**Санкт-Петербургский государственный университет информационных технологий, механики и оптики**

*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**

Диссертация на соискание ученой степени
кандидата технических наук

Научный руководитель – кандидат технических наук,
доцент Птицын А.В.

Санкт-Петербург

2010

# ОГЛАВЛЕНИЕ

# ВВЕДЕНИЕ

**Актуальность темы**

Беспроводные технологии с каждый годом становятся все более незаменимыми 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.

В наше время доступ к корпоративной сети требуется практически каждому служащему, однако прокладка медного кабеля повсюду, где это необходимо, - вещь, разумеется, мало осуществимая на практике. Сеть WLAN (Wireless Local Area Network – беспроводная локальная сеть) - вид локальной вычислительной сети (LAN), использующий для связи и передачи данных между узлами высокочастотные радиоволны, а не кабельные соединения. Это гибкая система передачи данных, которая применяется как расширение - или альтернатива - кабельной локальной сети внутри одного здания или в пределах определенной территории.

Сеть WLAN обеспечивает не привязанную к отдельным помещениям сеть и доступ в Интернет, она дает пользователям возможность перемещаться по территории предприятия или организации, оставаясь подключенными к сети.

Также она обеспечивает простое и быстрое построение локальной сети. Беспроводную сеть можно построить там, где нельзя протянуть кабели, за счет этого происходит снижение стоимости самой сети. Технология WLAN облегчает временную установку сети и ее перемещение. В результате достигается экономия, тем более значительная, чем чаще меняется окружение. Расширение и реконфигурация сети для WLAN не является сложной задачей: пользовательские устройства можно интегрировать в сеть, установив на них беспроводные сетевые адаптеры. Различные марки совместимых клиентских и сетевых устройств будут взаимодействовать

между собой.

Беспроводные локально-вычислительные сети существуют уже не один год, но до последнего времени для них не было разработано общепризнанных стандартов; кроме того, высокая стоимость оборудования, используемые лицензионные частоты и невысокая скорость передачи данных являлись ограничивающими факторами, препятствующими широкому распространению такого типа сетей, поэтому их использовали, прежде всего, для решения узкоспециальных задач.

Популярные беспроводные технологии узаконил принятый в 1997 г. американский стандарт IEEE 802.11 “Wireless LAN Medium Access Control and Physical Layer specifications” и аналогичный международный стандарт ISO 802.11 1998 г. Принятие стандартов 802.11b, а впоследствии, 802.11a и 802.11g, которые увеличивают теоретическую скорость передачи данных до 54 Мбит/сек, в корне изменило эту ситуацию. Основным фактором, способствующим продвижению беспроводных сетей этого стандарта, явилась используемая нелицензионная частота и дешевизна оборудования. На сегодняшний день основная масса устройств для беспроводных сетей выпускается в соответствии с данным стандартом. В то же время появляются все новые модели, превосходящие по характеристикам стандартное оборудование.

Ныне беспроводные технологии позволяют успешно решить проблему расширения зоны действия традиционной проводной сети. И надо сказать, что во многих случаях каналы беспроводной связи могут стать единственной возможностью подключения к локально-вычислительной сети и выхода в Интернет. Беспроводные локальные сети, построенные в соответствии со стандартом IEEE 802.11, вот уже несколько лет используются как в корпоративной, так и в приватной областях. Растущая популярность свидетельствует, что с их помощью удалось решить целый ряд проблем: например, в локальных сетях наконец-то стали возможны «мобильные вычисления» с приемлемой скоростью передачи данных, пусть все еще на

порядок меньшей по сравнению с проводными сетями, но уже достаточно высокой для удовлетворения львиной доли мобильных потребностей. Организация связи между зданиями нуждается в не лицензируемой технологии, применение которой делает ненужным аренду выделенных линий. А в общественных местах WLAN выступает в качестве недорогой альтернативы для предоставления услуг доступа в Интернет с высокой пропускной способностью.

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 (БС). 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.

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

**Целью работы** является разработка модели семейства профилей защиты для беспроводной сети, которая позволит значительно упростить и ускорить процесс сертификации данного вида сетей в соответствии с ГОСТ Р ИСО/МЭК 15408, что, в свою очередь, приведет к увеличению доверия к самой сети со стороны как внешних, так и внутренних пользователей.

Разработка метода построения профиля защиты для данного вида сетей на основе реализованных в ней механизмов защиты информации также является актуальной задачей, так как позволяет оценить защищенность сети, как на этапе ее построения, так и в ходе проведения аудита безопасности сети.

**Объектом исследования** в данной работе 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.

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

**Научная новизна** 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.

**Структура работы** выглядит следующим образом:

- **в первой части работы** проведен обзор семейства стандартов IEEE 802.11 и описанных в нем механизмов защиты информации, также обозначены основные виды угроз для беспроводных сетей;

- **во второй части работы** 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 третьей части работы** на базе созданной модели, 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 четвертой части работы** описывается методика построения профиля защиты для беспроводной сети, рассматриваются аспекты экономической целесообразности реализации системы защиты. Также на базе построенной ранее модели и предложенного на ее основе метода разрабатывается методика проведения аудита защищенности беспроводной сети по требованиям безопасности ГОСТ Р ИСО/МЭК 15408, приводятся рекомендации по практическому применению методики.

# ГЛАВА 1. ОБЗОР СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ БЕСПРОВОДНОЙ СЕТИ, ВКЛЮЧЕННЫХ В СЕМЕЙСТВО СТАНДАРТОВ 802.11

## 1.1 Развитие беспроводных технологий стандарта IEEE 802.11

Первые образцы беспроводного оборудования были созданы для диапазона 902—928 МГц. Типовой пример подобного оборудования — серия Aironet 1000 со скоростью передачи в канале от 215 до 860 кбит/с по технологии расширения спектра прямой последовательностью. На максимальной скорости ширина спектра сигнала составляет около 19 МГц, и в полосе частот 26 МГц удается разместить только один частотный канал. При минимальной скорости 215 кбит/с ширина спектра сигнала около 5 МГц, что позволяет разместить в полосе частот, выделенной для передачи, пять не перекрывающихся частотных каналов (реально 12 перекрывающихся).

Скорости передачи в этом диапазоне, казалось бы, достаточны, чтобы удовлетворить многих пользователей. Однако следует иметь в виду, что речь идет о “технической” скорости передачи битов в физическом канале. Кроме информационной, сообщение должно также содержать и служебную часть. К тому же необходимо время для установления связи и синхронизации. Реальная скорость передачи информации, как правило, не превышает 70% технической. Следует также учитывать, что при использовании беспроводных технологий общая среда передачи в каждый момент времени выделяется в монопольное использование только одному абоненту, т. е. пропускная способность сети для каждого абонента будет меньше 70% “технической” скорости в n раз (где n — количество абонентов). Так, при 10 одновременно работающих абонентах на каждого придется не более 60 кбит/с реальной пропускной способности. Это обстоятельство, а также использование диапазона другими радиосредствами (в частности, сетями сотовой связи GSM-900), создающими помехи для БС, привело к тому, что

беспроводные сети диапазона 902—928 МГц не получили широкого распространения.

Более удобным оказался диапазон 2400—2483,5 МГц — и по большей пропускной способности, и в смысле меньшего уровня помех от других радиосредств. Следует, правда, оговорить два обстоятельства. Во-первых, в ряде стран разрешено лишь частичное использование этого диапазона. Второе обстоятельство связано с величиной, эквивалентной изотропно излучаемой мощности (ЭИИМ) сигнала. В Европе Институт стандартизации в области телекоммуникаций ограничил значение ЭИИМ 100 мВт (20 дБм). Оборудование выпускается исходя из этих ограничений. Если же значение ЭИИМ превышает допустимое значение — необходимо специальное разрешение на выпуск подобных устройств. Ситуация не отличается от имеющей место в России, где действует обобщенное решение Государственной комиссии по радиочастотам о разрешении использования диапазона на вторичной основе, но требуется регистрация оборудования в Госсвязьнадзоре [47]. Принятие в России европейских ограничений существенно упростило бы жизнь операторам беспроводных сетей без какого-либо ущерба другим системам этого диапазона.

Вплоть до 1997 г. каждый изготовитель выпускал оборудование этого диапазона, не сдерживаемый практически никакими ограничениями, кроме частотно-энергетических. Беспроводным системам, однако, все еще недоставало важнейшего элемента - стандартов. Стандарты стабилизируют продукцию, сокращают расходы на исследования и разработки, что в конечном итоге приводит к снижению цены [32]. Совместная работа изделий различных производителей тоже невозможна без стандартов, обеспечивающих совместимость продукции независимых компаний и организаций.

Комитет по стандартам IEEE 802 сформировал рабочую группу по стандартам для беспроводных локальных сетей 802.11 в 1990 году. Эта группа занялась разработкой всеобщего стандарта для радиооборудования и

сетей, работающих на частоте 2,4 ГГц, со скоростями доступа 1 и 2 Мбит/с. Работы по созданию стандарта были завершены через 6 лет, последний черновой вариант стандарта был представлен в ноябре 1995 г. Представление в Международную организацию по стандартизации (International Organization for Standardization, ISO) произошло в марте 1996 г. Первые комплексные испытания прошли в марте 1996 г., окончательные комплексные испытания - в июле 1996 г., а в июне 1997 года была ратифицирована первая спецификация стандарта 802.11 [57].

Стандарт IEEE 802.11 являлся первым стандартом для продуктов WLAN от независимой международной организации, разрабатывающей большинство стандартов для проводных сетей. Как и у других стандартов серии 802, главной функцией стандарта 802.11 является обеспечение работы устройств обслуживания передачи данных для доступа к среде передачи на уровне протокола управления логическим каналом. Иными словами, стандартизованное оборудование осуществляет передачу пакетов данных между сетевыми платами без проводов. Однако к тому времени, заложенная первоначально скорость передачи данных в беспроводной сети, уже не удовлетворяла потребностям пользователей. Для того чтобы сделать технологию Wireless LAN популярной, дешёвой, а главное, удовлетворяющей современным жёстким требованиям бизнес-приложений, разработчики были вынуждены создать новый стандарт.

В сентябре 1999 года IEEE ратифицировал расширение предыдущего стандарта. Названное IEEE 802.11b (также известное, как 802.11 High rate), оно определяет стандарт для продуктов БС, которые работают на скорости 11 Мбит/с, что позволяет успешно применять эти устройства в крупных организациях.

Позже появились еще различные типы беспроводных сетей, которые отличаются друг от друга радиусом действия, поддерживаемыми скоростями соединения и технологией кодирования данных. Так стандарт IEEE 802.11b+

предусматривает максимальную скорость соединения 22 Мбит/с, стандарты IEEE 802.11g и 802.11a - 54 Мбит/с.

Будущее стандарта 802.11a довольно туманно. Наверняка, в России и в Европе этот стандарт не получит широкого распространения, да и в США, где он сейчас используется, скорее всего, в ближайшее время произойдет переход на альтернативные стандарты. Преимущество стандарта 802.11g заключается в том, что он полностью совместим со стандартами 802.11b и 802.11b+, то есть любое устройство, поддерживающее стандарт 802.11g, будет работать (правда, на меньших скоростях соединения) и в сетях стандарта 802.11b/b+, а устройство, поддерживающее стандарт 802.11b/b+ — в сетях стандарта 802.11g, хотя и с меньшей скоростью соединения.

Совместимость стандартов 802.11g и 802.11b/b+ обусловлена, во-первых, тем, что они предполагают использование одного и того же частотного диапазона, а во-вторых, что все режимы, предусмотренные в протоколах 802.11b/b+, реализованы и в стандарте 802.11g. Поэтому стандарт 802.11b/b+ можно рассматривать как подмножество стандарта 802.11g.

Принятие 24 июня 2004 г. стандарта обеспечения безопасности в беспроводных сетях 802.11i - событие настолько знаменательное, что значение его трудно переоценить. Данный стандарт, который не могли ратифицировать более четырех лет, вышел как поправка № 6 к IEEE 802.11 редакции 1999 г. и имеет полное название «IEEE 802.11i Medium Access Control Security Enhancements», т. е. расширения по безопасности для MAC-уровня. В описании сказано, что в данной поправке определены механизмы безопасности для стандарта IEEE 802.11, включающие WEP (Wired Equivalent Privacy) для обеспечения обратной совместимости с оригинальным стандартом редакции 1999 г. Эта поправка определяет протоколы TKIP (Temporal Key Integrity Protocol)) и CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), которые предлагают более надежные механизмы защиты данных в дополнение к WEP

[36]. Кроме того, указано, как IEEE 802.1x может быть использован протоколом IEEE 802.11 для эффективной аутентификации [37].

Совместимость продуктов различных производителей гарантируется независимой организацией, которая называется Wireless Ethernet Compatibility Alliance (WECA). Эта организация была создана лидерами индустрии беспроводной связи в 1999 году. В настоящее время членами WECA являются более 80 компаний, в том числе такие известные производители, как Cisco, 3Com, IBM, Intel, Apple, Compaq, Dell, Fujitsu, Siemens, Sony, AMD и прочие [51].

Обзор беспроводных протоколов целесообразно начат именно с протокола 802.11, который, хотя уже и не встречается в чистом виде, в то же время является прародителем всех остальных протоколов. Как и все стандарты IEEE 802, 802.11 работает на нижних двух уровнях модели взаимодействия открытых систем (ISO/OSI), физическом уровне и канальном уровне (рис. 1.1). Любое сетевое приложение, сетевая операционная система, или протокол (например, TCP/IP), будут так же хорошо работать в сети 802.11, как и в любой другой проводной сети.

Основная архитектура, особенности и службы 802.11b определяются в первоначальном стандарте 802.11. Спецификация 802.11b затрагивает только физический уровень, добавляя лишь более высокие скорости доступа.

На физическом уровне определены два широкополосных радиочастотных метода передачи и один – в инфракрасном диапазоне. Радиочастотные методы работают в диапазоне 2,4 ГГц и обычно используют полосу 83 МГц от 2,400 ГГц до 2,483 ГГц. Технологии широкополосного сигнала, используемые в радиочастотных методах, увеличивают надёжность, пропускную способность, позволяют многим несвязанным друг с другом устройствам разделять одну полосу частот с минимальными помехами друг для друга [24].


Рис. 1.1Уровни модели ISO/OSI и их соответствие стандарту 802.11

В стандарте 802.11 предусмотрено два скоростных режима: 1 и 2 Мбит/с. Для кодирования данных на физическом уровне используется метод прямой последовательности DSSS (Direct-Sequence Spread Spectrum) с 11-чиповыми кодами Баркера. При информационной скорости 1 Мбит/с скорость следования отдельных чипов последовательности Баркера составляет 11×106 чип/с, а ширина спектра такого сигнала составляет 22 МГц [18]. Учитывая, что ширина частотного диапазона составляет 83,5 МГц, получаем, что всего в данном частотном диапазоне можно уместить 3 не перекрывающихся частотных канала. Весь частотный диапазон, однако, принято делить на 11 частотных перекрывающихся каналов по 22 МГц, отстоящих друг от друга на 5 МГц. К примеру, первый канал занимает частотный диапазон от 2400 до 2423 МГц и центрирован относительно частоты 2412 МГц. Второй канал центрирован относительно частоты 2417 МГц, а последний, одиннадцатый канал, центрирован относительно частоты 2462 МГц. При таком рассмотрении первый, шестой и последний, одиннадцатый каналы не перекрываются друг с другом и имеют трех

мегагерцовый зазор друг относительно друга. Именно эти три канала могут использоваться независимо друг от друга.

Информационная скорость 1 Мбит/с является обязательной в стандарте IEEE 802.11 (Basic Access Rate), но опционально возможна и скорость в 2 Мбит/с (Enhanced Access Rate). Для передачи данных на такой скорости используется та же технология DSSS с 11-чиповыми кодами Баркера, но для модуляции несущего колебания применяется относительная квадратурная фазовая модуляция DQPS (Differential Quadrature Phase Shiftey).

Протокол IEEE 802.11b, принятый в июле 1999 года, является своего рода расширением базового протокола 802.11 и кроме скоростей 1 и 2 Мбит/с предусматривает скорости 5,5 и 11 Мбит/с.

Стандарт IEEE 802.11g является логическим развитием стандарта 802.11b/b+ и предполагает передачу данных в том же частотном диапазоне, но с более высокими скоростями. Кроме того, стандарт 802.11g полностью совместим с 802.11b, то есть любое устройство 802.11g должно поддерживать работу с устройствами 802.11b. Максимальная скорость передачи в стандарте 802.11g составляет 54 Мбит/с.

При разработке стандарта 802.11g рассматривались несколько конкурирующих технологий: метод ортогонального частотного разделения OFDM (Orthogonal Frequency-Division Multiplexing), предложенный к рассмотрению компанией Intersil, и метод двоичного пакетного сверточного кодирования PBCC (Packet Binary Convolutional Coding), опционально реализованный в стандарте 802.11b и предложенный компанией Texas Instruments [18]. В результате стандарт 802.11g основан на компромиссном решении: в качестве базовых применяются технологии OFDM и CCK (Complementary Code Keying), а опционально предусмотрено использование технологии PBCC [59].

До сих пор мы рассматривали лишь физический уровень протоколов семейства 802.11. На физическом уровне определяются механизмы, которые используются для преобразования данных и для обеспечения требуемой

скорости передачи в зависимости от среды передачи данных. Таким образом, физический уровень определяет методы кодирования/декодирования и модуляции/демодуляции сигнала при его передаче и приеме.

Канальный уровень 802.11 состоит из двух подуровней: управления логической связью (Logical Link Control, LLC) и управления доступом к носителю (MAC). 802.11 использует тот же LLC и 48-битовую адресацию, что и другие сети 802. Это позволяет легко объединять беспроводные и проводные сети, однако MAC уровень имеет кардинальные отличия.

MAC уровень 802.11 очень похож на реализованный в 802.3, где он поддерживает множество пользователей на общем носителе, когда пользователь проверяет носитель перед доступом к нему. Для проводных сетей стандарта 802.3 используется протокол Carrier Sence Multiple Access with Collision Detection (CSMA/CD), который определяет, как станции Ethernet получают доступ к проводной линии, и как они обнаруживают и обрабатывают коллизии, возникающие в том случае, если несколько устройств пытаются одновременно установить связь по сети. Чтобы обнаружить коллизию, станция должна обладать способностью и принимать, и передавать одновременно. Стандарт 802.11 предусматривает использование полудуплексных приёмопередатчиков, поэтому в беспроводных сетях 802.11 станция не может обнаружить коллизию во время передачи.

Чтобы учесть это отличие, 802.11 использует модифицированный протокол, известный как Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), или Distributed Coordination Function (DCF). CSMA/CA пытается избежать коллизий путём использования явного подтверждения пакета (Acknowledge, ACK), что означает, что принимающая станция посылает ACK пакет для подтверждения того, что пакет получен неповреждённым.

CSMA/CA работает следующим образом. Станция, желающая передавать, тестирует канал, и если не обнаружено активности, станция ожидает в течение некоторого случайного промежутка времени, а затем

передаёт пакет, если среда передачи данных всё ещё свободна. Если пакет приходит целым, принимающая станция посылает пакет ACK, по приёму которого отправителем завершается процесс передачи. Если передающая станция не получила пакет ACK, в силу того, что не был получен пакет данных, или пришёл повреждённый ACK, делается предположение, что произошла коллизия, и пакет данных передаётся снова через случайный промежуток времени.

Для определения того, является ли канал свободным, используется алгоритм оценки чистоты канала (Channel Clearance Algorithm, CCA). Его суть заключается в измерении энергии сигнала на антенне и определения мощности принятого сигнала (Received Signal Strength Indication, RSSI). Если мощность принятого сигнала ниже определённого порога, то канал объявляется свободным, и MAC уровень получает статус clear to send (CTS). Если мощность выше порогового значения, передача данных задерживается в соответствии с правилами протокола. Стандарт предоставляет ещё одну возможность определения незанятости канала, которая может использоваться либо отдельно, либо вместе с измерением RSSI – метод проверки несущей. Этот метод является более выборочным, так как с его помощью производится проверка на тот же тип несущей, что и по спецификации 802.11 [4]. Наилучший метод для использования зависит от того, каков уровень помех в рабочей области.

Таким образом, CSMA/CA предоставляет способ разделения доступа по радиоканалу. Механизм явного подтверждения эффективно решает проблемы помех. Однако он добавляет некоторые дополнительные накладные расходы, которых нет в 802.3, поэтому сети 802.11 будут всегда работать медленнее, чем эквивалентные им проводные локальные сети.

802.11 определяет два типа оборудования – клиент, который обычно представляет собой компьютер, укомплектованный беспроводной сетевой интерфейсной картой (Network Interface Card, NIC), и точку доступа (Access point, AP), которая выполняет роль моста между беспроводной и проводной

сетями. AP обычно содержит в себе приёмопередатчик, интерфейс проводной сети (802.3), а также программное обеспечение, занимающееся обработкой данных. В качестве беспроводной станции может выступать ISA, PCI или PC Card сетевая карта в стандарте 802.11, либо встроенные решения, например, телефонная гарнитура 802.11.

Стандарт IEEE 802.11 определяет два режима работы сети – режим "Ad-hoc" и клиент/сервер (или режим инфраструктуры – infrastructure mode).

В режиме клиент/сервер (рис. 1.2) БС состоит из, как минимум, одной точки доступа, подключенной к проводной сети, которая выполняет в беспроводной сети роль своеобразного концентратора (аналогично тому, как это происходит в традиционных кабельных сетях), и некоторого набора беспроводных оконечных станций. Такая конфигурация носит название базового набора служб (Basic Service Set, BSS). В режиме BSS все станции связываются между собой только через AP, которая может выполнять также роль моста к внешней сети. Два или более BSS, образующих единую подсеть, формируют расширенный набор служб (Extended Service Set, ESS). В расширенном режиме ESS существует инфраструктура нескольких сетей BSS, причем сами точки доступа взаимодействуют друг с другом, что позволяет передавать трафик от одной BSS к другой. Между собой AP соединяются с помощью либо сегментов кабельной сети, либо радиомостов.

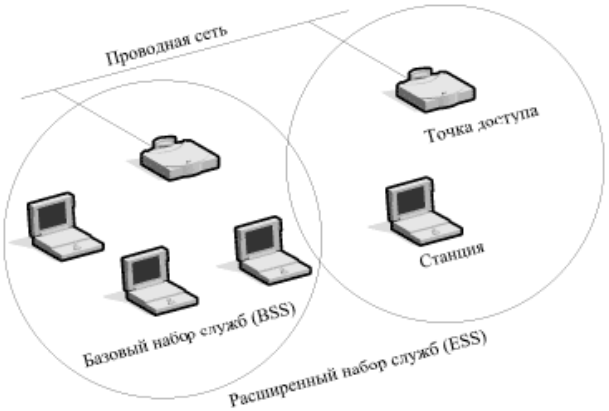


Рис. 1.2. Архитектура БС «клиент/сервер»

Так как большинству беспроводных станций требуется получать доступ к файловым серверам, принтерам, Интернет, доступным в проводной локальной сети, они будут работать в режиме клиент/сервер.

Режим "Ad-hoc" (также называемый точка-точка (Peer to Peer), или независимый базовый набор служб, IBSS) – это простая сеть, в которой связь между многочисленными станциями устанавливается напрямую, без использования специальной точки доступа (рис. 1.3). Такой режим полезен в том случае, если инфраструктура БС не сформирована, либо по каким-то причинам не может быть сформирована. Основными недостатками режима «Ad-hoc» являются ограниченный диапазон действия возможной сети и невозможность подключения к внешней сети (например, к Интернету).


Рис. 1.3. Архитектура БС «Ad-hoc»

Кроме двух различных режимов функционирования беспроводных сетей на MAC уровне определяются правила коллективного доступа к среде передачи данных. Необходимость существования таких регламентирующих правил вполне очевидна. Представим себе ситуацию, когда каждый узел БС, не соблюдая никаких правил, стал бы передавать данные в эфир. В результате интерференции нескольких таких сигналов узлы, которым предназначалась отправленная информация, не смогли бы не только ее получить, но и понять, что данная информация адресована им. Именно поэтому, необходимо существование жестких регламентирующих правил, которые определяли бы коллективный доступ к среде передачи данных.

