Р ИСО/МЭК 15408, и БФП ПЗ, соответствующий этому УД.

На третьем и заключительном этапе происходит непосредственное построение ПЗ для исследуемого ОО. За основу берется БФП для УД к БС, который был получен в результате исследований ОО на предыдущем этапе.

Если уровень доверия был определен как УД5, то за основу берется БФП, соответствующий УД4, к которому добавляются такие ФТБ, которые были противопоставлены каждому дополнительному механизму защиты, усиливающему, по мнению экспертов либо группы экспертов, всю систему защиты БС.

Дальнейший процесс формирования ПЗ для БС является стандартным и соответствует процессу формирования ПЗ для любой проводной сети. Но особое внимание стоит уделить таким разделам ПЗ, как описание объекта оценки и его среды безопасности.

В качестве специфических особенностей функционирования ОО можно обозначить следующие:

- отсутствие капитальных инженерных сооружений;
- отсутствие постоянной контролируемой территории;
- сложность установки систем наблюдения и сигнализации;
- сложность организации защиты от несанкционированного физического доступа к средствам обработки информации и средствам обеспечения их работоспособности;
- использование для передачи информации открытых каналов связи.

При описании среды безопасности ОО необходимо акцентировать внимание на предположениях безопасности, связанных с физической защитой БС, и предполагаемых угрозах по отношению к БС в силу ее широковещательной природы.

Во втором разделе рассматриваются экономическая целесообразность внедрения той или иной системы защиты информации в БС в зависимости от ценности информации, передаваемой в ней.

Для оценки целесообразности вложения средств в защиту информации введём следующие обозначения:

Цз - ценность информации для защищающейся (обладающей информацией и пытающейся сберечь её) стороны и,

Ца - ценность информации для атакующей (пытающейся добыть информацию) стороны;

$С_з$, Са - средства, выделяемые на защиту или добывание информации;

$р_з$, ра - вероятность успеха защищающейся и атакующей сторон.

Очевидно, что бессмысленно вкладывать в защиту или добывание информации больше средств, чем составляет ценность этой информации:

$$C_З \leq Цз, \quad (14)$$

$$Ca \leq Ца. \quad (15)$$

Предположим, вероятности определяются формулами:

$$p_з = \frac{q_з \cdot C_з}{q_з \cdot C_з + q_a \cdot C_a} \quad (16)$$

$$p_a = \frac{q_a \cdot C_a}{q_з \cdot C_з + q_a \cdot C_a}, \quad (17)$$

где $q_з$, q_a - своего рода весовые коэффициенты, определяющие, насколько какая-то из сторон ближе к цели.

Если предположить, что сумма средств, выделенных атакующей стороной равна ценности информации, а информация имеет одинаковую ценность для обеих сторон, а также, что противоборствующие стороны находятся в равных условиях, то сумма затрат на защиту информации не должна превышать

$$C_з = Ц_з \cdot \frac{\sqrt{5}-1}{2}. \quad (18)$$

Эффективность предлагаемой модели оценки затрат, требуемых для обеспечения защиты информации, зависит от того, насколько точно получится сформулировать вероятность успеха и определить ценность защищаемой информации.

В третьем разделе описывается методика проведения аудита защищенности беспроводной сети, основывающаяся методе определения УД к БС.

В настоящее время все более востребованной на рынке информационной безопасности становится услуга аудита. Однако, как показывает практика, и заказчики, и поставщики этой услуги зачастую суть аудита понимают по-разному.

По своей сути, аудит сети сводится к проверке системы информационной безопасности и сравнению результатов данной проверки с неким идеалом.

Причины проведения аудита на соответствие стандарту (и сертификации) можно условно разделить по степени обязательности данной услуги по отношению к компании:

- обязательная сертификация;
- сертификация, вызванная «внешними» объективными причинами;
- сертификация, позволяющая получить выгоды в долгосрочной перспективе;
- добровольная сертификация.

При разработке методики аудита защищенности беспроводной сети во главу угла ставится непосредственно аудит на соответствие стандартам, а именно ГОСТ Р ИСО/МЭК 15408.