Такие правила коллективного доступа можно образно сравнить с правилами дорожного движения, которые регламентируют совместное использование автодорог всеми участниками движения [58].

Основное дополнение, внесённое 802.11b в основной стандарт – это поддержка двух новых скоростей передачи данных – 5,5 и 11 Мбит/с. Для достижения этих скоростей был выбран метод DSSS, так как метод частотных скачков в силу ограничений не может поддерживать более высокие скорости. Из этого следует, что системы 802.11b будут совместимы с DSSS системами 802.11 [31].

Для поддержки очень зашумлённых сред, а также работы на больших расстояниях, сети 802.11b используют динамический сдвиг скорости, который позволяет автоматически изменять скорость передачи данных в зависимости от свойств радиоканала. Например, пользователь может подключиться с максимальной скоростью 11 Мбит/с, но в том случае, если повысится уровень помех, или пользователь удалится на большое расстояние, мобильное устройство начнёт передавать на меньшей скорости – 5,5, 2 или 1 Мбит/с [9]. В том случае, если возможна устойчивая работа на более высокой скорости, мобильное устройство автоматически начнёт передавать с более высокой скоростью. Сдвиг скорости – механизм физического уровня, и является прозрачным для вышестоящих уровней и пользователя.

MAC уровень 802.11 несёт ответственность за то, каким образом клиент подключается к AP. Когда клиент 802.11 попадает в зону действия одной или нескольких точек доступа, он на основе мощности сигнала и наблюдаемого значения количества ошибок выбирает одну из них и подключается к ней. Как только клиент получает подтверждение того, что он принят AP, он настраивается на радиоканал, в котором она работает. Время от времени он проверяет все каналы 802.11, чтобы посмотреть, не предоставляет ли другая AP службы более высокого качества. Если такая

точка доступа находится, то станция подключается к ней, перенастраиваясь на её частоту [44] (рис. 1.4).

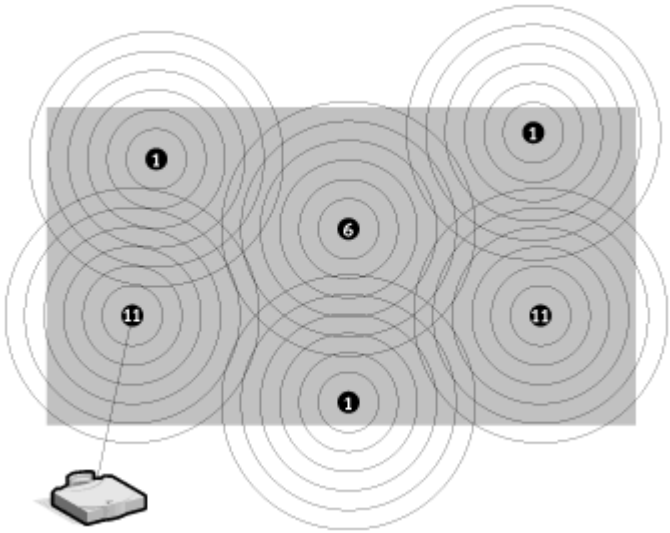


Рис. 1.4 Процесс подключения к БС AP

Переподключение обычно происходит в том случае, если станция была физически перемещена от AP, что привело к ослаблению сигнала. В других случаях повторное подключение происходит из-за изменения радиочастотных характеристик здания, или просто из-за большого сетевого трафика через первоначальную точку доступа. В последнем случае эта функция протокола известна как "балансировка нагрузки", так как её главное назначение – распределение общей нагрузки на БС наиболее эффективно по всей доступной инфраструктуре сети.

Процесс динамического подключения и переподключения позволяет сетевым администраторам устанавливать беспроводные сети с очень широким покрытием, создавая частично перекрывающиеся "соты". Идеальным вариантом является такой, при котором соседние перекрывающиеся AP будут использовать разные DSSS каналы, чтобы не создавать помех в работе друг другу.

## 1.2 Алгоритмы аутентификации

На сегодняшний день для обеспечения безопасности любой сети, как проводной, так и беспроводной, необходимо обеспечить решение трех основных проблем: конфиденциальность (данные должны быть надежно зашифрованы), целостность (данные гарантированно не должны быть изменены третьим лицом) и аутентичность (надежная проверка того, что данные получены от правильного источника).

Беспроводные ЛВС, ввиду их широковещательной природы, требуют реализации дополнительных механизмов для:

- аутентификации абонентов с целью предотвращения несанкционированного доступа к сетевым ресурсам;
- обеспечения конфиденциальности данных с целью обеспечения целостности и защиты при передаче по общедоступному радиоканалу.

Изначально стандарт IEEE 802.11 предусматривает два механизма аутентификации беспроводных абонентов: открытую аутентификацию и аутентификацию с общим ключом [63].

Аутентификация в стандарте IEEE 802.11 ориентирована на аутентификацию абонентского устройства радиодоступа, а не конкретного абонента как пользователя сетевых ресурсов.

Процесс аутентификации абонента БС состоит из следующих этапов (рис. 1.5):

1. Абонент посылает пакет запроса состояния (probe request) во все радиоканалы.
2. Каждая точка доступа, в зоне радиовидимости которой находится абонент, посылает ответный пакет о состоянии (probe response).
3. Абонент выбирает предпочтительную для него АР и посылает в обслуживаемый ею радиоканал запрос на аутентификацию (authentication request).

4. AP посылает подтверждение аутентификации (authentication reply).

5. В случае успешной аутентификации абонент посылает AP пакет с запросом ассоциирования (association request).

6. AP посылает ответный пакет ассоциирования (association response).

7. Абонент может теперь осуществлять обмен пользовательским трафиком с точкой доступа и проводной сетью.

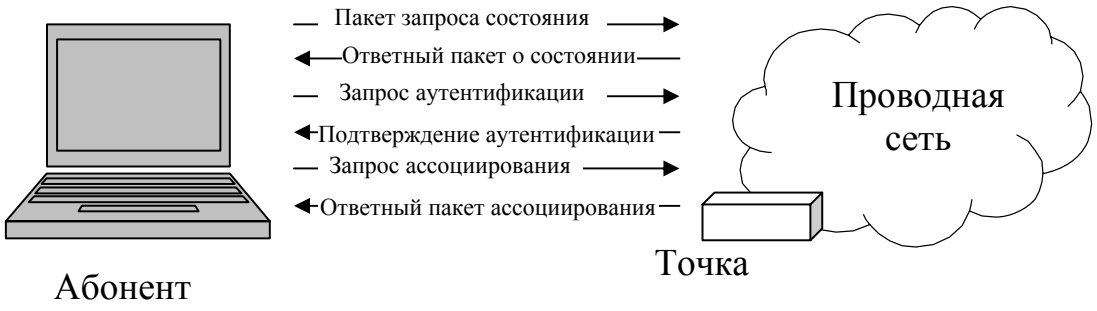


Рис. 1.5 Процесс аутентификации абонента в БС

При активизации в БС абонент начинает поиск точек доступа в своей зоне радиовидимости с помощью управляющих пакетов запроса состояния. Фреймы probe request посылаются в каждый из радиоканалов, поддерживаемых абонентским радиоинтерфейсом, в попытке найти все AP с требуемыми клиенту идентификатором SSID (service set identifier) и поддерживаемыми скоростями радиообмена.

Каждая точка доступа, из находящихся в зоне радиовидимости абонента и удовлетворяющая запрашиваемым в пакете probe request параметрам, отвечает пакетом probe response, содержащем синхронизирующую информацию и данные о текущей загрузке AP. Абонент определяет, с какой точкой доступа он будет работать, путем сопоставления поддерживаемых ими скоростей радиообмена и загрузки. После того, как предпочтительная AP определена, абонент переходит в фазу аутентификации.

Открытая аутентификация по сути не является алгоритмом аутентификации в привычном понимании [51]. Точка доступа удовлетворит

любой запрос открытой аутентификации. На первый взгляд, использование этого алгоритма может показаться бессмысленным, однако следует учитывать, что разработанные в 1997 году методы аутентификации IEEE 802.11 ориентированы на быстрое логическое подключение к беспроводной сети. Вдобавок к этому, многие IEEE 802.11-совместимые устройства представляют собой портативные блоки сбора информации (сканеры штрих-кодов и т.п.), не имеющие достаточной процессорной мощности, требующейся для реализации сложных алгоритмов аутентификации.

В процессе открытой аутентификации происходит обмен сообщениями двух типов:

• запрос аутентификации;

• подтверждение аутентификации.

Таким образом, при открытой аутентификации возможен доступ любого абонента к БС. Если в беспроводной сети не используется шифрование, то любой абонент, знающий идентификатор SSID AP, получит доступ к сети. При использовании точками доступа шифрования WEP сами ключи шифрования становятся средством контроля доступа. Если абонент не располагает корректным WEP-ключом, то даже в случае успешной аутентификации он не сможет ни передавать данные через точку доступа, ни расшифровывать данные, переданные точкой доступа (рис. 1.6).

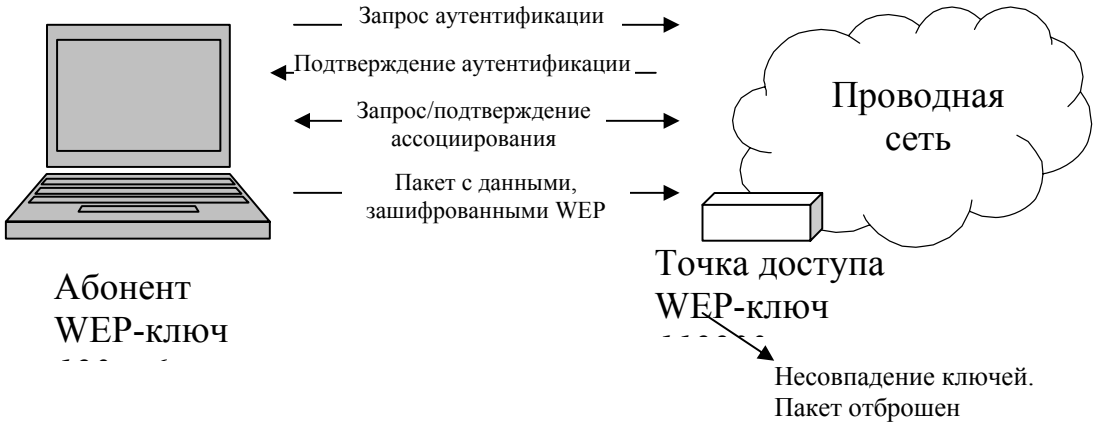


Рис. 1.6 Процесс открытой аутентификации

Аутентификация с общим ключом является вторым методом аутентификации стандарта IEEE 802.11 [6]. Аутентификация с общим ключом требует настройки у абонента статического ключа шифрования WEP. Процесс аутентификации иллюстрирует рис. 1.7:

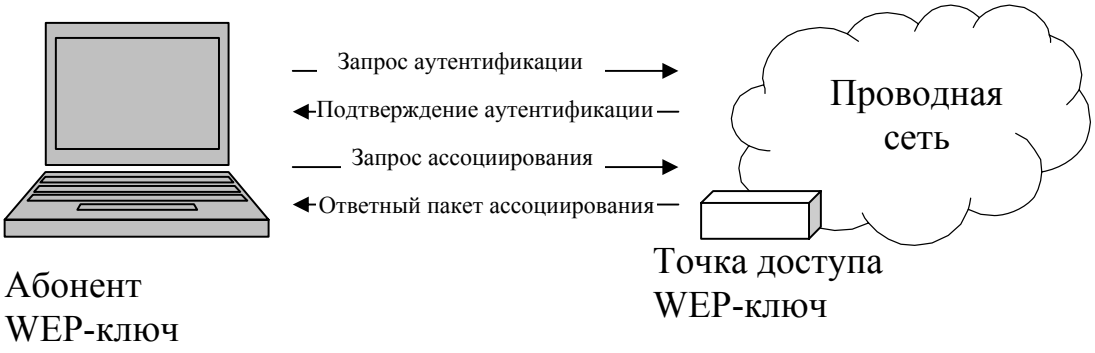


Рис. 1.7 Процесс аутентификации с общим ключом

1. Абонент посылает AP запрос аутентификации, указывая при этом необходимость использования режима аутентификации с общим ключом.
2. Точка доступа посылает подтверждение аутентификации, содержащее так называемый «испытательный текст» (challenge text).
3. Абонент шифрует challenge text своим статическим WEP-ключом, и посылает AP запрос аутентификации.
4. Если AP в состоянии успешно расшифровать запрос аутентификации и содержащийся в нем challenge text, она посылает абоненту подтверждение аутентификации, таким образом, предоставляя доступ к сети [59].

IEEE 802.1x применяется для авторизации, аутентификации и аккаунтинга пользователей, чтобы проверить возможность предоставления доступа к сети. В случае 802.1x используются уже динамические ключи шифрования, что является несомненным плюсом. 802.1x предназначен для работы со сторонними средствами, такими как сервер RADIUS (Remote Access Dial-In User Server) и протокол EAP (Extensive Authentication Protocol).

В структуре решения по обеспечению защиты от несанкционированного доступа (НСД) на базе стандарта 802.1x выделяется три основных компонента: суппликант, коммутирующее устройство с поддержкой 802.1x и сервер аутентификации [16].

Суппликант - программный код на стороне клиента, который обеспечивает взаимодействие аппаратуры клиента с пограничным сетевым устройством в соответствии со спецификациями 802.1x [42]. Именно суппликант обеспечивает передачу атрибутов доступа к ресурсам на коммутатор.

Аутентификатор - пограничное сетевое устройство, которое обеспечивает проверку полномочий абонента на доступ к ресурсам сети [54]. Это устройство (коммутатор) осуществляет запрос на проверку полученных атрибутов доступа в сеть от суппликанта на сервер аутентификации, в качестве которого выступает RADIUS сервер и принимает решение о переводе соответствующего сетевого порта в активное состояние.

Сервер аутентификации - RADIUS сервер, с поддержкой EAP метода аутентификации [41]. Сервер аутентификации имеет доступ к базе данных учетных записей, на основе которой и принимается решение о возможности предоставления доступа для того или иного клиента в зависимости от ряда параметров, ключевым из которых является баланс абонента, рассматривая применение решения на базе 802.1x в структуре сетей коммерческих операторов связи.

Ключевой идеей стандарта 802.1x являет то, что по умолчанию порт пограничного устройства находится в неактивном состоянии и не обеспечивает передачу данных [55].

После успешной аутентификации порт устройства переводится в активное состояние и обеспечивает передачу данных. Таким образом, в зависимости от полномочий абонента, решение на базе 802.1x позволяет управлять непосредственно портами 802.1x совместимого коммутатора на канальном уровне. Порты коммутатора могут динамически менять свое

состояние из активного в пассивное и наоборот. Важно понимать, что однажды аутентифицировавшись корректно, абонент посредством супликанта переводит порт в активное состояние, что создает определенные уязвимости в сетевой безопасности. Будучи переведенным в активное состояние правильной аутентификацией, порт коммутатора обеспечивает передачу данных всего сетевого сегмента, подключенного к нему, даже в том случае, если используется MAC-фильтрация.

Для аутентификации в сети на базе 802.1x используется протокол EAP. Различные производители создали свои реализации протокола EAP для обеспечения безопасности БС [51] (табл. 1.1).

Табл.1.1 Реализация протокола EAP

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

EAP-MD5 подтверждает подлинность пользователя путем проверки пароля. Являясь процедурой односторонней аутентификации супликанта сервером аутентификации, основанной на применении хеш-суммы MD5 имени пользователя и пароля как подтверждения для сервера RADIUS. Вопрос использования шифрования трафика отдан на откуп администратору сети. Данный метод не поддерживает ни управления ключами, ни создания динамических ключей. Слабость EAP-MD5 заключается в отсутствии обязательного использования шифрования [60].

Протокол «легковесный EAP» (Lightweight EAP, LEAP), который создала компания Cisco, предусматривает не только шифрование данных, но и ротацию ключей. LEAP не требует наличия ключей у клиента, поскольку они безопасно пересылаются после того, как пользователь прошел процесс аутентификации. Это позволяет пользователям легко подключаться к сети, используя учетную запись и пароль.

Ранние реализации LEAP обеспечивали только одностороннюю аутентификацию пользователей. Позднее Cisco добавила возможность взаимной аутентификации. Однако выяснилось, что протокол LEAP уязвим к атакам по словарю [28]. LEAP безопасен в той мере, насколько стоек пароль к попыткам подбора.

Более сильный вариант реализации EAP — EAP-TLS, который использует предустановленные цифровые сертификаты X.509 на клиенте и сервере, был разработан компанией Microsoft. Этот метод обеспечивает взаимную аутентификацию и полагается не только на пароль пользователя, но также поддерживает ротацию и динамическое распределение ключей. Неудобство EAP-TLS заключается в необходимости установки сертификата на каждом клиенте, что может оказаться достаточно трудоемкой и дорогостоящей операцией. К тому же этот метод непрактично использовать в сети, где наблюдается частая смена сотрудников [29].

Производители беспроводного оборудования продвигают решения упрощения процедуры подключения к БС авторизированных пользователей. Эта идея вполне осуществима, если включить LEAP и раздать имена пользователей и пароли. Но если возникает необходимость использования цифрового сертификата или ввода длинного WEP-ключа, процесс может стать утомительным.

Компании Microsoft, Cisco и RSA совместными усилиями разработали новый протокол — PEAP, объединивший простоту использования LEAP и безопасность EAP-TLS. PEAP использует сертификат, установленный на сервере, и аутентификацию по паролю для клиентов [21].

Tunneled TLS (TTLS) - EAP, разработанный компаниями Funk Software и Certicom и расширяющий возможности EAP-TLS. EAP-TTLS использует безопасное соединение, установленное в результате TLS-квитирования для обмена дополнительной информацией между суппликантом и сервером аутентификации [1]. В результате дальнейший процесс может производиться с помощью других протоколов аутентификации, например таких, как: PAP, CHAP, MS-CHAP или MS-CHAP-V2. Сильной стороной этого протокола является простота применения и довольно высокий уровень обеспечиваемой безопасности.

Разные производители поддерживают различные типы EAP, а также несколько типов одновременно. Процесс EAP аналогичен для всех типов (рис. 1.8).


Рис. 1.8 Процесс аутентификации по алгоритму EAP

Сервер RADIUS - своего рода "проходная", на которой решается, пустить пользователя в сеть или нет [43]. К чести некоторых производителей беспроводного доступа (например, D-Link и U.S. Robotics), возможность авторизации и аутентификации пользователя на сервере RADIUS с помощью 802.1x предусмотрена даже в достаточно старых устройствах стандарта 802.11b.

В настоящее время есть несколько популярных реализаций RADIUS-серверов: FreeRadius, GNU Radius, Cistron Radius, Radiator Radius, Microsoft IAS, Advanced Radius. Некоторые из них - коммерческие продукты, некоторые - доступны для бесплатного использования с соблюдением соответствующих лицензионных требований.

В общем случае алгоритм привязки RADIUS-сервера к беспроводной сети может быть таков:

1. сетевой администратор дает команду RADIUS-серверу завести новую учетную карточку пользователя с занесением в нее имени пользователя, под которым он будет проходить аутентификацию, и его пароля;
2. внесенный в базу RADIUS-сервера пользователь с помощью беспроводной связи подключается к точке доступа;
3. точка доступа запрашивает у пользователя его имя и пароль;
4. точка доступа связывается с RADIUS-сервером и дает запрос на аутентификацию пользователя;
5. RADIUS-сервер находит валидные имя пользователя и пароль, разрешает новую сессию и заводит в журнале соответствующую запись о начале новой сессии;
6. точка доступа предоставляет пользователю возможность работать с теми сервисами, которые ему предписаны;
7. по окончании сессии, которая может быть прервана либо самим пользователем, либо RADIUS-сервером, RADIUS-сервер делает в журнале запись об окончании сеанса [46].

Данная процедура достаточно строгая, но в тоже время логически верная - хотя и относится лишь к управлению доступом.

Открытая аутентификация не позволяет точке доступа определить, является ли абонент легитимным или нет. Это становится серьезной брешью в системе безопасности в том случае, если в БС не используется шифрование WEP. В случаях, когда использование шифрования WEP не требуется или невозможно (например, в беспроводных сетях публичного доступа), следует использовать методы аутентификации более высокого уровня.

Аутентификация с общим ключом требует настройки у абонента статического WEP-ключа для шифрования «испытательного текста», отправленного точкой доступа. Но в то же время обмен фреймами, содержащими этот текст, происходит по открытому радиоканалу, а значит, подвержен атакам со стороны стороннего наблюдателя.

Все уязвимости семейства протоколов аутентификации EAP можно подразделить на две группы: уязвимости вне зависимости от используемого типа EAP и уязвимости отдельных EAP разновидностей. К первым относится посылка фальшивых EAP-пакетов через локальную сеть, циклический перебор идентификаторов EAP, а также преждевременной отправкой EAP-пакетов.

Самый первый стандартизированный тип EAP - это EAP-MD5. Его основной уязвимостью является отсутствие какой-либо аутентификации с "серверной" стороны, сопряженное с отсутствием туннелирования трафика этого протокола. Таким образом, злоумышленник может представить свою "пиратскую" точку доступа с большей силой сигнала и сопряженным RADIUS-сервером, и "переманив" клиентские машины на ее сторону после массовой DoS-атаки пакетами деаутентификации, перехватить имена и пароли пользователей. Помимо перехвата паролей, атакующая сторона с помощью данного метода может пытаться взломать подсоединившиеся хосты напрямую.

EAP-LEAP - один из широко распространенных типов EAP. Перехватив обмен запросами между клиентом и точкой доступа, можно использовать оптимизированную атаку перебора по словарю для того, чтобы извлечь пароль. Оптимизация атаки против этого частного протокола возможна потому, что имя пользователя незашифрованно, защищен только пароль.

Что же касается считающихся безопасными EAP-PEAP и EAP-TTLS, использующих туннелирование обмена данными аутентификации, они не так хорошо защищены, как кажется. Старая проблема EAP-MD5, а именно отсутствие аутентификации с "серверной" стороны всплывает здесь с новой силой. Основная часть атак на эти протоколы основана на установлении злоумышленником "пиратской" точки доступа, сопряженной с фальшивым RADIUS-сервером [10].

### 1.3 Криптографическая защита данных в беспроводных сетях

Одними из наиболее эффективных методов защиты информации на сегодняшний день являются криптографические методы защиты информации. Если мы говорим о беспроводных сетях, то широкое распространение для защиты БС приобрели два алгоритма – первоначально WEP, основанный на RC4, а после - AES.

Для того чтобы объективно оценить все плюсы и минусы вышеупомянутых алгоритмов, рассмотрим их структуру.

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 шифрования данных стандарт предоставляет возможности шифрования с использованием алгоритма RC4 с 40-битным разделяемым ключом,

разработанным Роном Райвестом, одним из основателей компании RSA Data Securiy [40].

Рассмотрим основные принципы, на которых построен данный алгоритм шифрования.

При потоковом шифровании выполняется побитовое сложение по модулю 2 ключевой последовательности, генерируемой алгоритмом шифрования на основе заранее заданного ключа, и исходного сообщения. Ключевая последовательность имеет длину, соответствующую длине исходного сообщения, подлежащего шифрованию (рис. 1.9).

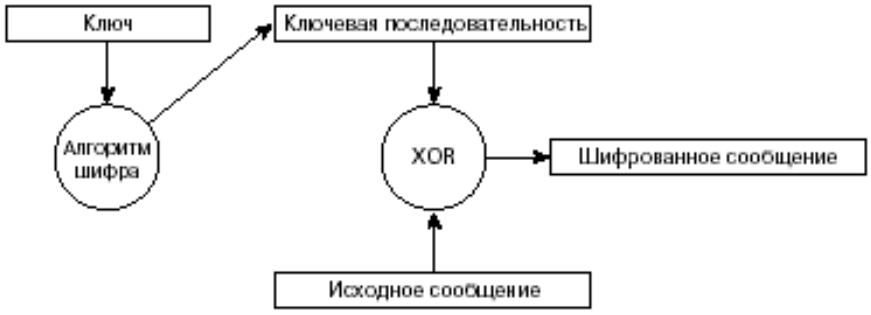


Рис. 1.9 Принцип поточного шифрования

Потоковое шифрование использует метод электронной кодовой книги ECB (Electronic Code Book). Метод ECB характеризуется тем, что одно и то же исходное сообщение на входе всегда порождает одно и то же зашифрованное сообщение на выходе. Это представляет собой потенциальную брешь в системе безопасности, ибо сторонний наблюдатель, обнаружив повторяющиеся последовательности в зашифрованном сообщении, в состоянии сделать обоснованные предположения относительно идентичности содержания исходного сообщения [26].

Для устранения указанной проблемы используют векторы инициализации IV (Initialization Vectors). Вектор инициализации используется для модификации ключевой последовательности. При использовании вектора инициализации ключевая последовательность

генерируется алгоритмом шифрования, на вход которого подаётся секретный ключ, конкатенированный с IV [61]. При изменении вектора инициализации ключевая последовательность также меняется. Стандарт IEEE 802.11 рекомендует использование нового значения вектора инициализации для каждого нового фрейма, передаваемого в радиоканал. Таким образом, один и тот же нешифрованный фрейм, передаваемый многократно, каждый раз будет порождать уникальный шифрованный фрейм.

Сам алгоритм WEP является алгоритмом симметричного потокового шифрования, он достаточно прост и заключается в следующем. Из 24-х битного инициализационного вектора IV, который увеличивается на единицу на каждом следующем пакете, а также из ключа длиной 40 бит, формируется путем склейки 64-разрядный вектор начальной установки. Он используется для приведения в исходное состояние генератора псевдослучайных последовательностей, базирующегося на шифре Вернама, начинающего формировать псевдослучайную последовательность двоичных символов, равную длине передаваемого пакета с 4-байт контрольной комбинацией циклического кода CRC. Такая последовательность складывается поразрядно с символами передаваемого пакета и CRC. Данная операция выполняется с целью избегания методов взлома, основанных на статистических свойствах открытого текста. После этого, к сформированному коду добавляется входящий в открытом виде инициализационный вектор, а также номер использованного ключа [3]. Вектор инициализации присутствует в нешифрованном виде в заголовке фрейма в радиоканале, с тем, чтобы принимающая сторона могла успешно декодировать этот фрейм. Далее, пакет передается через эфир.

Дешифрование пакета на принимающей стороне происходит в обратном порядке. На принимающей стороне из пакета выделяется 4-разрядный вектор инициализации, из которого в результате конкатенации с тем же секретным ключом, что и на передающей стороне, формируется вектор начальной установки генератора псевдослучайной

последовательности. Сформированная последовательность суммируется по модулю 2 с зашифрованной частью принятого пакета, в результате чего выделяются незашифрованные данные и CRC, используемая для контроля правильности приема пакета данных (рис. 1.10) [7].

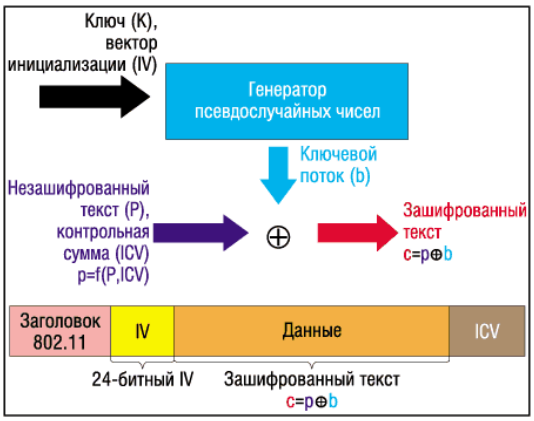


Рис. 1.10 Схема работы шифрования по алгоритму WEP

Когда используется шифрование, точка доступа будет посылать зашифрованный пакет любой станции, пытающейся подключиться к ней. Клиент должен использовать свой ключ для шифрования корректного ответа для того, чтобы аутентифицировать себя и получить доступ в сеть. Выше второго уровня сети 802.11b поддерживают те же стандарты для контроля доступа и шифрования (например, IPSec), что и другие сети 802.

Достоинства алгоритма WEP:

- возможность периодической смены ключа и частой смены вектора инициализации;
- самосинхронизация шифра по каждому сообщению, что снижает вероятность потери пакетов;
- эффективность алгоритма и возможность его реализации как программными, так и аппаратными средствами;
- статус дополнительной возможности, что позволяет пользователю самому решать вопрос об использовании этого алгоритма.

Однако столь простая система защиты трафика недостаточно устойчива к некоторым вариантам атак. Система защиты БС, основанная на WEP со статическими ключами, 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.

Усовершенствования версии WEP2 устраняют проблему конфликтов IV, но совместное администрирование WEP-ключей в различных системах и устранение уязвимости контроля целостности так и осталось без изменений [34].

Стандартом IEEE 802.11 не предусмотрены какие-либо механизмы управления ключами шифрования. По определению, алгоритм WEP поддерживает лишь статические ключи, которые заранее распространяются тем или иным способом между абонентами и точками доступа беспроводной сети. Поскольку IEEE 802.11 аутентифицирует физическое устройство, а не его пользователя, утрата абонентского адаптера, точки доступа или собственно секретного ключа представляют опасность для всей системы безопасности в целом. В результате при каждом подобном инциденте администратор сети будет вынужден вручную произвести смену ключей у всех абонентов и в точках доступа. Эти административные действия приемлемы для небольшой БС, но совершенно неприемлемы для сетей, в которых абоненты исчисляются сотнями и тысячами, и/или распределены территориально [17]. В условиях отсутствия механизмов генерации и распространения ключей администратор вынужден пристально охранять абонентские адаптеры и оборудование инфраструктуры сети, что на практики является весьма трудновыполнимой задачей.

Следующим шагом на пути увеличения безопасности беспроводных сетей является применение нового алгоритма шифрования AES, который принят в качестве государственного стандарта шифрования США взамен утратившего свои позиции DES.

AES – это симметричный итерационный блочный шифр, оперирующий блоками данных размером 128 и длинной ключа 128, 192 или 256 бит – название стандарта соответственно «AES-128», «AES-192» и «AES-256» (рис. 1.11).


Рис. 1.11 Принцип блочного шифрования

Алгоритм является нетрадиционным блочным шифром, поскольку не использует сеть Фейстеля для криптопреобразований [70]. Алгоритм AES представляет каждый блок кодируемых данных в виде двухмерного массива байтов размером 4x4, 4x6 или 4x8 в зависимости от установленной длины блока. Далее на соответствующих этапах производятся преобразования либо над независимыми столбцами, либо над независимыми строками, либо вообще над отдельными байтами в таблице.

Алгоритм состоит из определённого количества раундов (от 10 до 14 - это зависит от размера блока и длины ключа), в которых последовательно выполняются преобразования. Для AES количество раундов определено равным 10. Преобразование каждого раунда состоит из четырех различных преобразований, называемых слоями. Каждый слой разрабатывался с учетом

противодействия линейному и дифференциальному криптоанализу. В основу каждого слоя положена своя собственная функция [33].

Все преобразования в шифре AES имеют строгое математическое обоснование. Структура алгоритма AES и последовательность операций позволяют эффективно выполнять данный алгоритм как на 8-ми, так и на 32-битовых процессорах. В структуре алгоритма заложена возможность параллельного исполнения некоторых операций [2]. С алгоритма AES сняты все патентные ограничения - его можно использовать в любой криптопрограмме без отчисления каких-либо средств создателям.

Можно отметить следующие преимущества, относящиеся к аспектам реализации данного алгоритма:

- AES может выполняться быстрее, чем обычный блочный алгоритм шифрования за счет выполнения оптимизация между размером таблицы и скоростью выполнения;
- преобразование раунда допускает параллельное выполнение, что является важным преимуществом для будущих процессоров и специализированной аппаратуры;
- алгоритм шифрования не использует арифметические операции, поэтому тип архитектуры процессора не имеет значения;
- алгоритм шифрования полностью "самоподдерживаемый", то есть он не использует других криптографических компонентов;
- длины блоков от 192 до 256 бит позволяют создавать хэш-функции без коллизий, использующие AES в качестве функции сжатия;
- разработка позволяет специфицировать варианты длины блока и длины ключа в диапазоне от 128 до 256 бит с шагом в 32 бита;
- хотя число раундов AES зафиксировано, в случае возникновения проблем с безопасностью оно может модифицироваться и выступать в качестве параметра [57].

Недостатком же 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. Он появился совсем недавно и обладает хорошей криптостойкостью (на данный алгоритм пока нет известных атак), а его симметричная природа делает его достаточно быстрым. Таким образом, на сегодняшний день атаки на AES не увенчались успехом [19]. Хотя недавно были открыты поразительные алгебраические особенности AES и родственных ему методов. Хотя до реальной атаки на AES еще очень далеко, однако теоретически добраться до нее можно.

## 1.4 Классификация угроз и атак на беспроводные сети

Так как беспроводные сети используют воздух и пространство для передачи и приема информации (сигналы являются открытыми для любого лица, находящегося в зоне действия), безопасность передачи данных является очень важным аспектом безопасности всей системы в целом. Без обеспечения должной защиты конфиденциальности и целостности информации при ее передаче между рабочими станциями и точками доступа нельзя быть уверенным в том, что информация не будет перехвачена злоумышленником, и что рабочие станции и точки доступа не будут подменены посторонним лицом.

Широкое распространение беспроводных устройств и их небольшая стоимость приводят к тому, что в периметре сетевой безопасности возникают бреши.

Специфика БС подразумевает, что данные могут быть перехвачены и изменены в любой момент. Для одних технологий достаточно стандартного беспроводного адаптера, для других требуется специализированное оборудование. Но в любом случае, эти угроза реализуются достаточно

просто, и для противостояния им требуются эффективные криптографические механизмы защиты данных.

По своей природе беспроводные сети не могут обеспечивать высокую доступность. Различные природные, техногенные и антропогенные факторы могут эффективно нарушать нормальное функционирование радиоканала. Этот факт должен учитываться при проектировании сети, и БС не должны использоваться для организации каналов при высоких требованиях к доступности [14].

Изначально определим основные термины, которые будут использоваться в дальнейшем: "уязвимость", "угроза" и "атака". Под уязвимостью системы защиты понимается такое ее свойство (архитектурный, либо иной недостаток), которое может быть использовано злоумышленником для осуществления НСД к информации. Другими словами, уязвимость – это "канал" НСД к защищаемой информации. При этом любая уязвимость системы защиты несет в себе угрозу осуществления злоумышленником НСД к информации, посредством реализации атаки (либо атак, которые в общем случае могут принципиально различаться) на уязвимость в системе защиты [56].

Таким образом, именно уязвимость системы защиты – это признак системы, а наличие (отсутствие) уязвимостей является характеристикой защищенности системы [5].

Очевидно, что в общем случае причиной уязвимости (существования "канала" НСД) может являться либо некорректность реализации механизма защиты, либо недостаточность набора механизмов для условий использования защищаемого объекта информатизации. Вообще говоря, свойства корректности реализации и полноты (достаточности для условий использования) являются основополагающими свойствами любой технической системы, в том числе, и свойствами системы защиты информации [62].

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.

Готовясь к обеспечению безопасности беспроводных сетей, прежде всего, необходимо установить, что может им угрожать.

Сразу необходимо заметить, что беспроводные сети отличаются от кабельных только на первых двух - физическом и отчасти канальном - уровнях семиуровневой модели взаимодействия открытых систем. Более высокие уровни реализуются в соответствии с теми же принципами, что и в проводных сетях, а реальная безопасность сетей обеспечивается именно на этих нижележащих уровнях.

Принято считать, что безопасности беспроводных сетей угрожают:

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

Угрозу сетевой безопасности могут представлять природные явления и технические устройства, однако только люди внедряются в сеть для намеренного получения или уничтожения информации и именно они представляют наибольшую угрозу.

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.

Кроме того, до сих пор не разработана детальная модель угроз, существующих в области цифровых сетей беспроводного доступа, и методов борьбы с ними.

В табл. 1.2 и 1.3 представлена общая информация об основных типах угроз и средствах их нейтрализации, как на сигнальном, так и на информационном уровне.

Нужно отметить, что высокая степень защищенности канала на сигнальном уровне не является гарантией обеспечения столь же высокой информационной защищенности всей системы. Это обусловлено тем, что основным показателем успешного функционирования отдельного компонента системы является реализация его целевой функции. Сигнальный уровень является нижним и обеспечивает нейтрализацию конфликтного компонента или угрозы только на своем участке.

Табл. 1.2 Типы и источники угроз в БС на сигнальном уровне

| **Угроза** | **Условия реализации угрозы** | **Уязвимый элемент системы** | **Средства нейтрализации угрозы** |
|---|---|---|---|
| **Угрозы естественного происхождения** | | | |
| Электромагнитное излучение | Плохое экранирование приемной аппаратуры, побочные полосы | Приемник | Адаптивное управление параметрами приемного и передающего трактов |

Продолжение табл. 1.2

| **Угроза** | **Условия реализации угрозы** | **Уязвимый элемент системы** | **Средства нейтрализации угрозы** |
|---|---|---|---|
| Интерференция | Наличие отражающих поверхностей, низкое расположение антенн | Приемник, передатчик | Выбор оптимального расположения антенны передатчика |
| Механические перемещения | Наличие незакрепленных деталей | Антенны | Уменьшение вибраций, выбор оптимального расположения антенн |
| **Угрозы, возникающие в результате деятельности человека** | | | |
| Аппаратные и программные ошибки при разработке | Неполное тестирование аппаратуры | Система в целом | Проведение комплексной предэксплуатацион-ной проверки |
| Ошибки протокола обмена | Наличие пересечений в сигнальных и логических областях команд и директив | Система управления | Фильтрация сигналов и директив управления на информационном уровне |

Продолжение табл. 1.2

| **Угроза** | **Условия реализации угрозы** | **Уязвимый элемент системы** | **Средства нейтрализации угрозы** |
|---|---|---|---|
| Нарушения регламента связи | Неполная реализация протокола | Система управления | Дополнение регламентированных сигналов и директив управления |
| Ошибки при передаче и приеме сигнала | Работа в условиях помех | Приемная и передающая системы | Повышение уровня фильтрации |
| Перехват сигнала в основном канале | Наличие аппаратуры на прием | Канал передачи | Изменение каналов в ходе сеанса связи |
| Перехват сигнала в побочных каналах | Низкая фильтрация сигнала основного канала | Цепи питания и заземления | Установка фильтров в дополнительных цепях |
| Перехват сигналов до и после шифрования | Наличие в каналах незашифрованной и расшифрованной информации | Приемные и передающие тракты | Задержка при передаче шифрованного сигнала, повышение уровня фильтрации |

Продолжение табл. 1.2

| Угроза | Условия реализации угрозы | Уязвимый элемент системы | Средства нейтрализации угрозы |
|---|---|---|---|
| Перехват сопровождающих передачу акустических, вибрационных и других сигналов | Доступность пунктов приема и передачи | Система в целом | Маскировка побочных сигналов, создание помех для аппаратуры перехвата |

Табл. 1.3 Типы угроз в БС на информационном уровне

| Угроза | Условия реализации угрозы | Уязвимый элемент | Средства нейтрализации угрозы |
|---|---|---|---|
| **Перехват информации** | | | |
| Выявление канала передачи для перехвата | Наличие в передаваемых данных отличительных признаков, работа на одном канале | Системы шифрования и управления каналами | Исключение отличительных признаков данных, изменение номера канала в течение сеанса связи |
| Определение формата данных | Использование стандартных форматов без дополнительной коррекции | Системы кодирования и шифрования | Использование оригинальных форматов, проведение коррекции данных |

Продолжение табл. 1.3

| **Угроза** | **Условия реализации угрозы** | **Уязвимый элемент** | **Средства нейтрализации угрозы** |
|---|---|---|---|
| Восстановление пакетов (кадров) | Отсутствие маскировки синхронизации и маркеров доступа | Система управления обменом | Применение адаптивного кодирования |
| Линейное декодирование | Возможность сбора статистики передачи информации, использование при передаче открытых кодов | Кодер/декодер | Применение мер защиты на сигнальном уровне |
| Дешифрование декодированных данных | Наличие коррелятов в базе принимаемого (перехваченного) сигнала, компрометация ключей, получение блока нешифрованного сигнала | Система организации обмена данными | Оптимизация регламента обмена по критериям времени работы, смена кодов и ключевых последовательностей |

Продолжение табл. 1.3

| **Угроза** | **Условия реализации угрозы** | **Уязвимый элемент** | **Средства нейтрализации угрозы** |
|---|---|---|---|
| **Искажение данных** | | | |
| Передача ложного сигнала в ходе имитации вызова | Возможность определения протокола обмена | Система приема и управления приемом | Использование специальных маркеров идентификации и аутентификации в каждом кадре (блоке) сеанса связи |
| Передача ложного сигнала в ходе сеанса связи | Возможность выделения и определения идентификационных преамбул | Система приема и управления приемом | Использование дополнительного канала для передачи служебных маркеров, разнесение во времени передачи контрольных сумм и квитанций |
| Легальная передача ложной информации | Наличие логического или физического адреса объекта воздействия | Система в целом | Проверка в процессе передачи подлинности адресных ссылок, аутентификация абонентов |

Продолжение табл. 1.3

| **Угроза** | **Условия реализации угрозы** | **Уязвимый элемент** | **Средства нейтрализации угрозы** |
|---|---|---|---|
| Искажение сигнала передачи | Возможность вскрытия синхронизации и входа в канал без ее нарушения | Приемопередающая система | Использование двойной синхронизации, в том числе по дополнительному каналу |
| **Перехват управления** | | | |
| Передача управляющих последовательностей абоненту | Возможность получения мастер-кодов, компрометация кодов систем защиты | Системы управления связью | Отложенное выполнение команд, исключение возможности дистанционного перепрограммирования абонентского комплекта |
| Передача управляющих последовательностей на центральную станцию | Возможность получения мастер-кодов, компрометация кодов систем защиты, доступ к процессору и программам управления. | Системы управления связью и коммутации | Проведение организационных мероприятий, совершенствование ПО безопасности и защиты информации |

# ГЛАВА 2. МОДЕЛЬ ПОСТРОЕНИЯ СЕМЕЙСТВА ПРОФИЛЕЙ ЗАЩИТЫ ДЛЯ БЕСПРОВОДНОЙ СЕТИ

## 2.1 Специфика создания профиля защиты для сетей стандарта 802.11

ГОСТ Р ИСО/МЭК 15408 определяет критерии, за которыми исторически закрепилось название "Общие критерии" (ОК). Он направлен на защиту информации от несанкционированного раскрытия, модификации или потери возможности ее использования.

На сегодняшний день "Общие критерии" - самый полный и современный оценочный стандарт. На самом деле, это метастандарт, определяющий инструменты оценки безопасности информационных систем (ИС) и порядок их использования; он не содержит предопределенных классов безопасности. Такие классы можно строить, опираясь на заданные требования.

ОК содержат два основных вида требований безопасности:

- функциональные, соответствующие активному аспекту защиты, предъявляемые к функциям (сервисам) безопасности и реализующим их механизмам;
- требования доверия, соответствующие пассивному аспекту; они предъявляются к технологии и процессу разработки и эксплуатации [13].

Требования безопасности формулируются, и их выполнение проверяется для определенного объекта оценки (ОО) - аппаратно-программного продукта или информационной системы.

ОК способствуют формированию двух базовых видов используемых на практике нормативных документов - это профиль защиты (ПЗ) и задание по безопасности (ЗБ) [52].

ГОСТ Р ИСО/МЭК 15408 содержит критерии, которые должны использоваться оценивающими (экспертами) при формировании суждений о

соответствии ОО требованиями по их безопасности. Документ описывает множество общих действий, которые должен выполнить эксперт, и функции безопасности, в соответствии с которыми выполняются эти действия. Отметим, что ОК не определяют процедуры, которым надо следовать при проведении этих действий.

Для того чтобы достичь большей сравнимости результатов оценки между собой, оценки должны выполняться в рамках согласованной системы (схемы) оценки, которая учитывает стандарты, следит за качеством оценок и управляет правилами, которым должны соответствовать средства оценки и оценивающие.

Использование общей методологии оценок содействует воспроизводимости и объективности результатов, но само по себе не является достаточным. Многие из критериев оценки требуют применения экспертного заключения и дополнительных знаний и навыков, по которым труднее достичь согласованности. Чтобы повысить согласованность полученных данных по оценке, окончательные результаты оценки можно подвергнуть процессу сертификации. Процесс сертификации является независимой проверкой результатов оценки, ведущей к выработке конечного сертификата или подтверждения. Сертификат обычно публично доступен.

Общие критерии представляют собой требования безопасности под определенные категории функциональных требований и требований гарантии [23].

Функциональные требования накладываются на те функции ОО, которые существуют специально для поддержки безопасности продукта информационных технологий и определяют желаемое поведение в части безопасности [64].

При создании и развитии сложных, распределенных, тиражируемых информационных систем (ИС) требуется гибкое формирование и применение гармонизированных совокупностей базовых стандартов и нормативных документов разного уровня, выделение в них требований и рекомендаций,

необходимых для реализации заданных функций ИС. Для унификации и регламентирования такие совокупности базовых стандартов должны адаптироваться и конкретизироваться применительно к определенным классам проектов, функций, процессов и компонентов ИС [35]. В связи с этой потребностью выделилось и сформировалось понятие профилей защиты, как основного инструмента функциональной стандартизации.

Профиль - это совокупность нескольких (или подмножество одного) базовых стандартов с четко определенными и гармонизированными подмножествами обязательных и факультативных возможностей, предназначенная для реализации заданной функции или группы функций. Функциональная характеристика объекта стандартизации является исходной для формирования и применения профиля этого объекта или процесса [49]. В профиле защиты выделяются и устанавливаются допустимые факультативные возможности и значения параметров каждого базового стандарта и/или нормативного документа, входящего в профиль. Профиль не может противоречить использованным в нем базовым стандартам и нормативным документам. Он должен применять выбранные из альтернативных вариантов факультативные возможности и значения параметров в пределах допустимых. На базе одной совокупности базовых стандартов могут формироваться и утверждаться различные профили для разных ОО. Эти ограничения базовых документов профиля и их гармонизация, проведенная разработчиками профиля, должны обеспечивать качество, совместимость и корректное взаимодействие компонентов системы, соответствующих профилю, в заданной области его применения.

Состояние и развитие стандартизации в области информационных технологий характеризуются следующими особенностями:

- несколько сотен международных и национальных стандартов не полностью и неравномерно удовлетворяют потребности в стандартизации ОО и процессов их создания;

- длительные сроки разработки, согласования и утверждения международных и национальных стандартов (обычно данный процесс занимает порядка 3-5 лет) приводят к их консерватизму и хроническому отставанию от современных технологий;
- современные стандарты в области информационных технологий (ИТ) должны учитывать необходимость построения ИС как открытых систем, обеспечивать их расширяемость при наращивании или изменении выполняемых функций: переносимость программного обеспечения и возможность взаимодействия с другими ИС [35].

В международной функциональной стандартизации ИТ принята жесткая трактовка понятия профиль. Считается, что его основой могут быть только международные и национальные, утвержденные стандарты - не допускается использование стандартов де-факто и нормативных документов негосударственных организаций. Подобное понятие профиля активно используется в гамме международных функциональных стандартов, конкретизирующих и регламентирующих основные процессы и объекты взаимосвязи открытых систем, в которых возможна и целесообразна жесткая формализация профилей (функциональные стандарты ИСО 10607 - 10613 и соответствующие им ГОСТ Р) [8]. Однако при таком подходе невозможны унификация, регламентирование и параметризация множества конкретных функций и характеристик сложных объектов архитектуры и структуры современных ИС.

Новый, прагматический подход к разработке и применению ПЗ состоит в использовании совокупности адаптированных и параметризованных базовых международных и национальных стандартов и открытых спецификаций, отвечающих стандартам де-факто и рекомендациям международных консорциумов.

Профиль защиты информации должен обеспечивать реализацию политики информационной безопасности, разрабатываемой в соответствии с требуемой категорией безопасности и критериями безопасности [12].

Специфика создания ПЗ для БС базируется на специфике их построения, особенностях конфигурации и технологии обработки и передачи информации, которые уже были рассмотрены ранее. За счет открытой среды передачи данных в беспроводных сетях должны быть усилены требования безопасности, выдвигаемые к ОО на этапах аутентификации, контроля доступа и шифрования передаваемой информации.