Во многом методика аудита защищенности БС схожа с методикой построения ПЗ для БС на основе смоделированного семейства ПЗ для БС. Всю процедуру проведения аудита защищенности также можно подразделить на несколько этапов::

- анализ беспроводной сети в соответствие с системой критериев оценки защищенности с целью выявления механизмов защиты, реализованных в соответствие с семейством стандартов IEEE 802.11;
- анализ беспроводной сети с целью выявления дополнительных механизмов защиты информации;
- исследование основных механизмов защиты с целью определения УД к БС на основе разработанной системы уровней доверия отдельно по криптографическим функциям и функциям аутентификации;
- определение промежуточного УД к ОО;

- сопоставление дополнительных механизмов защиты, реализованных в сети, с функциональным требованиям безопасности второй части ГОСТ Р ИСО/МЭК 15408;
- определение истинного УД к БС с учетом реализованных дополнительных механизмов защиты в ней;
- вычисление экономической целесообразности реализованной системы защиты информации в ОО;
- анализ полученных результатов с целью оценки защищенности БС и при необходимости разработки решений для изменения системы защиты БС в соответствии с требованиями заказчика.

На всех этапах аудита защищенности БС главную роль играют мнения эксперта или группы экспертов, и правильность результатов напрямую зависит от их профессионализма.

В заключении обозначена практическая ценность разработанных в диссертационной работе модели и метода построения семейства профилей защиты для беспроводной сети. Определены основные направления дальнейших исследований в данной области защиты информации.

Список работ, опубликованных по теме диссертации:

1. Иващук И.Ю. Критерии оценки безопасности беспроводных сетей // Теория и технология программирования и защиты информации: сб. трудов XI междунар. научно-практ. конф. (Санкт-Петербург, 18 мая 2007 г.). - Санкт-Петербург, 2007. – С. 76-80.
2. Иващук И.Ю. Аудит безопасности беспроводных сетей // День антивирусной безопасности: сб. трудов научно-практ. конф. (Санкт-Петербург, 22 окт. 2007 г.). - Санкт-Петербург, 2007. – С. 25-27.
3. **Иващук И.Ю. Предотвращение wormhole атак в беспроводных сетях с помощью пакетных меток // Научно-технический вестник СПбГУ ИТМО. – 2008. - № 52. – С. 188-194.**
4. Иващук И.Ю. Замирание сигнала в широкополосных беспроводных сетях // Теория и технология программирования и защиты информации: сб. трудов XII междунар. научно-практ. конф. (Санкт-Петербург, 15-16 мая 2008 г.). - Санкт-Петербург, 2008. – С. 81-84.
5. **Иващук И.Ю. Модель создания профиля защиты для беспроводной сети // Информационные технологии: сб. трудов VI всерос. межвуз. конф. молодых ученых (Санкт-Петербург, 14-17 апр. 2009 г.). – Санкт-Петербург, 2009. - №6. – С. 16-19.**
6. Иващук И.Ю. Система уровней доверия к беспроводной сети на основе реализованных в ней механизмов защиты // Теория и технология программирования и защиты информации: сб. трудов XIV междунар. научно-практ. конф. (Санкт-Петербург, 20 мая 2009 г.). – Санкт-Петербург, 2009. – С. 31-33.
7. Иващук И.Ю. Подход к созданию базового функционального пакета семейства профилей защиты для беспроводной сети // Информационная безопасность регионов России: тезисы докл. VI межрег. конф. (Санкт-Петербург, 28-30 окт. 2009 г.). - Санкт-Петербург, 2009. – С.107.
8. **Иващук И.Ю. Метод формирования семейства профилей защиты для беспроводной сети // Актуальные инновационные исследования: наука и практика: электр. науч. изд. – 2010. - №1. - URL: http://actualresearch.ru/nn/2010_1/Article/science/ivashchuk.htm (дата обращения 04.04.2010).**

Тиражирование и брошюровка выполнены в
Центре «Университетские Телекоммуникации».
Санкт-Петербург, Кронверский пр., 49. Тел. (812) 233-46-69.
Лицензия ПДЛ №69-182 от 26.11.96 Тираж 100 экз.