Зачастую положения ПЗ для БС во многом пересекаются с традиционным содержанием подобных документов (табл. 2.1). Так, например, требования по физической защиты точек доступа вполне перекрываются вопросами физической безопасности активного сетевого оборудования [14] .

Табл. 2.1 Основные требования безопасности к БС

| **Требования к безопасности** | **Специфика беспроводных сетей** |
|---|---|
| Контроль подключений к сети | Уровень риска, связанного с подключением несанкционированной точки доступа или клиента беспроводной сети, можно снизить путем отключения неиспользуемых портов коммутаторов, фильтрации по MAC-адресам (port-security), аутентификации 802.1x, систем обнаружения атак и сканеров безопасности, контролирующих появление новых сетевых объектов. |

Продолжение табл. 2.1

| **Требования к безопасности** | **Специфика беспроводных сетей** |
|---|---|
| Физическая безопасность | Контроль мощности излучаемого сигнала позволяет ограничить вероятность подключения к сети беспроводных устройств. Описание в политике безопасности (ПБ) организации ограничения доступа пользователей и посетителей к сетевым портам и слотам расширения компьютера снижает вероятность подключения беспроводного устройства. |
| Минимизация привилегий пользователя | Если пользователь работает на компьютере с минимально необходимыми правами, то снижается вероятность самовольного изменения настроек беспроводных интерфейсов |
| Контроль политики безопасности | Средства анализа защищенности, такие как сканеры уязвимостей, позволяют обнаруживать появление в сети новых устройств и определить их тип (функции определения версий ОС и сетевых приложений), а также отслеживать отклонения настроек клиентов от заданного профиля. |
| Инвентаризация ресурсов | Наличие актуального обновляемого списка сетевых ресурсов облегчает обнаружение новых сетевых объектов. |
| Обнаружение атак | Применение систем обнаружения атак как традиционных, так и беспроводных дает возможность своевременно определять попытки несанкционированного доступа |

Но выделим ряд требований, которые ставятся во главу угла при написании ПЗ для БС, так как при их использовании или внедрении требуется внесение дополнений в разделы ПЗ, приведенные в таблице 2.2:

Табл. 2.2 Дополнительные требования безопасности к БС

| **Требования к безопасности** | **Специфика беспроводных сетей** |
|---|---|
| Нормативно-правовое обеспечение | Использование беспроводных сетей попадает под действие как российских, так и международных нормативных актов. Так, в России использование частотного диапазона 2,4 ГГц регулируется решением государственной комиссии по радиочастотам от 06.12.2004 (№04-03-04-003). 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. |
| Обнаружение атак | Должны быть определены требования к системам обнаружения беспроводных атак, закреплена ответственность за анализ событий. |

Продолжение табл. 2.2

| **Требования к безопасности** | **Специфика беспроводных сетей** |
|---|---|
| Разделение сетей | В связи со спецификой беспроводных сетей 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. |
| Допустимость использования программного и аппаратного обеспечения | Должны быть отдельно специфицированы требования к точкам доступа, беспроводным коммутаторам и клиентам беспроводной сети. |
| 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. |

## 2.2 Графо-аналитическая модель структуры семейства профилей защиты

В Руководящем документе «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.

Функциональные требования безопасности (ФТБ), общие для всех изделий ИТ некоторой группы составляют функциональный пакет группы. В функциональный пакет группы включается базовый функциональный пакет (БФП) семейства ПЗ и требования безопасности, специфичные для изделий ИТ данной группы (рис. 2.1) [53]. ФТБ, общие для всех изделий ИТ одного типа составляют БФП семейства ПЗ.


Рис. 2.1 Процесс разработки функционального пакета группы

Для построения графо-аналитической модели структуры семейства ПЗ представим сам ПЗ в наглядном виде. В общем виде структура профиля защиты представлена на рис. 2.2.

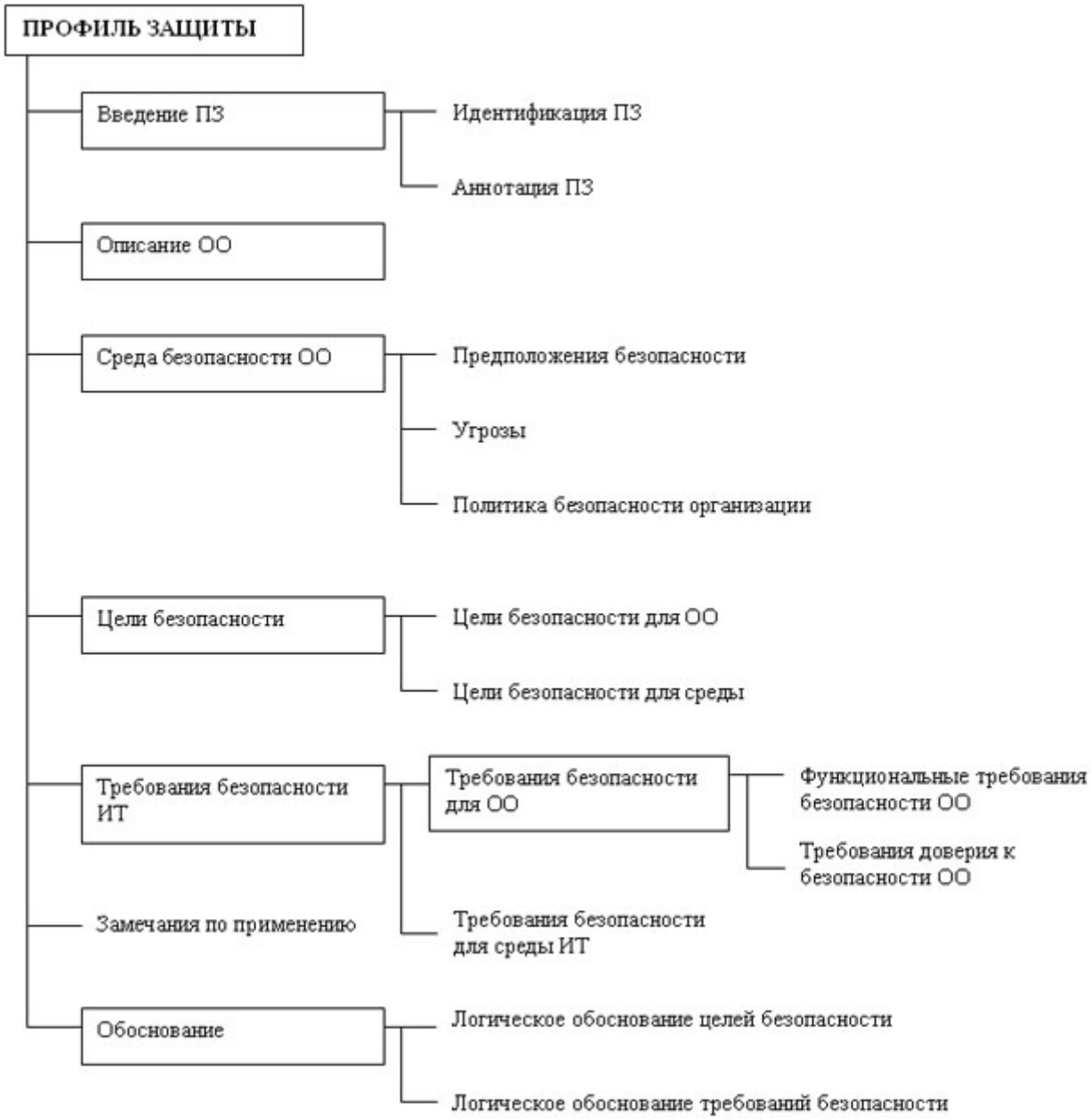


Рис. 2.2 Общая структура профиля защиты

Объединив описанные выше понятия ПЗ и БФП семейства ПЗ, построим схему формирования ПЗ на основе выработанного для семейства БФП (рис. 2.3).

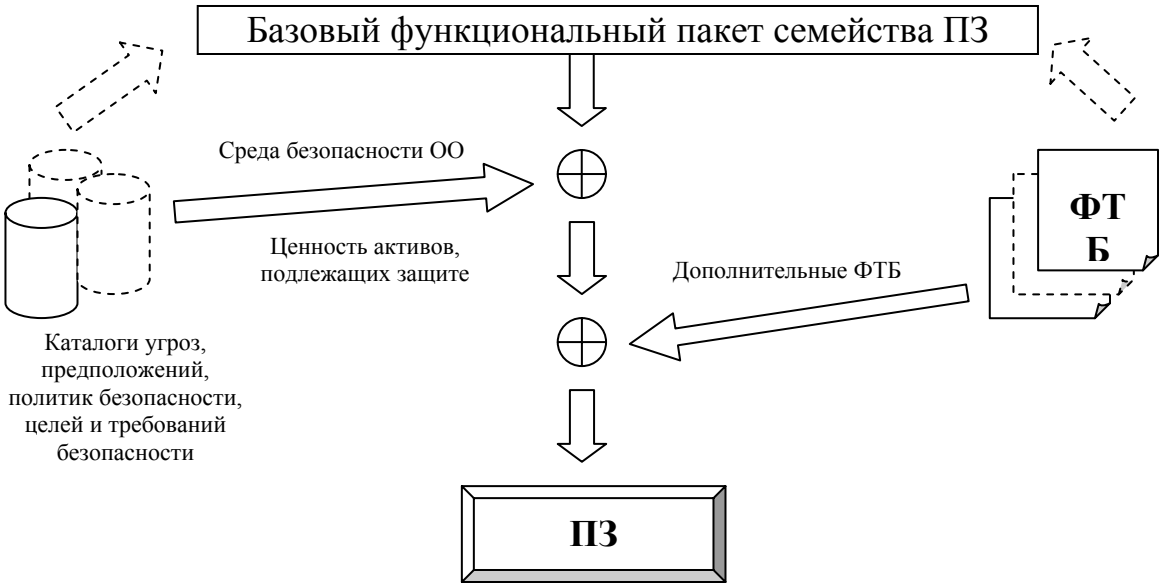


Рис. 2.3 Схема формирования профиля защиты

Исходя из приведенной выше структуры типового ПЗ и прибегая к теории графов, построим в общем виде модель данной структуры (рис. 2.4):

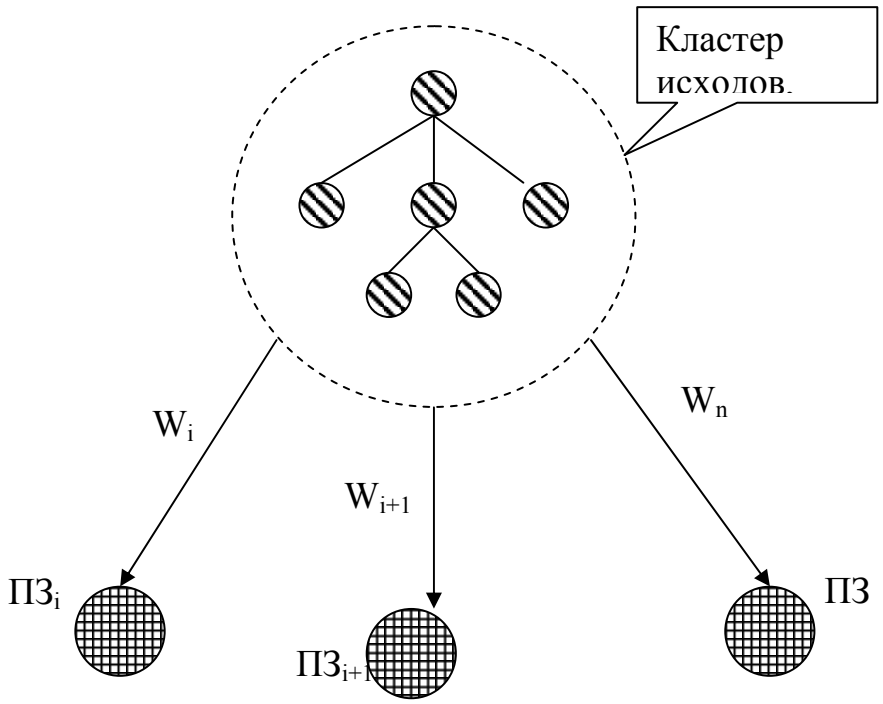


Рис 2.4 Модель структуры семейства профилей защиты

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

$$БФП = \{W_б\} = \{У_б, ЦБ_б\}, \quad (2.1)$$

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

$\{У_б, ЦБ_б\}$ – множество базовых угроз для ОО и противопоставляемых им базовых целей безопасности (ЦБ) [22].

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

$$\{W_d\} = \{У_d, ЦБ_d\}. \quad (2.2)$$

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

$$ПЗ_i = БФП + \{W_d\} = \{W_б\} + \{W_d\} = \{У_б, ЦБ_б\} \cup \{У_d, ЦБ_d\}. \quad (2.3)$$

Таким образом, мы получили совокупность компонентов ПЗ исходя из принципа формирования семейства ПЗ.

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 [30].

Обозначим ПЗ как следующее множество – совокупность четырех сервисных служб защиты – аутентификации, конфиденциальности, достоверности и контроля доступа, которые и реализуются агентами защиты (рис. 2.5):

$$ПЗ = \{G_А, G_К, G_Д, G_Ц\}, \quad (2.4)$$

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).

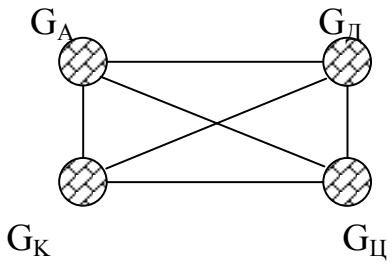


Рис. 2.5 Модель структуры профиля защиты при равном весе агентов защиты

Все сервисные службы по умолчанию имеют равнозначный вес при построении ПЗ, но в зависимости от специфики ОО и его среды безопасности одни могут превалировать над другими (рис. 2.6).

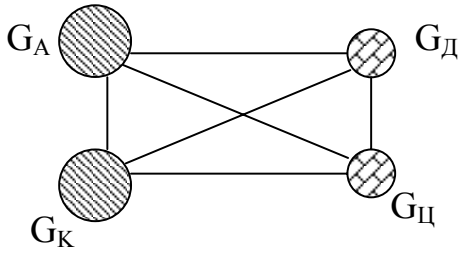


Рис. 2.6 Модель структуры профиля защиты при неравном весе агентов защиты

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 (2.3) и (2.4). Приравняв их, получаем следующее:

$$\{У_б, ЦБ_б\} \cup \{У_д, ЦБ_д\} = \{G_А, G_R, G_Д, G_Ц\}. \quad (2.5)$$

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:

$$ПЗ = \{G_{А_б}, G_{К_б}, G_{Д_б}, G_{Ц_б}\} + \{G_{А_д}, G_{К_д}, G_{Д_д}, G_{Ц_д}\}. \quad (2.6)$$

Проинтегрируем полученное равенство (2.6):

$$ПЗ = \sum_x \int_{i=1}^{n} G_{x_б} dM + \sum_x \int_{j=1}^{m} G_{x_д} dM , \quad (2.7)$$

где $x = \{A, K, Д, Ц\}$, 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:

$$\{i + j\} \subseteq \{W\} . \quad (2.8)$$

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

$$ПЗ = \sum_x \int_{z=1}^{n+m} G_{x_z} dM . \quad (2.9)$$

Таким образом, исходя из полученных равенств (2.6) и (2.9), для построения семейства ПЗ первоначально необходимо определить множество базовых агентов защиты беспроводной сети, другими словами определить ее защищенность.

Для того, чтобы оценить защищенность беспроводной сети, а впоследствии проанализировать полученные результаты, нам необходимо

выработать ряд критериев, в соответствии с которыми будет возможно произвести оценку сети.

## 2.3 Критерии оценки защищенности беспроводной сети

Обратимся к определению информационной безопасности (ИБ), ИБ - обозначает защиту информацию и информационных систем от неавторизированного доступа, использования, обнаружения, искажения, уничтожения, модификации. ИБ обеспечивает доступность, целостность и конфиденциальность информации [20]. Для реализации ИБ БС используются средства (механизмы) защиты информации.

Для получения критериев оценки защищенности беспроводной сети предлагается метод, цель которой заключается в оценке безопасности БС на основе использующих в ней средств защиты информации. Причем рассматриваются только те средства, которые описаны непосредственно в семействе стандартов 802.11 [13], то есть мы исключаем механизмы защиты, направленные на предотвращение конкретных видов атак и включаемые в систему защиты беспроводной сети дополнительно, например, для предотвращения атак по типу «червя» (wormhole-атак) [25], для борьбы с которыми используется либо специфическое оборудование (например, направленные антенны) либо разрабатываются специальные протоколы маршрутизации (LiteWorp или TIK).

Для разработки системы критериев оценки защищенности БС проведем анализ семейства стандартов 802.11 в разрезе реализованных в них механизмов защиты.

Как уже упоминалось выше, особенностью реализации БС является открытость каналов передачи информации, так как физически они практически незащищены. Исходя из этого, большое внимание уделяется защите информации, передаваемой по этим каналам. На сегодняшний день лучшим методом защиты данных является их шифрование. Таким образом,

можно сформировать первую группу критериев, которые будут оценивать защищенность сети с точки зрения, реализованных в ней криптографических функций.

Но недостаточно просто ограничиться шифрованием трафика. Использовавшийся изначально алгоритм WEP имеет достаточное количество уязвимостей [38], и усиление его криптографической стойкости за счет увеличения длины ключа либо вектора инициализации заведомо не может привести к должному уровню безопасности сети.

Получив НСД к каналу передачи данных БС, злоумышленник может считать передаваемую информацию и в дальнейшем использовать ее в своих целях. Для предотвращения НСД к передаваемому уже зашифрованному трафику необходимо контролировать возможность доступа к самой сети и ее каналам связи.

Для этих целей используется идентификация пользователей и подключаемого к сети оборудования, их аутентификация и авторизация.

Таким образом, можно выделить две группы критериев, в соответствии с которыми и будет произведено исследование средств защиты, реализованных в семействе стандартов 802.11: криптографические критерии и критерии аутентификации.

В БС шифрование трафика, как уже упоминалось выше, осуществляется посредством использования двух криптографических алгоритмов. Первоначально в качестве стандарта для беспроводных сетей был принят алгоритм WEP. Но после того, как было обнаружено достаточное число его уязвимостей, он был заменен на алгоритм следующего поколения AES. Соответственно первым критерием при оценке защищенности сети является используемый в ней криптографический алгоритм.

Изменение алгоритма шифрования данных в стандарте 802.11 представляло собой довольно длительный процесс. Для выхода из сложившейся ситуации, когда используемый алгоритм уже не мог обеспечить должного уровня безопасности передаваемых данных, а новый

еще не был одобрен в качестве стандарта, было предложено увеличить длину ключевой последовательности. Это привело к улучшению криптостойкости шифра. С введением в стандарт нового алгоритма AES возможность варьировать длину ключа не исчезла, что позволило ранжировать уровень безопасности сети в зависимости от среды ее развертывания, используемого при ее построении оборудования и других факторов. Таким образом, вторым критерием при оценке защищенности является длина используемого при шифровании ключа.

Те же причины, которые повлияли на применение при шифровании ключей разной длины, привели и к использованию динамических ключей. Изначально ключ был статистическим. Так как данное свойства ключа непосредственно влияет на криптозащищенность трафика сети, то его можно использовать в качестве третьего критерия.

Все выработанные выше критерии призваны обеспечивать конфиденциальность сети.

Для реализации такого свойства ИБ как целостность в БС используются специальные технологии проверки целостности сообщений. Они представляют следующий критерий в группе криптографических критериев. Принадлежность технологий проверки целостности сообщений именно к этой группе критериев определяется криптографической основой при построении контрольных пакетов целостности данных.

Для поддержания последнего свойства ИБ: доступности – в беспроводных сетях применяются средства защиты направленные на контроль доступа к ней. Для их структуризации выработаем ряд критериев аутентификации.

Одним из важнейших средств защиты в данной сфере является протокол, в соответствии с которым и осуществляется разграничение доступа. Используемый протокол аутентификации как раз и представляет первый и основной критерий в этой группе.

Развитие семейства стандартов 802.11 как с точки зрения криптографии, так и с точки зрения аутентификации происходило параллельно. Для улучшения безопасности и усиления защиты сети вводятся новые алгоритмы. Зачастую они уже были реализованы и широко используются в проводных сетях, но для их адаптации к задачам беспроводных соединений потребовалось значительно больше времени.

Наиболее защищенными принято считать такие виды сетей, как проводные, так и беспроводные, в которых наряду с криптографической защитой передаваемых данных реализована также и криптографическая защиты данных пользователей, используемая для получения доступа к ресурсам сети. Для БС подобная возможность была выражена при помощи применения, а впоследствии и закрепления в стандарте 802.11i, цифровых сертификатов. Их наличие либо отсутствие при построении сети значительно влияет на ее конечную защищенность. Таким образом, использование цифровых сертификатов при доступе к БС стоит включить в критерии аутентификации в качестве последнего критерия.

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

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

- Криптографические критерии
- 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.

## 2.4 Сопоставление критериев оценки защищенности беспроводной сети функциональным требованиям безопасности ГОСТ Р ИСО/МЭК 15408

Для каждого выделенного критерия поставим в соответствии определенный класс или семейство ФТБ.

Функциональные требования сгруппированы на основе выполняемой ими роли или обслуживаемой цели безопасности. Всего 11 функциональных классов (в трёх группах), 66 семейств, 135 компонентов.

1. Первая группа определяет элементарные сервисы безопасности:
    1. FAU — аудит, безопасность (требования к сервису, протоколирование и аудит);
    2. FIA — идентификация и аутентификация;
    3. FRU – использование ресурсов (для обеспечения отказоустойчивости).
2. Вторая группа описывает производные сервисы, реализованные на базе элементарных:
    1. FCO — связь (безопасность коммуникаций отправитель-получатель);
    2. FPR — приватность;
    3. FDP — защита данных пользователя;
    4. FPT — защита функций безопасности объекта оценки.
3. Третья группа классов связана с инфраструктурой объекта оценки:
    1. FCS — криптографическая поддержка (обслуживает управление криптоключами и крипто-операциями);

2. FMT — управление безопасностью;
3. FTA — доступ к объекту оценки (управление сеансами работы пользователей);
4. FTP — доверенный маршрут/канал.

В качестве ОО рассматривается беспроводная сеть в целом, а не отдельные рабочие места с интегрированными беспроводными сетевыми адаптерами.

Рассмотрим первую группу критериев. Во второй части ГОСТ Р ИСО/МЭК 15408 этой группе 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. Класс FCS применяют, когда ОО имеет криптографические функции, которые могут быть реализованы аппаратными, программно-аппаратными и/или программными средствами.

Класс FCS состоит из двух семейств: FCS_CKM "Управление криптографическими ключами" и FCS_COP "Криптографические операции". В семействе FCS_CKM рассмотрены аспекты управления криптографическими ключами, тогда как в семействе FCS_COP рассмотрено практическое применение этих криптографических ключей.

Семейство FCS_CKM предназначено для поддержки жизненного цикла и поэтому определяет требования к следующим действиям с криптографическими ключами: генерация, распределение, доступ к ним и их уничтожение. Это семейство следует использовать в случаях, когда имеются функциональные требования управления криптографическими ключами.

Компонент FCS_CKM.1 содержит требования по определению длины криптографических ключей и метода их генерации, что может быть сделано в соответствии с некоторыми принятыми стандартами. Его следует

использовать для определения длины криптографических ключей и метода (т.е. алгоритма) их генерации.

Этому компоненту соответствует критерий длина ключа (1.2), используемый для зашифрования передаваемой информации по каналам БС.

Компонент FCS_CKM.2 содержит требование определения метода распределения ключей, который может соответствовать некоторому принятому стандарту.

В FCS_CKM.2.1 следует определить, какой метод используется для распределения криптографических ключей: динамическое и статистическое распределение ключей, т.е. критерий 1.3.

У криптографической операции может быть один или несколько криптографических режимов операции, ассоциированных с ней. В этом случае их необходимо определить. Примерами криптографических режимов операций являются сцепление блоков зашифрованного текста, осуществление обратной связи по выходу, применение электронной книги кодов и осуществление обратной связи по зашифрованному тексту.

Криптографические операции могут использоваться для поддержки одной или нескольких функций безопасности ОО.

В компоненте FCS_COP.1 содержатся требования указания криптографических алгоритмов и длины ключей, используемых при выполнении определяемых криптографических операций и основанных на некотором принятом стандарте.

В FCS_COP.1.1 следует определить выполняемые криптографические операции. Типичными криптографическими операциями являются генерация и/или верификация цифровых подписей, генерация криптографических контрольных сумм для обеспечения целостности и/или верификации контрольных сумм, безопасное хэширование (вычисление хэш-образа сообщения), зашифрование и/или расшифрование данных, зашифрование и/или расшифрование криптографических ключей, согласование криптографических ключей и генерация случайных чисел. Данному

компоненту можно поставить в соответствие такой криптографический критерий как технология проверки целостности сообщений.

В FCS_COP.1.1 следует определить, какой криптографический алгоритм будет использован: AES либо WEP.

Таким образом, семейство FCS_COP.1.1 включает в себя все оставшиеся критерии – 1.1 и 1.4.

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

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

Любые протоколы аутентификации, используемые в БС можно описать с использованием компонентов этого семейства, поэтому критерию протокол из группы критериев аутентификации противопоставляется сразу же все семейство FIA_UAU. Но несмотря на это, все же рассмотрим компоненты, входящие в него, чтобы понять, все ли они имеют значения при оценке БС.

Компонент FIA_UAU определяет список действий, которые выполняются при посредничестве ФБО и допускаются ФБО от имени пользователя до того, как будет произведена аутентификация пользователя. Эти действия, выполняемые при посредничестве ФБО, не следует относить к безопасности для пользователей, неверно идентифицировавших себя еще до аутентификации. Все прочие действия, выполняемые при посредничестве ФБО и не включенные в этот список, разрешаются пользователю только после завершения аутентификации.

В FIA_UAU.1.1 следует специфицировать список действий, выполняемых при посредничестве ФБО от имени пользователя прежде, чем завершится аутентификация пользователя. Этот компонент особенно актуален при аутентификации с открытым ключом, когда как таковая аутентификация по сути отсутствует.

Компонент FIA_UAU.2 содержит требование завершения аутентификации пользователя до выполнения любых действий при посредничестве ФБО от имени этого пользователя.

Компонент FIA_UAU.3 содержит требования к механизмам, предоставляющим защиту аутентификационных данных. Аутентификационные данные, заимствованные у другого пользователя или полученные незаконным способом, следует обнаружить и/или отвергнуть. Эти механизмы предоставляют уверенность, что пользователи, аутентифицированные ФБО, действительно те, кем они представляются.

Компонент FIA_UAU.4 содержит требования к механизмам аутентификации, основанным на аутентификационных данных одноразового использования. В качестве таких данных может использоваться то, что пользователь имеет или знает, но не свойства самого пользователя. Примеры одноразовых данных аутентификации пользователя: одноразовые пароли, зашифрованные метки времени, случайные числа секретной таблицы преобразований.

В FIA_UAU.4.1 следует привести список механизмов аутентификации, к которым применяется это требование.

Применение компонента FIA_UAU.5 позволяет специфицировать требования к применению нескольких механизмов аутентификации в ОО. Требования, применяемые к каждому отдельному механизму, необходимо выбирать из класса FIA. Чтобы отразить различающиеся требования к разным механизмам аутентификации, можно многократно использовать один и тот же выбранный компонент.

В FIA_UAU.5.1 следует определить предоставляемые механизмы аутентификации. В FIA_UAU.5.2 следует специфицировать правила, описывающие, как механизмы обеспечивают аутентификацию, и когда используется каждый из них. Это значит, что для любой возможной ситуации необходимо указать совокупность механизмов, которые могли бы использоваться для аутентификации.

В компоненте FIA_UAU.6 рассматривается потенциальная потребность повторной аутентификации пользователей в определенные моменты времени. Это может возникнуть при обращении пользователя к ФБО с запросом о выполнении действий, критичных по безопасности, а также при запросах о повторной аутентификации, исходящих от сущностей, не связанных с ФБО, например, от серверного приложения, которое запрашивает от ФБО повторную аутентификацию обслуживаемого клиента.

В компоненте FIA_UAU.7 рассматривается обратная связь с пользователем в процессе аутентификации. В некоторых системах обратная связь выражается в том, что пользователю сообщается количество набранных им символов, но сами символы скрываются, в других системах даже эта информация может считаться неприемлемой.

Этот компонент содержит требование, чтобы аутентификационные данные не возвращались пользователю в первоначальном виде.

Исходя из рассмотренных выше компонентов семейства FIA_UAU, видно, что любой протокол аутентификации, используемый в БС можно оценить с их помощью.

Семейство FIA_SOS определяет требования к механизмам, которые реализуют определенную метрику качества для предоставляемых секретов и генерируют секреты, удовлетворяющие определенной метрике. Примерами таких механизмов могут быть автоматическая проверка предоставляемых пользователями паролей или автоматическая генерация паролей.

Секреты могут генерироваться вне ОО, например, выбираться пользователями и вводиться в систему. При этом может быть использован компонент FIA_SOS.1 для обеспечения соответствия секретов, сгенерированных вне системы, конкретным условиям, таким как минимально допустимый размер и/или неприменение ранее.

Секреты могут генерироваться самим ОО. В этом случае требование, чтобы сгенерированные ОО секреты соответствовали специфицированной метрике, обеспечивается компонентом FIA_SOS.2.

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. Оно обеспечивает, чтобы две распределенные части ОО синхронизировали свои состояния после действий, связанных с безопасностью.

Компонент FPT_SSP.2 содержит требование, что в дополнение к предоставлению подтверждения получения передаваемых данных принимающей части ФБО необходимо обратиться к передающей части за уведомлением о получении подтверждения.

Например, локальная часть ФБО передает данные удаленной части ФБО. Последняя подтверждает успешный прием сообщения и запрашивает у передавшей сообщение части ФБО уведомление, что она получила подтверждение. Этот механизм дает дополнительную уверенность, что обе части ФБО, участвующие в передаче данных, извещены об успешном завершении передачи.

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).

Компонент FDP_DAU.1 может быть реализован с помощью односторонних хэш-функций (криптографической контрольной суммы, отображения отпечатков пальцев, хэш-образа сообщения) для генерации хэш-значения определяемого документа, которое может использоваться при верификации правильности или подлинности содержащейся в нем информации.

Суммируя все вышесказанное, получаем соответствие критериев для оценки защищенности БС ФТБ ГОСТ Р ИСО/МЭК 15408. Результаты представлены в таблице 2.3.

Табл. 2.3 Соответствие критериев 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 |

Используя полученные данные можно значительно упростить процесс как построения семейства ПЗ, так и построения непосредственного ПЗ на этапе сопоставления реализованных в сети механизмов защиты информации с ФТБ ГОСТ Р ИСО/МЭК 15408.

# ГЛАВА 3. МЕТОД ОПРЕДЕЛЕНИЯ УРОВНЯ ДОВЕРИЯ К БЕСПРОВОДНОЙ СЕТИ НА ОСНОВЕ РЕАЛИЗОВАННЫХ В НЕЙ МЕХАНИЗМОВ ЗАЩИТЫ ИНФОРМАЦИИ

## 3.1 Построение системы уровней доверия для беспроводной сети

Требования доверия безопасности составляют содержание третьей части ГОСТ Р ИСО/МЭК 15408.

Доверие в трактовке "Общих критериев" - это основа для уверенности в том, что изделие ИТ отвечает целям безопасности. Доверие обеспечивается через активное исследование (оценку) изделия ИТ [15].

Требования доверия безопасности охватывают весь жизненный цикл изделий ИТ и предполагают выполнение следующих действий:

- оцениваются ЗБ и ПЗ, ставшие источниками требований безопасности;
- анализируются различные представления проекта ОО и соответствие между ними, а также соответствие каждого из них требованиям безопасности;
- проверяются процессы и процедуры безопасности, их применение;
- анализируется документация;
- верифицируются представленные доказательства;
- анализируются тесты и их результаты;
- анализируются уязвимости ОО;
- проводится независимое тестирование, в том числе тестовые "взломы".

В соответствии с «Общими критериями» оценочный уровень доверия определяется как пакет компонентов доверия из третьей части ОК, представляющий некоторое положение на предопределенной в ОК шкале доверия.

В "Общих критериях" определено семь упорядоченных по возрастанию оценочных уровней доверия (ОУД) безопасности, содержащих рассчитанные на многократное применение комбинации требований доверия (не более одного компонента из каждого семейства). Наличие такой шкалы дает возможность сбалансировать получаемый уровень доверия со сложностью, сроками, стоимостью и самой возможностью его достижения.

Предполагается, что в ПЗ и ЗБ будут фигурировать или сами оценочные уровни, или их усиления, полученные путем расширения требований (за счет добавления к ОУД новых компонентов) либо увеличения строгости и/или глубины оценки (посредством замены компонентов более сильным вариантом из того же семейства). Таким образом, ОУД играют роль опорных точек в многомерном пространстве требований доверия.

Оценочный уровень доверия 1 (ОУД1), предусматривающий функциональное тестирование, применяется, когда требуется некоторая уверенность, что ОО работает безукоризненно, а угрозы безопасности не считаются серьезными. Его можно достичь без помощи разработчика и с минимальными затратами посредством анализа функциональной спецификации, спецификации интерфейсов, эксплуатационной документации в сочетании с независимым тестированием.

Оценочный уровень доверия 2 (ОУД2) предусматривает структурное тестирование и доступ к части проектной документации и результатам тестирования разработчиком. ОУД2 применим, когда разработчикам или пользователям требуется независимо получаемый умеренный уровень доверия при отсутствии доступа к полной документации по разработке.

В дополнение к ОУД1 предписывается анализ проекта верхнего уровня. Анализ должен быть поддержан независимым тестированием функций безопасности, актом разработчика об испытаниях, основанных на функциональной спецификации, выборочным независимым подтверждением результатов тестирования разработчиком, анализом стойкости функций и свидетельством поиска явных уязвимостей. Требуется наличие списка

конфигурации ОО с уникальной идентификацией элементов конфигурации и свидетельства безопасных процедур поставки.

Оценочный уровень доверия 3 (ОУД3), предусматривающий систематическое тестирование и проверку, позволяет достичь максимально возможного доверия при использовании обычных методов разработки. Он применим в тех случаях, когда разработчикам или пользователям требуется умеренный уровень доверия на основе всестороннего исследования ОО и процесса его разработки.

По сравнению с ОУД2 на данном уровне добавлено требование, которое предписывает разработчику создавать акт об испытаниях с учетом особенностей не только функциональной спецификации, но и проекта верхнего уровня. Кроме того, требуется контроль среды разработки и управление конфигурацией ОО.

Оценочный уровень доверия 4 (ОУД4) предусматривает систематическое проектирование, тестирование и просмотр. Он позволяет достичь доверия, максимально возможного при следовании общепринятой практике коммерческой разработки. Это самый высокий уровень, на который, вероятно, экономически целесообразно ориентироваться для существующих типов продуктов.

ОУД4 характеризуется анализом функциональной спецификации, полной спецификации интерфейсов, эксплуатационной документации, проектов верхнего и нижнего уровней, а также подмножества реализации, применением неформальной модели политики безопасности ОО. Среди других дополнительных требований - независимый анализ уязвимостей, демонстрирующий устойчивость к попыткам проникновения нарушителей с низким потенциалом нападения, и автоматизация управления конфигурацией.

Отличительные особенности оценочного уровня доверия 5 (ОУД5) - полуформальное проектирование и тестирование. С его помощью достигается доверие, максимально возможное при следовании строгой

практике коммерческой разработки, поддержанной умеренным применением специализированных методов обеспечения безопасности. ОУД5 востребован, когда нужен высокий уровень доверия и строгий подход к разработке, не влекущий излишних затрат.

Для достижения ОУД5 требуется формальная модель политики безопасности ОО и полуформальное представление функциональной спецификации и проекта верхнего уровня, полуформальная демонстрация соответствия между ними, а также модульная структура проекта ОО. Акт об испытаниях должен быть основан еще и на проекте нижнего уровня. Необходима устойчивость к попыткам проникновения нарушителей с умеренным потенциалом нападения. Предусматривается проверка правильности анализа разработчиком скрытых каналов и всестороннее управление конфигурацией.

Оценочный уровень доверия 6 (ОУД6) характеризуется полуформальной верификацией проекта. Он позволяет получить высокое доверие путем применения специальных методов проектирования в строго контролируемой среде разработки при производстве высококачественных изделий ИТ и при защите ценных активов от значительных рисков.

Особенности ОУД6 заключаются в следующем:

- структурированное представление реализации;
- полуформальное представление проекта нижнего уровня;
- иерархическая структура проекта ОО;
- устойчивость к попыткам проникновения нарушителей с высоким потенциалом нападения;
- проверка правильности систематического анализа разработчиком скрытых каналов;
- использование структурированного процесса разработки;
- полная автоматизация управления конфигурацией ОО.

Оценочный уровень доверия 7 (ОУД7), предусматривающий формальную верификацию проекта, применим к разработке изделий ИТ для

использования в ситуациях чрезвычайно высокого риска или там, где высокая ценность активов оправдывает повышенные затраты.

На седьмом уровне дополнительно требуются:

- формальное представление функциональной спецификации и проекта верхнего уровня и формальная демонстрация соответствия между ними;
- модульная, иерархическая и простая структура проекта ОО;
- добавление представления реализации как основы акта об испытаниях;
- полное независимое подтверждение результатов тестирования разработчиком.

После проведения анализа защищенности беспроводной сети в соответствии с ранее выработанными критериями, представляется возможным определить минимальный уровень доверия к данному объекту оценки, исходя из совокупности оценок средств защиты, которые используется для обеспечения безопасности в ней.

Для оценки защищенности БС вводится пять уровней доверия (УД) к ОО по аналогии с ОУД, описанными в третьей части ГОСТ Р ИСО/МЭК 15408. Причем пятый уровень будет отражать требования к наиболее защищенному ОО, в то время как первый – напротив, к наименее.

Данные УД могут присваиваться сети после проведения анализа по критериям оценки защищенности.

Уровень доверия к беспроводной сети определяется минимальным значением веса, который был получен при анализе. Таким образом, если по всем критериям для данного ОО значение весов равно 4, в то время как лишь по одному – 2, то общий уровень доверия тоже будет равен 2.

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 средства защиты информации 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 механизмы защиты 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.

## 3.2 Исследование логических связей в структуре механизмов защиты

Для ранжирования механизмов защиты беспроводной сети по выработанным уровням доверия необходимо проанализировать семейство стандартов 802.11 по критериям оценки защищенности, полученным во второй главе. В результате анализа предполагается получить полный структурированный набор механизмов защиты, которые описываются стандартах для БС.

Первоначально исследуем механизмы защиты, призванные обезопасить сеть с точки зрения защиты передаваемых данных. Для этих целей проанализируем семейство стандартов с помощью криптографических критериев.

Основополагающим механизмов в этой сфере является криптографический алгоритм, используемый для шифрования передаваемого трафика.

На заре становления беспроводных технологий этим целям удовлетворял алгоритм WEP, используемый совместно с 40-битным разделяемым ключом. Позже для усиления его криптостойкости стали использовать уже 128-битный ключ, в то время как сам алгоритм остался прежним.

В стандарте 802.11i вводится новый алгоритм AES, который обладает значительно большей криптостойкостью по сравнению с предшественником. Но усиление защитных свойств алгоритма приводит к значительному увеличению ресурсоемкости оборудования для развертывания БС. Именно поэтому на первых этапах внедрения алгоритм AES также применяется с со 128-битным ключом. Но в стандарте сразу же закладывается возможность последующего расширения, и алгоритм AES можно использовать как со 192-битным ключом, так и со 256-битным.

Возможность изменения ключа на протяжении сеанса связи тоже была введена не сразу. Когда БС только начали появляться на рынке сетевых технологий, статистический ключ вполне удовлетворял поставленным целям безопасности. Но пропорционально росту популярности беспроводной связи увеличиваются и требования конечных пользователей к уровню безопасности, который могут обеспечить подобные соединения. Наравне с увеличением длины ключа применяется методика его периодической смены, ключ становится динамическим.

Для проверки целостности передаваемых сообщений в стандартах семейства 802.11 описываются два протокола: MIC и CCMP.

Таким образом, был получен полный набор механизмов защиты БС в соответствии с криптографическими критериями. Представим его в наглядном виде с учетом существующих логических связей (рис. 3.1). Причем сплошная линия указывает на обязательность использования механизмов защиты совместно, в то время как пунктирная – на возможность их совместного применения.

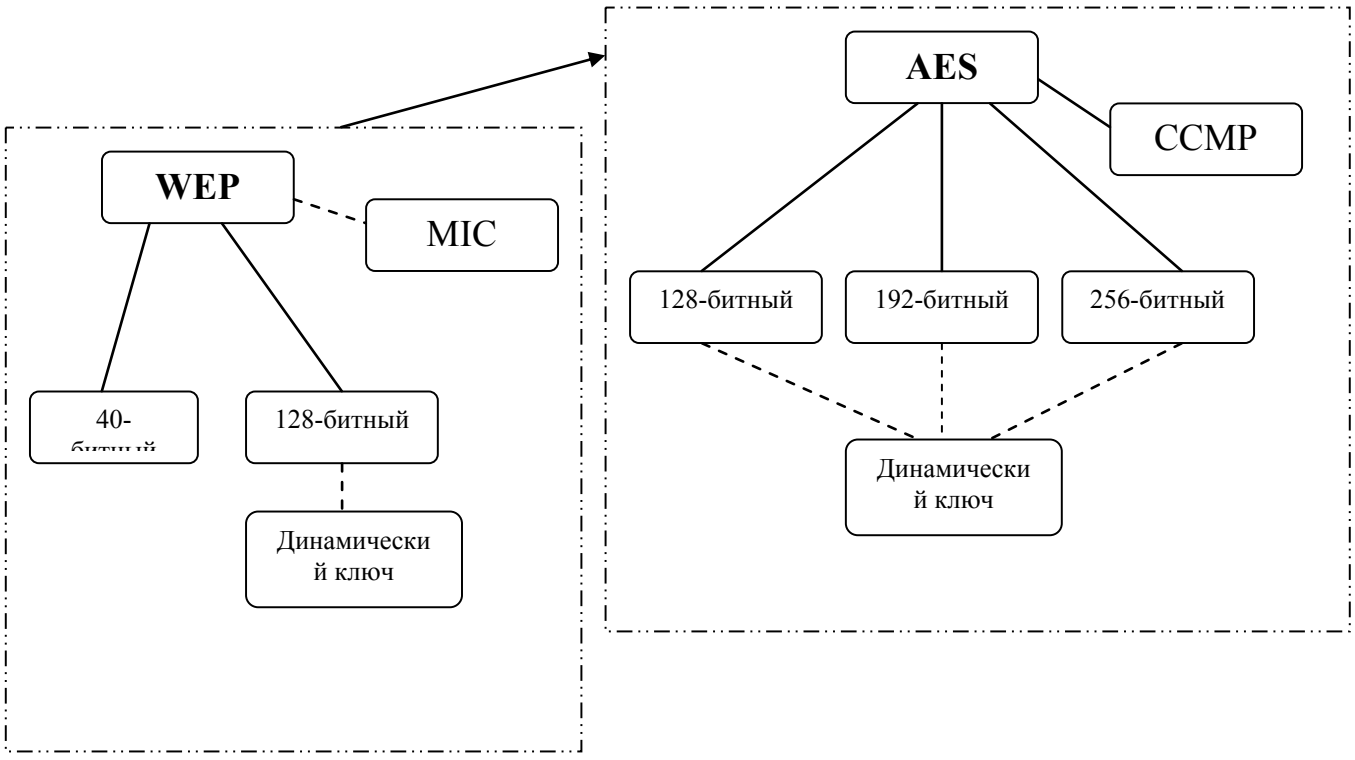


Рис. 3.1 Логическая структура криптографических механизмов защиты беспроводной сети

Обобщив данные по всем возможным реализациям криптографических механизмов защиты в БС, получаем следующее (табл. 3.1 и табл. 3.2):

Табл. 3.1 Сочетания криптографических механизмов защиты при использовании алгоритма WEP

| | | WEP-40 | WEP-128 |
|---|---|---|---|
| Статистический ключ | Есть проверка целостности | | + |
| | Нет проверки целостности | + | + |
| Динамический ключ | Есть проверка целостности | | + |
| | Нет проверки целостности | | + |

Итого получаем 5 возможных вариантов.

Табл. 3.2 Сочетания криптографических механизмов защиты при использовании алгоритма AES

| | | AES-128 | AES-192 | AES-256 |
|---|---|---|---|---|
| Статистический ключ | Есть проверка целостности | + | + | + |
| | Нет проверки целостности | + | + | + |
| Динамический ключ | Есть проверка целостности | + | + | + |
| | Нет проверки целостности | + | + | + |

Итого получаем 12 возможных вариантов.

Теперь исследуем механизмы защиты, направленные на контроль доступа к БС. При анализе семейства стандартов 802.11 воспользуемся полученными критериями аутентификации.

Если с точки зрения криптографической защиты данных алгоритм шифрования является основополагающим критерием, то с точки зрения защиты доступа к сетевым ресурсам основным критерием для оценки является протокол аутентификации, реализованный в ОО. В данной сфере тоже довольно-таки ярко прослеживается поступательная динамика усиления защитных свойств протокола с развитием беспроводных технологий.

На ранних этапах использовались примитивные схемы аутентификации, как то: аутентификация с открытым либо общим ключом. Первая, как уже упоминалось выше, по сути, не является как таковым алгоритмом аутентификации, а вторая - лишь незначительно усиливает первую за счет шифрования передаваемой служебной информации.

Полноценные протоколы аутентификации появляются позднее, после того, как было найдено и обосновано несоответствие возможностей WEP постоянно расширяющемуся кругу задач БС.

Разрабатывается семейство протоколов EAP. Его многообразие объясняется тем, что производители беспроводного оборудования внедряли свою версию протокола в зависимости от своего видения будущего развития беспроводных технологий. На сегодняшний день используется пять основных протоколов данного семейства, каждый из которых усиливает свойства предыдущего: EAP-MD5, LEAP, EAP-TLS, PEAP, EAP-TTLS.

Но защита беспроводной связи не ограничивается лишь схемой аутентификации пользователя в сети. Для достижения более высоких показателей в этой области вводятся дополнительные механизмы защиты.

Начиная с реализации протокола LEAP, в структуру решения по обеспечению защиты от НСД вводят сервер аутентификации, который обеспечивает дополнительные возможности разграничения прав

пользователя при работе в сети. Причем возможно два варианта его применения: с односторонней и взаимной аутентификацией.

Также в качестве дополнительных механизмов защиты можно рассматривать и использование цифровых сертификатов (начиная с реализации протокола EAP-TLS) для верификации предоставленной пользователем информации. Стоит отметить, что при реализации протокола EAP-TLS использование цифровых сертификатов является обязательным условием, в то время как в последующих протоколах семейства EAP – лишь дополнительной опцией.

Объединив полученные механизмы защиты БС в области контроля доступа, представим в наглядном виде логические связи между ними (рис. 3.2).

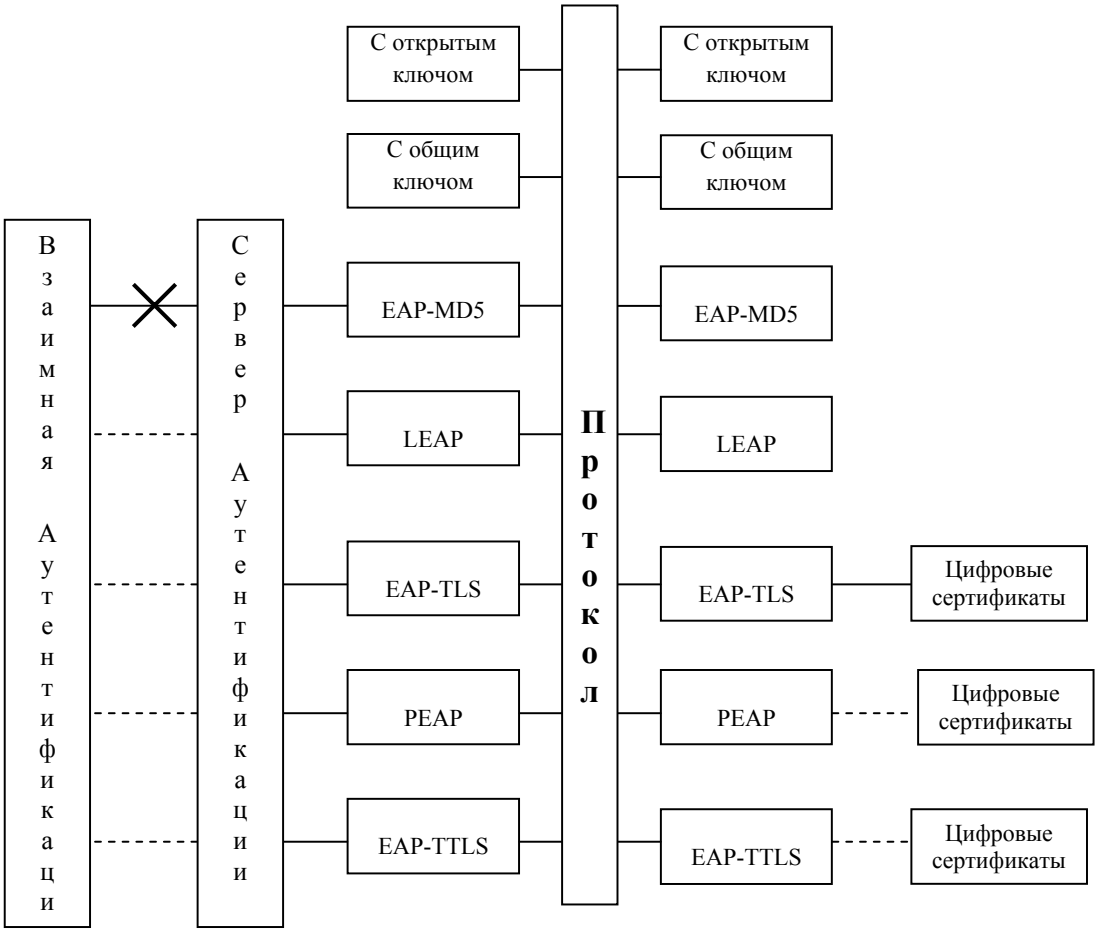


Рис. 3.2 Логическая структура механизмов аутентификации беспроводной сети

Также как и при построении логической структуры криптографических механизмов защиты, сплошная линия обозначает обязательность совместного применения механизмов, в то время как пунктирная – лишь возможность.

По аналогии с криптографическими средствами защиты информации составим сводную таблицу всех возможных наборов механизмов защиты, направленных на контроль доступа к сети (табл. 3.3).

Табл. 3.3 Сочетания механизмов защиты на этапе аутентификации

| **Протокол аутентификации** | **Сервер аутентификации** | | **Цифровые сертификаты** |
|---|---|---|---|
| | Отсутствует | Взаимная аутентификация | |
| С открытым ключом | - | | - |
| С общим ключом | - | | - |
| EAP-MD5 | | - | - |
| LEAP | | +/- | - |
| EAP-TLS | | +/- | + |
| PEAP | | +/- | +/- |
| EAP-TTLS | | +/- | +/- |

Итого получается 15 возможных вариантов реализации.

Подводя итог всему вышесказанному, построим общую структуру классифицированных средств защиты информации беспроводной сети в соответствии с выработанными критериями защищенности (рис. 3.3).

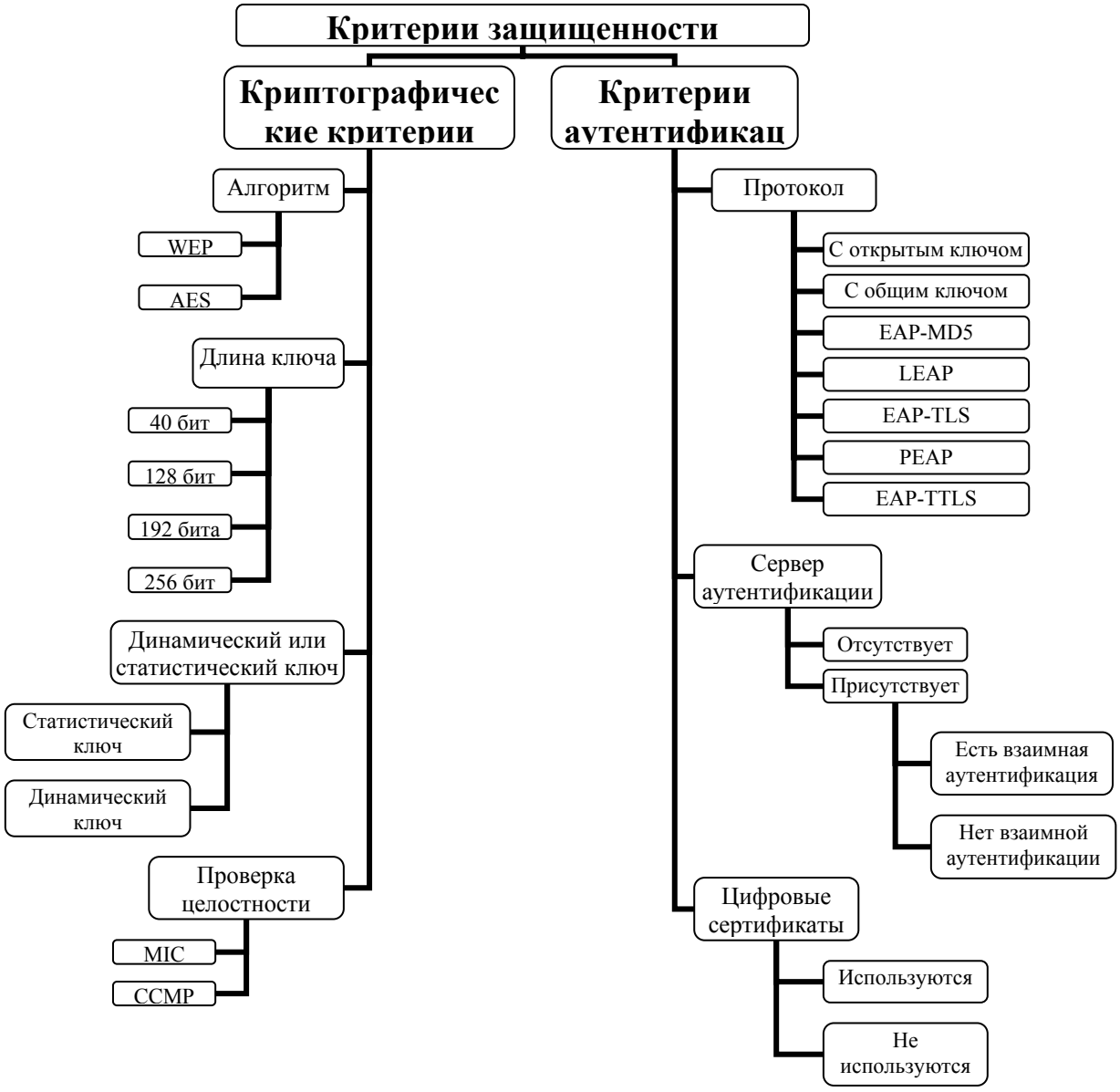


Рис. 3.3 Классификация механизмов защиты информации беспроводной сети

Таким образом, в части криптографической оценки защищенности сети мы имеем 17 возможных совокупных реализаций механизмов защиты информации, в то время как в части аутентификации - 15.

## 3.3 Ранжирование механизмов защиты по уровням доверия

Первоначально рассмотрим группу криптографических критериев.

При построении сети на базе беспроводных технологий могут быть использованы лишь два стандарта шифрования: WEP и AES. При использовании алгоритма WEP для шифрования передаваемой по каналам связи информации ОО может принадлежать только к 1 либо 2 уровню. Это связано с общеизвестными уязвимостями данного стандарта.

Использование ОО шифрования по средствам AES автоматически переводит его на 3 либо 4 УД.

Все последующие криптографические механизмы защиты находятся в прямой зависимости от использованного стандарта шифрования (WEP или AES), поэтому целесообразно все дальнейшие возможные варианты конфигурации сети рассматривать, отталкиваясь от этого первоначального критерия.

При использовании WEP УД к сети не может превышать второго, это связано с его низкой криптостойкостью и наличием большого числа уязвимостей. При шифровании передаваемой информации по средствам RC-4 используют длину ключа равную либо 40 либо 128 битам.

Самым незащищенным считается соединение, при установлении которого используется алгоритм WEP с 40-битным ключом (WEP-40), так как подобные схемы использовали еще на заре развития беспроводных технологий. При такой длине ключа возможен лишь один неизменяющийся ключ на протяжении всего сеанса связи (статистический). Также в то время еще никакой и речи не было о проверки целостности передаваемой информации. Таким образом, при использовании WEP-40 возможна только одна конфигурация сети, причем явно видно, что УД к ней будет минимальным, т.е равным первому.

С развитием стандарта 802.11 разработчики стали искать пути увеличения информационной безопасности сети, в связи с этим было введено

использование более длинного ключа в 128 бит (WEP-128). При его использовании стало возможным применение динамических ключей. Также было внедрено использование протокола MIC для проверки целостности сообщений.

Эти варианты являются однозначно более защищенным и ОО, в которых реализованы подобные механизмы защиты, уже можно отнести ко второму УД.

Но здесь бы хотелось отметить тот факт, что хотя с появлением WEP-128 взамен WEP-40 уровень безопасности возрос, но в то же время использование статистического ключа без проверки целостности сообщений не дает нам полной уверенности, что данная сеть может принадлежать к УД2, поэтому целесообразно данную конфигурацию используемых средств защиты информации отнести к УД1.

Теперь в свою очередь рассмотрим стандарт шифрования AES. Он оперирует длиной ключа 128, 192 или 256 бит – название стандартов соответственно AES-128, AES-192 либо AES-256.

Как можно увидеть из таблицы 3.2, при шифровании информации в сети по средствам AES мы имеем 12 возможных вариантов сочетаний механизмов защиты в БС.

При использовании AES-256 сеть «автоматически» находится на четвертом УД, так как этот алгоритм является на сегодняшний день наиболее криптостойким из тех, которые применяются в БС. Использование же AES-128 либо AES_192 относит исследуемый ОО на третий либо четвертый уровни соответственно, за исключением тех случаев, когда ключ на протяжении сеанса связи остается неизменным и отсутствует проверка целостности сообщений (CCMP). В таком случае ОО можно отнести только либо на второй либо на третий уровни соответственно.

Подводя итог вышесказанному, представим полученные результаты в таблицах 3.4 и 3.5.

Табл. 3.4 Ранжирование совокупностей криптографических механизмов защиты по УД при использовании алгоритма WEP

| | | **WEP-40** | **WEP-128** |
|---|---|---|---|
| Статистический ключ | Есть проверка целостности | | 2 |
| | Нет проверки целостности | 1 | 1 |
| Динамический ключ | Есть проверка целостности | | 2 |
| | Нет проверки целостности | | 2 |

Табл. 3.5 Ранжирование совокупностей криптографических механизмов защиты по УД при использовании алгоритма AES

| | | **AES-128** | **AES-192** | **AES-256** |
|---|---|---|---|---|
| Статистический ключ | Есть проверка целостности | 3 | 4 | 4 |
| | Нет проверки целостности | 2 | 3 | 4 |
| Динамический ключ | Есть проверка целостности | 3 | 4 | 4 |
| | Нет проверки целостности | 3 | 4 | 4 |

Перейдем ко второй группе критериев – критериям аутентификации. Обобщив знания в области семейства стандартов 802.11, мы получаем 15 возможных схем реализации аутентификации пользователей в сети (табл. 3.3). Проранжируем их по разработанной системе УД (табл.3.6).

Табл. 3.6 Ранжирование совокупностей механизмов защиты на этапе аутентификации

| № | Конфигурация | УД |
|---|---|---|
| 1 | Аутентификация с открытым ключом | 1 |
| 2 | Аутентификация с общим ключом | 1 |
| 3 | EAP-MD5-ВА-ЦС | 2 |
| 4 | LEAP-ВА | 2 |
| 5 | LEAP+ВА | 2 |
| 6 | EAP-TLS-ВА+ЦС | 3 |
| 7 | EAP-TLS+ВА+ЦС | 3 |
| 8 | PEAP-ВА-ЦС | 3 |
| 9 | PEAP-ВА+ЦС | 3 |
| 10 | PEAP+ВА-ЦС | 3 |
| 11 | PEAP+ВА+ЦС | 4 |
| 12 | EAP-TTLS-ВА-ЦС | 4 |
| 13 | EAP-TTLS-ВА+ЦС | 4 |
| 14 | EAP-TTLS+ВА-ЦС | 4 |
| 15 | EAP-TTLS+ВА+ЦС | 4 |

Открытая аутентификация не позволяет АР определить, является ли абонент легитимным или нет. При реализации в сети только аутентификации с открытым ключом УД к ней не может быть больше первого.

Аутентификация с общим ключом является вторым методом аутентификации стандарта IEEE 802.11. Аутентификация с общим ключом требует настройки у абонента статического ключа шифрования WEP.

Подобная методика аутентификации не может значительно увеличить защищенность беспроводного соединения, поэтому УД тоже будет равен первому, как и в случае с аутентификацией по открытому ключу.

Следующим шагом для усиления механизмов аутентификации в БС стало внедрение протокола EAP. Сразу стоит отметить, что при использовании протокола EAP в сети всегда используется сервер аутентификации.

EAP-MD5 был первым протоколом, реализованным в рамках семейства EAP. Уровень обеспечиваемой им защищенности в процессе получения доступа к сетевым ресурсам несравненно выше по сравнению с предыдущими протоколами аутентификации. Но если рассматривать его с точки зрения протоколов семейства, то при реализации аутентификации по средствам EAP-MD5, УД к БС не может превышать второго.

Протокол LEAP находится на ступень выше в иерархии протоколов семейства EAP, но в связи с его уязвимостью к атакам по словарю, УД при его использовании также может быть равен только второму.

Более сильный вариант реализации EAP — EAP-TLS, который использует предустановленные цифровые сертификаты X.509 на клиенте и сервере. Их использование сразу дает возможность причислить сети, где используется протокол EAP-TLS к третьему УД.

PEAP использует сертификат, установленный на сервере, и аутентификацию по паролю для клиентов.

EAP-TTLS использует безопасное соединение, установленное в результате TLS-квитирования для обмена дополнительной информацией между пользователем и сервером аутентификации.

Применение этих протоколов дает возможность присвоить сети 3 либо 4 УД соответственно. Но отдельно бы хотелось оговорить вариант, когда используется протокол PEAP с взаимной аутентификацией и цифровыми сертификатами. Подобная совокупность механизмов защиты является довольно-таки стойкой и ее в полной мере можно отнести к УД4.

Суммируя все вышесказанное, объединим полученные данные в таблицу 3.7.

Табл. 3.7 Ранжирование механизмов защиты беспроводной сети по уровням доверия

| **УД** | **Критерии** | **Механизмы защиты** |
|---|---|---|
| 1 | Криптографические | WEP-40 |
| | | WEP-128 + СК - ПЦ |
| | Аутентификации | Аутентификация с открытым ключом |
| | | Аутентификация с общим ключом |
| 2 | Криптографические | WEP-128 + СК + ПЦ |
| | | WEP-128 + ДК - ПЦ |
| | | WEP-128 + ДК+ ПЦ |
| | | AES-128 + СК - ПЦ |
| | Аутентификации | EAP-MD5 |
| | | 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 |

Продолжение табл. 3.7

| УД | Критерии | Механизмы защиты |
|---|---|---|
| 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 |

Также хотелось бы оговорить такую реализацию средств защиты информации в БС, когда вводятся дополнительные протоколы либо механизмы защиты, которые противодействуют какому-либо одному виду угроз или атак. Примером могут послужить wormhole (действующие по принципу червя) атаки, которые представляют серьезную угрозу для беспроводных сетей.

Суть данного вида атак заключается в том, что атакующая сторона прослушивает весь трафик сети, записывает его и передает по виртуальному каналу узлу-соучастнику, расположенному на достаточном отдалении, который уже непосредственно передает информацию в сеть. Причем передаваться может не полностью весь трафик, а отдельные пакеты или даже отдельные биты этого пакета. Это чрезвычайно негативно сказывается на протоколах маршрутизации, которые используются в сети, потому что становится практически невозможно построить правильные маршруты

между узлами, находящимися на расстоянии более одного либо двух «прыжков».

Для нахождения и предотвращения подобных атак в сети существует достаточно различных методик, как аппаратных (использование направленных антенн), так и программных (использование протоколов аутентификации, например TrueLink) [25].

Если в ходе проведения анализа защищенности БС выясняется, что она удовлетворяет четвертому УД, но в то ж е время в ней реализовано дополнительные механизмы защиты, то подобную сеть можно смело отнести к пятому уровню доверия.

Как уже упоминалось, разработанная система УД для определения защищенности БС основываются на ОУД ГОСТ Р ИСО/МЭК 15408. В этом документы существует семь ОУД, образующих возрастающую шкалу. Для оценки же защищенности БС используется только 4 УД и один дополнительный пятый уровень доверия.

ОУД6 используется с целью получения высококачественного ОО для защиты высоко оцениваемых активов от значительных рисков, что не ставилось в задачи в рамках данной работы, так как ситуации высокого риска приравниваются к защите государственной тайны.

ОУД7 же непосредственно рассчитана на оценку средств защиты информации, в то время как представляемая модель в качестве ОО рассматривает всю БС в комплексе [39].

Таким образом, чтобы теперь перейти к построению семейства профилей защиты проведем соответствие между ОУД и УД (табл. 3.8).

Табл. 3.8 Сопоставление ОУД и УД к БС

| **ОУД** | **Признак** | **УД** | **Признак** |
|---|---|---|---|
| 1 | Угрозы безопасности не рассматриваются как серьезные | 1 | Минимально возможный уровень безопасности |

Продолжение табл. 3.8

| ОУД | Признак | УД | Признак |
|---|---|---|---|
| 2 | Отсутствие доступа к полной документации по разработке | 2 | Усиление «старых» механизмов и алгоритмов новыми компонентами |
| 3 | Всестороннее исследование ОО, без существенных затрат на изменение технологии проектирования | 3 | Использование более надежного нового поколения механизмов и алгоритмов |
| 4 | Готовность нести дополнительные производственные затраты | 4 | Максимально возможный уровень безопасности |
| 5 | Для запланированной разработки | 5 | Введение дополнительных СЗИ, выходящих за рамки стандартов 802.11 |
| 6 | Модель соотношения затрат на СЗИ и ущерба в случае реализации рисков (угроз) | - | - |
| 7 | СЗИ | - | - |

## 3.4 Построение семейства базовых функциональных пакетов для беспроводной сети

Используя полученные данные о соответствии критериев оценки защищенности ФТБ (табл. 2.3), противопоставим каждому механизму защиты информации в БС соответствующий ему компонент ФТБ. Также как и при построении системы критериев оценки проведем исследование отдельно для криптографических механизмов и механизмов аутентификации.

В случае с криптографическими составляющими системы защиты БС взаимодействие происходит со строго регламентированным набором компонент семейств ФТБ. Это выражается в том, что для всех УД кроме первого совокупность требований безопасности будет одинаковой. УД1, как уже упоминалось выше, отличается от других уровней минимальной обеспечиваемой степенью защиты передаваемых данных, поэтому компонент FCS_CKM.2.1 не является обязательным (табл. 3.9).

Причем жирным курсивом выделены те функциональные требования, которые описывают возможные механизмы защиты на данном уровне, но не являются обязательными и соответственно не входят в БФП уровня.

Табл. 3.9 Совокупности ФТБ к криптографическим механизмам защиты БС, ранжированные по УД

| **УД** | **ФТБ** |
|---|---|
| УД1 | FCS_COP.1.1 |
| | FCS_CKM.1.1 |
| | ***FCS_CKM.2.1*** |
| УД2, УД3, УД4 | FCS_COP.1.1 |
| | FCS_CKM.1.1 |
| | FCS_CKM.2.1 |

Перейдем ко второй группе механизмов защиты, которые обеспечивают процесс аутентификации в беспроводной сети. В рамках данной совокупности отдельным критериям оценки могут соответствовать уже целые семейства ФТБ.

Первоначально проведем исследование соответствия компонентов ФТБ совокупностям механизмов защиты по каждому УД в зависимости от используемого протокола аутентификации.

При реализации системы защиты БС в соответствии с УД1 мы имеем дело только с самим протоколом аутентификации, поэтому все требования безопасности на этом уровне описываются только посредством семейства FIA_UAU.

Компонент FIA_UAU.1.1 является невостребованным при построении БС и в значительной степени представляет угрозу для ее безопасности. Разрешение пользователю определенных действий до окончания процесса аутентификации при использовании беспроводных технологий чревато реализацией серьезных атак. В первую очередь это связано именно с широковещательной природой данного вида сетей и отсутствием необходимости прямого физического доступа к аппаратному обеспечению для установления связи.

Компонент FIA_UAU.2 является обязательным для всех протоколов аутентификации на всех уровнях доверия, так как предписывает требование завершения процесса аутентификация пользователя до любых его действий в сети.

Компонент FIA_UAU.5.1 определяет предоставляемые механизмы аутентификации в рамках реализованного протокола. Так как любой протокол аутентификации, по сути, есть ни что иное, как набор правил, то данный компонент также является обязательным на любом УД.

Таким образом, для первого уровня доверия ФТБ к БС будут минимальны (табл. 3.10).

Табл. 3.10 Совокупность ФТБ к механизмам аутентификации в БС для УД1

| **Аутентификация с открытым ключом** | **Аутентификация с общим ключом** |
|---|---|
| FIA_UAU.2 | FIA_UAU.2 |
| FIA_UAU.5.1 | FIA_UAU.5.1 |

Начиная с УД2, для процесса аутентификации в сети используется семейство протоколов EAP. Все протоколы данного семейства при своей реализации используются выделенный сервер аутентификации, которому соответствует объединенная совокупность ФТБ FIA_SOS, а именно компонент FIA_SOS 2.2, который используется на всех отличных от первого уровнях доверия.

В связи с введением сервера аутентификации усложняется процедура доступа пользователя к информационным ресурсам сети. Появляется требование к обнаружению и предотвращению подделки данных аутентификации, которое сполна может быть выражено посредством компонента ФТБ FIA_UAU3.1.

Также, за счет усложнения процесса аутентификации, увеличивается число процедур, которые позволяют его успешно пройти. С введением протокола LEAP начинается использоваться компонент FIA_UAU.5.2, который специфицирует правила взаимодействия процедур и очередность их выполнения.

Еще на УД2 вводится такое понятие, как взаимная аутентификация, которая не является обязательной, но ощутимо увеличивает уровень безопасности ОО. Для ее описания при построении ПЗ необходимо использовать компонент ФТБ FPT_SSP.2, который обеспечивает взаимное надежное подтверждение данных.

Совокупность ФТБ для УД2 в зависимости от используемого протокола аутентификации представлена в таблице 3.11.

Табл. 3.11 Совокупность ФТБ к механизмам аутентификации в БС для УД2

| **Аутентификация по протоколу EAP-MD5** | **Аутентификация по протоколу LEAP** |
|---|---|
| FIA_UAU.2 | FIA_UAU.2 |
| FIA_UAU.3.1 | FIA_UAU.3.1 |

Продолжение табл. 3.11

| **Аутентификация по протоколу EAP-MD5** | **Аутентификация по протоколу LEAP** |
|---|---|
| FIA_UAU.5.1 | FIA_UAU.5.1 |
| FIA_SOS.2.2 | FIA_UAU.5.2 |
| | FIA_SOS.2.2 |
| | ***FPT_SSP.2*** |

Следующее поколение протоколов аутентификации для увеличения степени безопасности при доступе к сетевым ресурсам начинает использовать цифровые сертификаты, изначально предустановленные либо на клиенте, либо на сервере. Для описания этого процесса с помощью ФТБ используется семейство FDP_DAU.

Причем при реализации протокола EAP-TLS наличие цифровых сертификатов является обязательным и затрагивает такие компоненты как FDP_DAU.1.1 и FDP_DAU.1.2.

При использовании же протокола PEAP мы имеем дело только с компонентом FDP_DAU.1.2 в качестве параметра. Это связано с тем, что цифровые сертификаты являются обязательными для аутентификации клиента на сервере, в то время как авторизация пользователя происходит непосредственно по вводимому паролю.

Также на УД3 вводится новый компонент семейства FIA_UAU: FIA_UAU.7.1 для описания процедуры защищенной обратной связи в процессе аутентификации.

Результаты соответствия ФТБ аутентификационным механизмам защиты для УД3 представлены в таблице 3.12.

Табл. 3.12 Совокупность ФТБ к механизмам аутентификации в БС для УД3

| **Аутентификация по протоколу EAP-TLS** | **Аутентификация по протоколу PEAP** |
|---|---|
| FIA_UAU.2 | FIA_UAU.2 |
| FIA_UAU.3.1 | FIA_UAU.3.1 |
| FIA_UAU.5.1 | FIA_UAU.5.1 |
| FIA_UAU.5.2 | FIA_UAU.5.2 |
| FIA_UAU.7.1 | FIA_UAU.7.1 |
| FIA_SOS.2.2 | FIA_SOS.2.2 |
| FDP_DAU.1.1 | FDP_DAU.1.2 |
| FDP_DAU.1.2 | ***FPT_SSP.2*** |
| ***FPT_SSP.2*** | |

На УД4 большое значение уделяется аутентификации данных с идентификацией гаранта. Компоненты FDP_DAU.2.1 и FDP_DAU.2.2 являются уже обязательной и неотъемлемой частью системы защиты при построении ПЗ для БС с такой степенью защищенности. Полученные результаты представлены в таблице 3.13.

Табл. 3.13 Совокупность ФТБ к механизмам аутентификации в БС для УД4

| **Аутентификация по протоколу PEAP** | **Аутентификация по протоколу EAP-TTLS** |
|---|---|
| FIA_UAU.2 | FIA_UAU.2 |
| FIA_UAU.3.1 | FIA_UAU.3.1 |
| FIA_UAU.5.1 | FIA_UAU.5.1 |
| FIA_UAU.5.2 | FIA_UAU.5.2 |
| FIA_UAU.7.1 | FIA_UAU.7.1 |

Продолжение табл. 3.13

| **Аутентификация по протоколу PEAP** | **Аутентификация по протоколу EAP-TTLS** |
|---|---|
| FIA_SOS.2.2 | FIA_SOS.2.2 |
| FDP_DAU.1.2 | ***FDP_DAU.1.1*** |
| FPT_SSP.2 | FDP_DAU.2.1 |
| | FDP_DAU.2.2 |
| | ***FPT_SSP.2*** |

Исходя из приведенных выше данных, найдем общие ФТБ для каждого уровня доверия и составим для них БФП ПЗ (табл. 3.14):

Табл. 3.14 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 |

Продолжение табл. 3.14

| **Уровень доверия** | **Функциональные требования безопасности** |
|---|---|
| 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 |

Таким образом, были получены четыре базовых функциональных пакета для каждого уровня доверия к беспроводной сети, на основании которых можно построить непосредственно профиль защиты БС в зависимости от уровня ее защищенности и в дальнейшем провести ее аттестацию или сертификацию.

# ГЛАВА 4. МЕТОДИКА АУДИТА ЗАЩИЩЕННОСТИ БЕСПРОВОДНОЙ СЕТИ НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ГОСТ Р ИСО/МЭК 15408

## 4.1 Методика построения профиля защиты для беспроводной сети на основе соответствующего ей уровня доверия

Для построения профиля защиты для беспроводной сети первоначально необходимо провести анализ самой сети на предмет реализованных в ней механизмов защиты, причем стоит отметить, что особое внимание нужно уделить разграничению основных механизмов защиты, описанных в семействе стандартов 802.11, и дополнительных, реализованных в системе защиты в качестве контрмер определенным угрозам либо атакам.

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. Например, в ОО возможно использование нескольких протоколов шифрования: для защиты

циркулирующей в системе информации и для защиты передаваемых аутентификационных данных. Зачастую при передаче последних реализуются более серьезные и криптостойкие протоколы. Это связано с тем, что средства защиты БС развивались неравномерно по всем аспектам защиты ее активов: изначально большее внимание уделялось конфиденциальности передаваемой информации, а не контролю доступа к ней. Поэтому при зашифровании данных аутентификации пользователя обычно внедряют более поздние протоколы, которые обладают большей стойкостью к расшифрованию. Но здесь стоит отметить тот факт, что криптостойкость алгоритма практически прямо пропорциональна требуемым для его реализации возможностям аппаратного обеспечения и пропускной способности радиоканалов связи. То есть использовать такой протокол для защиты всей передаваемой информации нецелесообразно. Но, с другой стороны, объем аутентификационных данных невелик, поэтому для их защиты вполне допустимо и даже рекомендуемо обращение к протоколам шифрования, отличным от WEP либо AES.

Исследование же ОО по критериям оценки защищенности БС отдельно по каждому аспекту поможет избежать подобной неточности.

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. Как и на предыдущем этапе, совокупность рассматривается отдельно по двум аспектам защиты. То есть УД к БС находится первоначально по функциям системы защиты, связанным с конфиденциальностью данных, а затем по функциям, связанным с контролем доступа к ОО. Порядок исследования не имеет значения.

Итогом данного процесса является совокупность двух чисел, определяющих уровень доверия к сети с точки зрения криптографических алгоритмов либо протоколов аутентификации.

Теперь необходимо проанализировать полученную совокупность и уже окончательно определить единый УД к БС.

При первоначальном рассмотрении задача кажется достаточно тривиальной, так как в соответствии с принципами обеспечения защищенности информационной системы ОУД к ней, а в нашем случае УД, не может превышать минимального значения по каждому аспекту реализованной системы защиты. Таким образом, УД к БС должен быть определен как наименьшее число из полученной совокупности. Обозначим его как промежуточный уровень доверия - $УД_{пр}$.

$$УД_{пр} = \min\{УД_{кр}, УД_{ау}\}, \quad (4.1)$$

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 IEEE 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.

К сожалению, темпы роста количества новых угроз и атак на БС значительно опережают средние временные показатели ратификации новых стандартов в этой области телекоммуникационных технологий. Но условия жесткой конкурентной борьбы, которые являются реалиями современного мира, требуют своевременной разработки контрмер для отражения атак и

защиты от угроз для БС, поскольку в силу значительных преимуществ данного вида связи, о которых уже упоминалось ранее, вопрос использования только сетей на базе семейства стандартов 802.3 не рассматривается.

Для решения возникшей коллизии разработчики программного обеспечения и оборудования пошли по пути наименьшего сопротивления: появляющиеся на рынке продукты, призванные обезопасить БС, направлены на предотвращение только одного вида атак.

Ярким примером сложившейся ситуации являются wormhole-атаки на беспроводные сети. Существует порядка десяти решений, призванных обезопасить сеть от подобного вторжения, как программных, так и аппаратных, которые требуют немалых финансовых вложений: разработка более защищенных протоколов маршрутизации, как TrueLink либо LiteWrop[66, 69], использование направленных антенн [67], добавление в передаваемый информационный пакет определенной идентификационной метки [25, 68].

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. То есть другими словами, необходимо вычислить значение пересечения множества $D_{\text{ФТБ}}$ и разности двух множеств БФП: БФП для $УД_{пр}$ и БФП для $УД_{пр+1}$.

Значение пересечения вышеупомянутых множеств может принимать два значения: либо пустого множества, либо некоего множества $Z$, состоящего из некоторого набора ФТБ, входящих в БФП $УД_{пр+1}$.

$$D_{\text{ФТБ}} \cap \left(БФП_{пр+1} \setminus БФП_{пр}\right) = \begin{cases} \varnothing \\ Z \end{cases}, \qquad (4.2)$$

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

$$БФП_{пр} \cup Z = БФП_{пр+1}, \quad (4.3)$$

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

Если же

$$БФП_{пр} \cup Z \subset БФП_{пр+1}, \quad (4.4)$$

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. То есть другими словами, получается, что если в результате исследования основных механизмов защиты БС ей можно присвоить УД4, то все, что реализовано в ее системы защиты сверх этого, автоматически увеличивает уровень доверия к ней до УД5 в соответствии с равенством (4.3).

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 $УД_{пр}$. В данной ситуации невозможно выработать один либо несколько универсальных вариантов ее решения. 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. Процесс определения уровня доверия к БС в общем виде показан на рисунке 4.1.

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. То есть при формировании БФП для УД5 не стоит учитывать все элементы совокупности дополнительных средств защиты ОО, а только те, которые действительно могут соответствовать УД5.

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 ОО и его среды безопасности.

Описание ОО затрагивает не только саму БС, но и стандартное сетевое проводное оборудование, без которого было бы невозможно ее полное функциональное развертывание.

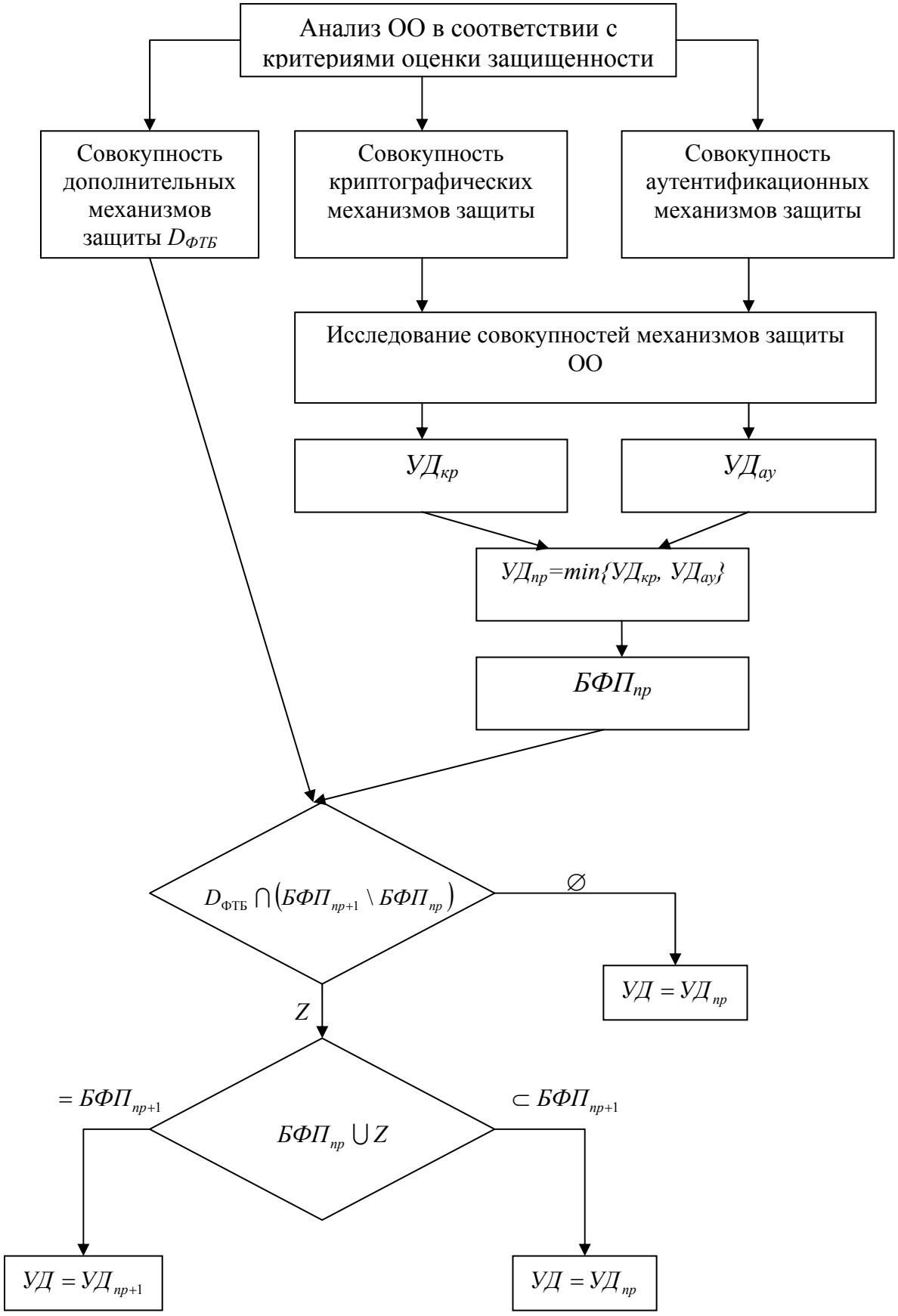


Рис. 4.1 Процесс определения УД к БС

Вариант реализации БС, при котором связь между участниками информационного обмена устанавливается в режиме «Ad-hoc», маловероятна, поскольку свидетельствует о неразвитой инфраструктуре сети. Так как разработка ПЗ для БС представляет собой трудоемкий процесс, требующий для своей реализации дополнительных вложений денежных средств, то экономически нецелесообразно проводить его для сети с подобной архитектурой.

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 [11].

Также стоит отметить, что активы беспроводной сети могут быть доступны внешним информационным системам, которые находятся вне политики безопасности ОО. Хотя пользователи внешних информационных систем могут быть в какой-то степени доверенными, они находятся вне области управления этим конкретным ОО, и так как никто не может предполагать об их намерениях, то они не должны рассматриваться как доверенные пользователи.

Необходимо учесть, что в силу специфики функционирования БС, защита компонентов информационной системы от несанкционированного физического доступа затруднена. В связи с этим, длительное хранение конфиденциальной информации, и других защищаемых активов, на данных компонентах невозможно. Поэтому, требуется предусмотреть возможность

резервного копирования, и хранения особо важной информации на носителях удаленной защищенной информационной системы.

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.

В разделе «Требования безопасности ИТ» помимо тех ФТБ, которые включаются на основании БФП для определенного УД к ОО, стоит рассмотреть добавление следующих (табл. 4.1):

Табл. 4.1 Перечень ФТБ для включения в ПЗ для БС

| **Компонент** | **Название** |
|---|---|
| FAU_ARP.1 | Сигналы нарушения безопасности |
| FAU_GEN.1 | Генерация данных аудита |
| FAU_SAA.1 | Анализ потенциального нарушения |
| FAU_SAR.1 | Просмотр аудита |
| FAU_SAR.2 | Ограниченный просмотр аудита |
| FAU_SAR.3 | Выборочный просмотр аудита |
| FAU_SEL.1 | Избирательный аудит |
| FAU_STG.1 | Защищенное хранение журнала аудита |
| FAU_STG.4 | Предотвращение потери данных аудита |
| FDP_RIP.2 | Полная защита остаточной информации |
| FDP_ROL.1 | Базовый откат |
| FDP_SDI.2 | Мониторинг целостности хранимых данных и предпринимаемые действия |
| FMT_MTD.1 | Управление данными ФБО |
| FMT_MTD.2 | Управление ограничениями данных ФБО |
| FMT_MTD.3 | Безопасные данные ФБО |
| FMT_SMR.1 | Роли безопасности |

Продолжение табл. 4.1

| Компонент | Название |
|---|---|
| FPT_PHP.2 | Оповещение о физическом нападении |
| FPT_PHP.3 | Противодействие физическому нападению |
| FPT_RCV.2 | Автоматическое восстановление |
| FPT_RCV.4 | Восстановление функции |
| FPT_RVM.1 | Невозможность обхода ПБО |
| FRU_FLT.1 | Пониженная отказоустойчивость |
| FRU_PRS.2 | Полный приоритет обслуживания |
| FRU_RSA.1 | Максимальные квоты |
| FTA_MCS.1 | Базовое ограничение на параллельные сеансы |
| FTA_TAH.1 | История доступа к ОО |

В раздел «Требования доверия к безопасности ОО» необходимо включить требования доверия, которые описаны в третьей части ГОСТ Р ИСО/МЭК 15408 для ОУД, используя прямую зависимость между ОУД и полученным УД к ОО (табл. 4.2). Причины отсутствие в таблице ОУД6 и ОУД7 приводились в третьей главе.

Табл. 4.2 Требования доверия к безопасности ОО, проранжированные по УД

| **Классы требований доверия к безопасности** | **Семейства требований доверия к безопасности** | **Компоненты требований доверия к безопасности** | | | | |
|---|---|---|---|---|---|---|
| | | ОУД1 (УД1) | ОУД2 (УД2) | ОУД3 (УД3) | ОУД4 (УД4) | ОУД5 (УД5) |
| Управление конфигурацией | ACM_AUT | | | | 1 | 1 |
| | ACM_CAP | 1 | 2 | 3 | 4 | 4 |
| | ACM_SCP | | | 1 | 2 | 3 |

Продолжение табл. 4.2

| **Классы требований доверия к безопасности** | **Семейства требований доверия к безопасности** | **Компоненты требований доверия к безопасности** | | | | |
|---|---|---|---|---|---|---|
| | | ОУД1 (УД1) | ОУД2 (УД2) | ОУД3 (УД3) | ОУД4 (УД4) | ОУД5 (УД5) |
| Поставка и эксплуатация | ADO_DEL | | 1 | 1 | 2 | 2 |
| | ADO_IGS | 1 | 1 | 1 | 1 | 1 |
| Разработка | ADV_FSP | 1 | 1 | 1 | 2 | 3 |
| | ADV_HLD | | 1 | 2 | 2 | 3 |
| | ADV_IMP | | | | 2 | 2 |
| | ADV_INT | | | | 2 | 1 |
| | ADV_LLD | | | | 1 | 1 |
| | ADV_RCR | 1 | 1 | 1 | 1 | 2 |
| | ADV_SPM | | | | 1 | 3 |
| Руководства | AGD_ADM | 1 | 1 | 1 | 1 | 1 |
| | AGD_USR | 1 | 1 | 1 | 1 | 1 |
| Поддержка жизненного цикла | ALC_DVS | | | 1 | 1 | 1 |
| | ALC_FLR | | | | 3 | |
| | ALC_LCD | | | | 2 | 2 |
| | ALC_TAT | | | | 1 | 2 |
| Тестирование | ATE_COV | | 1 | 2 | 2 | 2 |
| | ATE_DPT | | | 1 | 1 | 2 |
| | ATE_FUN | | 1 | 1 | 1 | 1 |
| | ATE_IND | 1 | 2 | 2 | 2 | 2 |
| Оценка уязвимостей | AVA_CCA | | | | 1 | 1 |
| | AVA_MSU | | | 1 | 2 | 2 |
| | AVA_SOF | | 1 | 1 | 1 | 1 |
| | AVA_VLA | | 1 | 1 | 3 | 3 |

## 4.2 Экономические аспекты защиты информации в беспроводной сети

При современном уровне развития техники разработка средств защиты или перехвата информации требуют значительных затрат. В свете этого возникает важная проблема – проблема соотношения цены на информацию и затрат на ее защиту или добывание [65].

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;

$С_3$, Са - средства, выделяемые на защиту или добывание информации;

$р_3$, ра - вероятность успеха защищающейся и атакующей сторон.

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

$$C_З \le Цз, \tag{4.5}$$

$$Са \le Ца. \tag{4.6}$$

Кроме ценности информации следует также учесть и вероятность того, что противнику удастся получить доступ к информации, исходя из этих соображений сумма средств, выделяемых на защиту или добывание информации не должна быть больше математического ожидания выгоды в случае успеха:

$$C_з \le p_a \cdot Ц_з, \tag{4.7}$$

$$C_a \le p_з \cdot Ц_a. \tag{4.8}$$

Вероятность сложно оценить, поскольку она не является константой, а зависит от действий противоборствующих сторон:

$$p = f(C_з, C_a). \tag{4.9}$$

Функция, определяющая зависимость вероятности успеха может быть очень сложной, и не во всех случаях удастся её чётко математически сформулировать. Можно лишь утверждать, что события успеха той или иной стороны несовместны и составляют полную группу событий:

$$p_з+p_a=1. \tag{4.10}$$

Предположим, вероятности определяются формулами:

$$p_з = \frac{q_з \cdot C_з}{q_з \cdot C_з + q_a \cdot C_a} \tag{4.11}$$

$$p_a = \frac{q_a \cdot C_a}{q_з \cdot C_з + q_a \cdot C_a}, \tag{4.12}$$

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

Чтобы оценить, сколько средств будет разумно вложить в защиту информации, подставим значение вероятности утечки информации (4.12) в неравенство (4.7):

$$C_з \le \frac{q_a \cdot C_a}{q_з \cdot C_з + q_a \cdot C_a} \cdot Ц_з. \tag{4.13}$$

Учитывая, что ценность информации и сумма вложенных средств не могут быть отрицательными, получаем систему неравенств:

$$q_з \cdot C_з^2 + q_a \cdot C_з \cdot C_a - q_a \cdot C_a \cdot Ц_з \le 0, \tag{4.14}$$

$$q_з, q_a, C_з, C_a, Ц_з \ge 0. \tag{4.15}$$

Решив систему (4.14), (4.15) получим, что максимальная сумма средств, которую целесообразно использовать на защиту информации, составит

$$C_з = \frac{\sqrt{q_a^2 \cdot C_a^2 + 4 \cdot q_a \cdot q_з \cdot C_a \cdot Ц_з} - q_a \cdot C_a}{2 \cdot q_з}. \tag{4.16}$$

Если предположить, что сумма средств, выделенных атакующей стороной равна ценности информации, а информация имеет одинаковую ценность для обеих сторон, то формула (4.16) примет вид:

$$C_з = Ц_з \cdot \frac{\sqrt{q_a^2 + 4 \cdot q_a \cdot q_з} - q_a}{2 \cdot q_з}. \tag{4.17}$$

Если также предположить, что противоборствующие стороны находятся в равных условиях, т.е. $q_з=q_a$, то сумма затрат на защиту информации не должна превышать

$$C_з = Ц_з \cdot \frac{\sqrt{5}-1}{2}. \qquad (4.18)$$

Эффективность предлагаемой модели оценки затрат, требуемых для обеспечения защиты информации, зависит от того, насколько точно получится сформулировать вероятность успеха в формулах (4.7), (4.8).

Если же нет возможности оценить вероятность успеха, но есть основания полагать, что противник находится в равных с нами условиях, то устанавливаемую формулой (4.18) сумму вложений можно рассматривать как максимальный экономически обоснованный предел [27].

## 4.3 Методика проведения аудита защищенности беспроводной сети

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.

На данный момент в информационной безопасности нет устоявшегося определения аудита. Вот лишь несколько формулировок, используемых специалистами: «Аудит информационных систем — это проверка используемых компанией информационных систем, систем безопасности, систем связи с внешней средой, корпоративной сети на предмет их соответствия бизнес-процессам, протекающим в компании, а также соответствия международным стандартам, с последующей оценкой рисков сбоев в их функционировании» [50] .

«Аудит информационной безопасности – системный процесс получения объективных качественных и количественных оценок о текущем состоянии информационной безопасности компании в соответствии с определенными критериями и показателями безопасности» [45].

Таким образом, аудит в данном случае сводится к проверке системы информационной безопасности и сравнению результатов данной проверки с неким идеалом. Для различных видов аудита различается все три составляющие услуги аудита: средства и способы проверки, результат проверки и идеал, с которым сравнивается результат проверки.

Одним из самых распространенных видов аудита является активный аудит. Это исследование состояния защищенности информационной системы с точки зрения хакера (или некоего злоумышленника, обладающего высокой квалификацией в области информационных технологий). Зачастую компании-поставщики услуг активного аудита именуют его инструментальным анализом защищенности, чтобы отделить данный вид аудита от других.

Суть активного аудита состоит в том, что с помощью специального программного обеспечения (в том числе, с помощью систем анализа защищенности) и специальных методов осуществляется сбор информации о состоянии системы сетевой защиты.

При осуществлении данного вида аудита на систему сетевой защиты моделируется как можно большее количество таких сетевых атак, которые может выполнить хакер. Естественно, атаки всего лишь моделируются и не оказывают какого-либо деструктивного воздействия на информационную систему. Их разнообразие зависит от используемых систем анализа защищенности и квалификации аудитора. Результатом активного аудита является информация обо всех уязвимостях, степени их критичности и методах устранения, сведения о широкодоступной информации (информация, доступная любому потенциальному нарушителю) сети заказчика.

По окончании активного аудита выдаются рекомендации по модернизации системы сетевой защиты, которые позволяют устранить опасные уязвимости и тем самым повысить уровень защищенности информационной системы от действий «внешнего» злоумышленника при минимальных затратах на информационную безопасность.

Однако без проведения других видов аудита эти рекомендации могут оказаться недостаточными для создания «идеальной» системы сетевой защиты.

Экспертный аудит можно условно представить как сравнение состояния информационной безопасности с «идеальным» описанием, которое базируется на следующем:

- требования, которые были предъявлены руководством в процессе проведения аудита;
- описание «идеальной» системы безопасности, основанное на аккумулированном в компании-аудиторе мировом и частном опыте.

Один из самых объемных видов работ, которые проводятся при экспертном аудите, – сбор данных об информационной системе путем интервьюирования представителей заказчика и заполнения ими специальных анкет.

Основная цель интервьюирования технических специалистов — сбор информации о функционировании сети, а руководящего состава компании – выяснение требований, которые предъявляются к системе информационной безопасности.

По результатам работ данного этапа предлагаются изменения (если они требуются) в существующей информационной системе и технологии обработки информации, направленные на устранение найденных недостатков с целью достижения требуемого уровня информационной безопасности.

В рамках экспертного аудита производится анализ организационно-распорядительных документов, таких как политика безопасности, план защиты и различного рода инструкции. Организационно-распорядительные документы оцениваются на предмет достаточности и непротиворечивости декларируемым целям и мерам информационной безопасности.

Результаты экспертного аудита могут содержать разноплановые предложения по построению или модернизации системы обеспечения информационной безопасности.

Суть данного вида аудита наиболее приближена к тем формулировкам и целям, которые существуют в финансовой сфере — при проведении данного вида аудита состояние информационной безопасности сравнивается с неким абстрактным описанием, приводимым в стандартах.

Официальный отчет, подготовленный в результате проведения данного вида аудита, включает следующую информацию:

- степень соответствия проверяемой информационной системы выбранным стандартам;
- степень соответствия собственным внутренним требованиям компании в области информационной безопасности;

- количество и категории полученных несоответствий и замечаний;
- рекомендации по построению или модификации системы обеспечения информационной безопасности, позволяющие привести её в соответствие с рассматриваемым стандартом;
- подробная ссылка на основные документы заказчика, включая политику безопасности, описания процедур обеспечения информационной безопасности, дополнительные обязательные и необязательные стандарты и нормы, применяемые к данной компании.

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.

Государственные организации, которые обрабатывают сведения, составляющие государственную тайну, в соответствии с российским законодательством обязаны проводить аттестацию информационной системы (во многом процедура аналогична сертификации). Однако такие организации чаще всего пользуются не услугой аудита на соответствие стандартам, а в обязательном порядке проводят аттестацию собственных информационных систем при участии аттестационных центров.

Среди государственных организаций (а также среди «полугосударственных» — организаций с большой долей уставного капитала, принадлежащего государству) велика доля тех, кто в соответствии с законодательством не обязан проводить аттестацию информационной системы. Для них аудит на соответствие стандартам более актуален. Чаще

всего его проводит компания-интегратор, которая имеет большой опыт успешного взаимодействия с компанией-заказчиком. При необходимости в качестве субподрядчиков привлекаются аттестационные центры.

В последнее время все большее количество компаний рассматривают получение сертификата, подтверждающего высокий уровень информационной безопасности, как «козырь» в борьбе за крупного клиента или делового партнера. В этом случае целесообразно проведение аудита и последующей сертификации на соответствие тем стандартам, которые являются значимыми для клиента или делового партнера.

Иногда руководство компании проявляет инициативу по сертификации системы информационной безопасности. Для таких организаций важны не только защита собственных ресурсов, но и подтверждение со стороны независимого эксперта (в роли которого выступает компания-аудитор) высокого уровня защиты [48].

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 2 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.

На первом этапе необходимо провести пассивный аудит защищенности сети, который представляет собой исследование ОО и выявление реализованных в нем механизмов защиты информации, исходя из возможностей имеющегося оборудования и целей и задач, которые были поставлены при развертывании БС, при отсутствии моделирования возможных угроз и атак на ресурсы сети. Всю процедуру желательно проводить по критериям оценки защищенности, так как в дальнейшем это значительно упростит и ускорит процессы определения уровня доверия к сети и построения профиля защиты для нее. Данная рекомендация не является обязательной при выполнении аудита в соответствии с данной методикой.

Второй этап, по сути, представляет собой продолжением первого и является его частью с тем лишь условием, что основное внимание уделяется

дополнительным механизмам защиты информации, внедренным в БС в качестве контрмер определенным видам угроз или атак.

На следующем этапе необходимо провести сравнительный анализ полученной совокупности механизмов защиты с целью определения уровня доверия к сети. Как и в случае построения ПЗ для БС, изначально определяется УД по каждой группе механизмов защиты, а потом на основании полученных данных – общий промежуточный УД.

После этого необходимо провести сопоставление полученной совокупности дополнительных механизмов защиты с ФТБ. Даже если в дальнейшем не планируется проводить сертификацию либо аттестацию ОО этому процессу стоит уделить должное внимание, так как от точности его результатов во многом зависит определение истинного УД к БС на следующем этапе и в целом корректность суждений об уровне ее защищенности.

После определения истинного УД к БС необходимо сравнить его с тем уровнем, который, по мнению заказчика, должен быть реализован по отношению к ОО. Вполне закономерными являются три возможных результата:

- $УД > \text{УД}_{\text{зак}}$ ;
- $УД = УД_{зак}$ ;
- $УД < \text{УД}_{\text{зак}}$ ;

где $УД_{зак}$ - требуемый либо предполагаемый уровень доверия к ОО, по мнению заказчика.

Идеальной представляется ситуация, когда выявленный УД равен тому, которому, по мнению заказчика, и должна соответствовать защищенность БС. Но, к сожалению, вероятность ее незначительна. Зачастую реальный УД ОО не равен предполагаемому. В этом случае необходимо рассчитать экономическую целесообразность реализованной системы защиты.

На основании полученных результатов и в соответствии с требованиями заказчика, можно дать рекомендации по изменению

механизмов защиты, использующих в БС, для соответствия ее требуемому уровню защищенности.

При необходимости усиления либо ослабления системы защиты стоит обратить внимание на уровни доверия, полученные для разных групп механизмов защиты. Вполне возможна ситуация, когда изменению можно будет подвергнуть не всю систему защиты полностью, а только ту ее часть, которая отвечает шифрование передаваемых данных либо за контроль доступа к сети.

В целом процесс проведения аудита защищенности БС схематично изображен на рисунке 4.2.

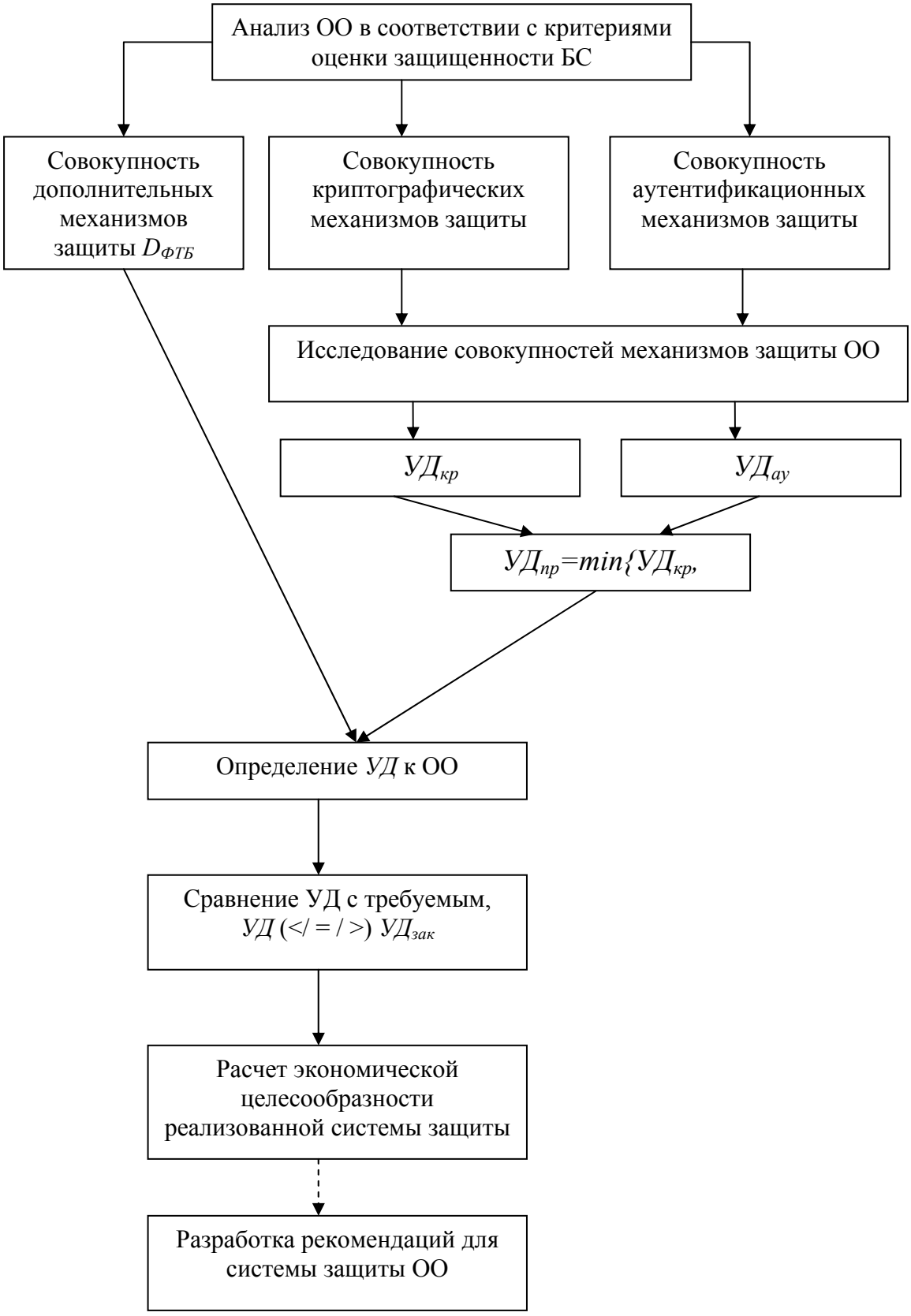


Рис. 4.2 Процесс проведения аудита защищенности БС

# ЗАКЛЮЧЕНИЕ

В результате проведенных исследований в области обеспечения информационной безопасности данных при их передаче по радиоканалам в рамках структуры БС была построена модель семейства ПЗ для данного вида сетей.

На основе модели был разработан метод построения семейства ПЗ для БС и был сформулирован перечень рекомендаций по данному вопросу.

Модель и метод построения семейства ПЗ для БС легли в основу разработанной методики формирования ПЗ для ИС, в которой в качестве ОО выступает беспроводная сеть. Также они явились основополагающими для разработки методики аудита защищенности БС в соответствии с ГОСТ Р ИСО/МЭК 15408.

Практическая значимость данного исследования заключается в том, что на основе описанной в ней модели семейства ПЗ для БС возможна разработка специализированных руководящих документов для сертификации и аттестации 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 и аттестации БС.

Результаты диссертационных исследований в дальнейшем могут быть использованы при разработке ЗБ для БС, на начальных этапах ее проектирования в соответствии с требуемым уровнем безопасности сети и требуемым уровнем доверия к ее системы защиты.

Также в дальнейшем возможны исследования в области защиты информации при ее передаче по беспроводным каналам связи, особенно в части стандартизации механизмов защиты в соответствии с ГОСТ Р ИСО/МЭК 15408 и формализации требований безопасности к беспроводным сетям.

# СПИСОК ЛИТЕРАТУРЫ


1. Барановский В. Беспроводная защита // Сети и телекоммуникации. – 2006. – 1 сентября [Электронный ресурс]. URL: http://www.seti-ua.com/?in=seti_show_article&seti_art_ID=179&_by_id=1&_CATEGORY=26 (дата обращения: 15.03.2009).
2. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии. – М.: Горячая Линия-Телеком, 2001. – 140 с.
3. Барсуков В.С., Пономарев А.А. Беспроводные технологии «последнего дюйма» // Специальная техника. – 2005. – № 1 [Электронный ресурс]. URL: http://www.ess.ru/publications/1_2005/barsukov/barsukov.htm (дата обращения: 21.11.2008).
4. Беделл П. Сети. Беспроводные технологии. – М.: НТ Пресс, 2008. – 448 с.
5. Бейс Р. Введение в обнаружение атак и анализ защищенности. – М.: Информзащита, 1999. – 298 с.
6. Беспроводные сети Wi-Fi / А.В. Пролетарский, И.В. Баскаков, Д.Н. Чирков и [др.]. – М.: Интуит, 2007. – 216 с.
7. Бойцев О.М. Защити свой компьютер от вирусов и хакеров. – СПб.: Питер, 2009. – 176 с.
8. Бойченко А.В., Филинов Е.Н. Проблемы и методика формирования профилей защиты открытых информационных систем. – 2001 [Электронный ресурс]. URL: http://www.elbib.ru/index.phtml?page=elbib/rus/methodology/profiles/Profile_IS (дата обращения: 18.10.2009).
9. Вишневский В.М., Семенова О.В. Системы поллинга. Теория и применение в широкополосных беспроводных сетях. – М.: Техносфера, 2007. – 312 с.

10. Владимиров А.А., Гавриленко К.В., Михайловский А.А. Wi-фу: «боевые» приемы взлома и защиты беспроводных сетей. - М.: НТ Пресс, 2005. – 464 с.
11. Воронов А.В. Метод и модель построения системы защиты информации мобильных подразделений таможенных органов: дис. … канд. техн. наук. – СПб, 2005. – 179 с.
12. Галатенко В.А. Основы информационной безопасности. – 4-е изд., стереотипное. – М.: Интуит, 2008. – 206 с.
13. Галатенко В.А. Стандарты информационной безопасности. – М.: Интуит, 2006. – 264 с.
14. Гордейчик С.В., Дубровин В.В. Безопасность беспроводных сетей. – М.: Горячая Линия-Телеком, 2008. – 288 с.
15. ГОСТ Р ИСО/МЭК 15408—2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. — М.: Изд-во стандартов, 2002. — 527 с.
16. Григорьев В.А., Лагутенко О.И., Распаев Ю.А. Сети и системы радиодоступа. – М.: Эко-Трендз, 2005. – 384 с.
17. Джонсон А. Обзор средств обеспечения безопасности беспроводных сетей. – 2008 [Электронный ресурс]. URL: http://www-europe.cisco.com/web/RU/products/hw/wireless/secure/wlan_secure.html (дата обращения: 19.11.2009).
18. Дэвис Дж. Создание защищенных беспроводных сетей 802.11 в Microsoft Windows. – М.: Эком, 2006. – 400 с.
19. Ермолаев Е. Без проводов и без защиты // Хакер. – 2005. - № 59. – С. 18-24.
20. Ерохин А.Л., Турута А.П. Идентификация нештатных ситуаций в информационных сетях // Бионика интеллекта. – 2006. - №1. – С. 46-55.

21. Есауленко А. Обустройство беспроводной России. – 2004. – 31 мая [Электронный ресурс]. URL: http://www.osp.ru/nets/2004/07/151471/ (дата обращения: 18.11.2009).
22. Захаров А.П. Методология оценки информационной безопасности профиля защиты. – 2005. – 20 мая [Электронный ресурс]. URL: http://www.bezpeka.com/ru/lib/spec/art114.html (дата обращения: 19.03.2009).
23. Зегжда Д.П., Ивашко А.М. Как построить защищенную информационную систему. – СПб.: Мир и семья, 1997. – 312 с.
24. 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.
25. Иващук И.Ю. Предотвращение wormhole атак в беспроводных сетях с помощью пакетных меток // Научно-технический вестник СПбГУ ИТМО. – 2008. - № 52. – С. 188-194.
26. Кайгородский Г.А., Иванов П.С. Механизм шифрования WEP. – 2008. – 5 ноября [Электронный ресурс]. URL: http://wifi-zone.ucoz.ru/publ/1-1-0-33 (дата обращения: 13.08.2009).
27. Карасев Р.Ю. Моделирование оценки затрат, требуемых для обеспечения защиты информации // Вестник СевКавГТУ: естественные науки. – 2004. - № 7. – С. 115-121.
28. Карпов А. WEP. Антология уязвимостей и атак. – 2003 [Электронный ресурс]. URL: http://ank-pki.ru/wep/wep_ank.html (дата обращения: 19.04.2008).
29. Кенин А. Самоучитель системного администратора. – 2-е изд., стереотипное. – СПб.: БХВ-Петербург, 2008. – 561 с.
30. Киселев А.А., Новиков С.Н. Алгоритм оценки профиля защиты информации в телекоммуникационных сетях // Исследовано в России: электронный научный журнал. – 2005 [Электронный ресурс]. URL:

http://zhurnal.ape.relarn.ru/articles/2005/197.pdf (дата обращения: 10.04.2009).

31. Коротыгин С. Развитие технологии беспроводных сетей: стандарт IEEE 802.11. – 2001. – 6 июля [Электронный ресурс]. URL: http://www.ixbt.com/comm/wlan.shtml (дата обращения: 18.08.2007).
32. Кунегин С.В. История развития беспроводных сетей. – 2000. – 1 декабря [Электронный ресурс]. URL: http://kunegin.narod.ru/ref1/wireless/history.htm (дата обращения: 17.12.2007).
33. Лапонина О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия. – М.: Интуит, 2005. – 608 с.
34. Леонов А. Как ломаются беспроводные сети. – 2006. – 31 января [Электронный ресурс]. URL: http://www.ferra.ru/online/networks/s26260/ (дата обращения: 15.10.2007).
35. Липаев В., Филинов Е. Формирование и применение профилей открытых информационных систем. – 1997. – 17 мая [Электронный ресурс]. URL: http://www.dvgu.ru/meteo/PC/IS.htm (дата обращения: 18.07.2009).
36. Малиновский Д.Г., Никифоров Д.Е. Защищенная конфигурация точки доступа. – 2007. – 20 марта [Электронный ресурс]. URL: http://www.oszone.net/4627_1/ (дата обращения: 18.02.2008).
37. Мартынюк И. Безопасность – это процесс. – 2005. – 18 июля [Электронный ресурс]. URL: http://ko.com.ua/node/21244 (дата обращения: 07.09.2007).
38. Мерритт М., Поллино Д. Безопасность беспроводных сетей. – М.: ДМК Пресс, 2004. – 288 с.
39. Минакова Н.А. Модель создания профилей защиты для сетей связи и систем коммутации // Научно-технический вестник СПбГУ ИТМО. – 2006. - № 25. – С. 121-124.

40. Монин С. Защита информации и беспроводные сети // Компьютер Пресс. – 2005. - № 04. – С. 16-19.
41. Мустогин Б.Д., Прокофьев А.А. Обзор стандарта 802.1x и типов аутентификации EAP. – 2004. – 18 января [Электронный ресурс]. URL: http://www.intel.com/support/ru/wireless/wlan/sb/cs-008413.htm (дата обращения: 24.03.2008).
42. Мучлер Ш. Беспроводные сети как часть инфраструктуры ИТ. – 2004. – 17 июня [Электронный ресурс]. URL: http://www.osp.ru/lan/2004/06/139214/ (дата обращения: 22.11.2009).
43. Патий Е. Проблемы безопасности в беспроводных сетях. – 2005. – 23 апреля [Электронный ресурс]. URL: http://www.citforum.ru/security/articles/wireless_sec/ (дата обращения: 12.02.2008).
44. Пахомов С.Д. Анатомия беспроводных сетей // Компьютер-Пресс. – 2002. - № 7. – С. 167-175.
45. Петренко А.А., Петренко С.А. Аудит безопасности Intranet. – М.: АйТи-Пресс, 2002. – 386 с.
46. [59] Петров А.С. Введение в стандарт 802.11. – 2001 [Электронный ресурс]. URL: http://www.ovislink.biz/tech.phtml?item_id=584 (дата обращения: 18.01.2008).
47. Пивоваров Д. Деньги из воздуха // Хакер. – 2005. - № 56. – С. 08-14.
48. Просянников Р. Избавиться от заблуждений. Виды аудита информационной безопасности // Connect!. – 2004. - № 12 [Электронный ресурс]. URL: http://www.andek.ru/show_paper.php?idpaper=55 (дата обращения: 22.11.2009).
49. Прохоров С.А., Федосеев А.А., Денисов В.Ф. Методы и средства проектирования профилей интегрированных систем обеспечения комплексной безопасности предприятий наукоемкого машиностроения: монография. – Самара: СЦН РАН, 2009. – 199 с.

50. Росс Дж. Wi-Fi. Беспроводная сеть. – М.: НТ Пресс, 2007. – 320 с.
51. Рошан П., Лиэри Дж. Основы построения беспроводных локальных сетей стандарта 802.11 / пер. с англ. – М.: Вильямс, 2004. – 302 с.
52. Руководящий документ. Безопасность информационных технологий. Положение по разработке профилей защиты и заданий по безопасности. – М.: Гостехкомиисия России, 2003.
53. Руководящий документ. Безопасность информационных технологий. Руководство по формированию семейств профилей защиты. – М.: Гостехкомиисия России, 2003.
54. Столингс В. Беспроводные линия связи и сети / пер. с англ. – М.: Вильямс, 2003. – 640 с.
55. Филиппов М. Вопросы обеспечения безопасности корпоративных беспроводных сетей стандарта 802.11. Специфика России. – 2003. – 3 июня [Электронный ресурс]. URL: http://www.bugtraq.ru/library/security/wireless.html (дата обращения: 15.01.2008).
56. Хоуи Дж. Виды атак на сети стандарта 802.11 // Windows IT Pro. – 2006. - № 02. – С. 19-22.
57. Шахнович И.В. Беспроводные локальные сети. Анатомия стандартов IEEE 802.11 // Электроника: НТБ. – 2003. - №1. – с. 38-48.
58. Шахнович И.В. Современные технологии беспроводной связи. – М.: Техносфера, 2003. – 288 с.
59. Широкополосные беспроводные сети передачи информации / В.М. Вишневский, А.И. Ляхов, С.Л. Портной и [др.]. – М.: Техносфера, 2005. – 592 с.
60. Шоуэнберг Р. Атаки на банки. – 2008. – 23 октября [Электронный ресурс]. URL: http://www.securelist.com/ru/analysis/204007628/Ataki_na_banki (дата обращения: 22.05.2009).

61. Штейнер Б. Прикладная криптография. – 2-е изд., стереотипное. – М.: Триумф, 2002. – 608 с.
62. Щеглов А.Ю. Требования к средствам защиты конфиденциальной информации. – 2005. – 22 ноября [Электронный ресурс]. URL: http://www.sec4all.net/statea118.html (дата обращения: 23.12.2009).
63. Щербаков А.К. Wi-Fi: все, что Вы хотели знать, но боялись спросить. – М.: Бук-Пресс, 2005. – 239 с.
64. Щербаков АЮ. Введение в теорию и практику компьютерной безопасности. – М.: Издатель Молгачева С.В., 2001. – 352 с.
65. Ященко В.В. Введение в криптографию. – СПб.: Питер, 2001. – 288 с.
66. Eriksson J., Krishnamurthy S.V., Faloutsos M. TrueLink: a practical countermeasure to the wormhole attack in wireless networks // Network Protocols. – 2009. - vol.3. – P.75-84.
67. Hu L., Evans D. Using directional antennas to prevent wormhole attacks // Wireless communication and networks. – 2005. - vol. 2. – P. 1193-1199.
68. Hu Y.-C., Perrig A., Johnson D.B. Wormhole attacks in wireless networks // IEEE design and test of computers. – 2007. - vol. 24. - num. 2. – P. 370-380.
69. Khalil I., Bagchi S., Shroff N.B. LiteWorp: a lightweight countermeasure for the wormhole attack in multihop wireless networks // Dependable System and Networks. 2005. - vol. 1. – P. 612-621.
70. Schneier B. Applies Cryptography: protocols, algorithms and source code. – 2-nd edition. – New York: John Wiley & Sons, 1996. – 758 p.