ФГБОУ ВПО «Воронежский государственный
технический университет»

Кафедра систем информационной безопасности

190-2015

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

к курсовому проектированию
по дисциплине «Беспроводные системы связи
и их безопасность»
для студентов специальности 090302
«Информационная безопасность
телекоммуникационных систем»
очной формы обучения

Воронеж 2015

Составитель канд. техн. наук С. А. Ермаков

УДК 004.5

Методические указания к курсовому проектированию по дисциплине «Беспроводные системы связи и их безопасность» для студентов специальности 090302 «Информационная безопасность телекоммуникационных систем» очной формы обучения / ФГБОУ ВПО «Воронежский государственный технический университет»; сост. С.А. Ермаков. Воронеж, 2015. 37 с.

Методические указания предполагают углубленное изучение лекционного материала и приобретение навыков по оценке риска нарушения безопасности беспроводных сетей стандарта IEEE 802.11.

Методические указания подготовлены в электронном виде в текстовом редакторе MW-2013 и содержатся в файле Ермаков_КП_БССиБ.pdf.

Табл. 6. Ил. 4. Библиогр.: 3 назв.

Рецензент д-р техн. наук, проф. А. Г. Остапенко

Ответственный за выпуск зав. кафедрой д-р техн. наук, проф. А.Г. Остапенко

Издается по решению редакционно-издательского совета Воронежского государственного технического университета

ВВЕДЕНИЕ

На сегодняшний день беспроводные сети получили широкое развитие в области передачи данных. Это объясняется удобством их использования, дешевизной и приемлемой пропускной способностью. Исходя из текущей динамики развития, можно сделать вывод о том, что по количеству и распространенности беспроводные сети в скором времени превзойдут проводные сети. Эта динамика непосредственным образом влияет на требования к защите информации в беспроводных сетях

Не вызывает сомнения и тот факт, что при создании и эксплуатации защищенной беспроводной сети необходимо осуществлять систематический анализ и управление рисками, целью которого является выявление возможных угроз безопасности информации, оценка возможности их реализации и ожидаемого ущерба от такой реализации в интересах обеспечения защиты сети [1].

Следствием отсутствия единой методической базы по оценке эффективности средств защиты произвольной информационной системы является необходимость выбора среди существующих разрозненных методик наиболее адекватной поставленной цели и учитывающей имеющийся объем информации об объекте исследования [2].

Таким образом, курсовая работа предлагает самостоятельную разработку модели, а затем и реализацию алгоритма оценки риска, который служит вспомогательным инструментом для оценки эффективности защиты информации и динамического управления защищенностью беспроводных сетей.

Данные методические указания по написанию курсовой работы содержат теоретические сведения, рекомендации, а также сроки выполнения курсовой работы.

1. ЦЕЛИ И ЗАДАЧИ КУРСОВОЙ РАБОТЫ

Целью курсовой работы является разработка модели и программная реализация алгоритма оценки риска безопасности беспроводной сети заданной конфигурации. При этом студенты должны познакомиться с архитектурными особенностями беспроводных сетей, принципами их функционирования и обеспечения безопасности циркулирующей в них информации.

При выполнении курсовой работы студенты должны освоить основные подходы к моделированию рисков сети и способы их применения для анализа рисков при решении различных задач: выявление различий в конфигурациях беспроводных сетей, анализ эффективности существующих альтернатив при настройке системы защиты и др.

Динамичность протекающих процессов и самой архитектуры беспроводной сети делает задачу адекватного анализа рисков сети крайне актуальной. Поэтому для оперативного решения практических задач по оценке эффективности применяемых средств защиты возникающих в процессе эксплуатации сети применяется алгоритм оценки риска, который позволяет на практике получать оценки в соответствии с ключевыми характеристиками сети.

Практическая часть курсовой работы ориентирована на разработку программного инструмента для оценки интегрального риска безопасности с учетом ключевых зависимостей в беспроводной сети заданной конфигурации.

Студентам рекомендуется использовать современные инструментальные средства при создании модели и соответствующей ей программной реализации алгоритма оценки риска, например, текстовый редактор Microsoft Office Word 2013, систему моделирования MATLAB R2009a, и среду разработки Microsoft Visual Studio 2012.

2. ТРЕБОВАНИЯ К СОДЕРЖАНИЮ И ОБЪЁМУ КУРСОВОЙ РАБОТЫ

Основные требования к курсовой работе (КР) установлены стандартом предприятия СТП ВГТУ 62-2007. КР состоит из расчетно-пояснительной записки (РПЗ) объёмом от 30 до 50 страниц печатного текста с иллюстративным графическим материалом, размещенным по разделам работы, чертежей, схем.

Пояснительная записка содержит следующие разделы:

а) титульный лист;

б) задание на курсовую работу;

в) лист «Замечания руководителя»;

г) содержание включает введение, наименование всех разделов, подразделов, пунктов (если они имеют наименование), заключение, список литературы, наименование приложений с указанием номеров страниц, с которых начинаются эти элементы пояснительной записки;

д) введение;

е) основную часть (исследовательскую) содержащую:

- формирование иерархической модели элементов сети;
- заполнение необходимых таблиц соответствия
- реализация алгоритма оценки;
- анализ полученных результатов.

ж) заключение;

з) список литературы;

и) приложения (при необходимости).

Также к КР прилагается диск с разработанным ПО и электронным вариантом курсовой работы.

2.1. График выполнения курсовой работы

Таблица 1

График выполнения курсовой работы

Срок выполнения	Содержание работы
1 – 2-я недели семестра	Выбор задания курсовой работы. Ознакомление с постановкой задачи
3 – 8-я недели семестра	Осмысление задания, изучение подхода к его выполнению, разработка иерархической модели элементов сети. Подготовка к программной реализации алгоритма.
9 – 12-я недели семестра	Программная реализация алгоритма и его тестирование
13 – 15-я недели семестра	Оформление пояснительной записки. Окончательная отладка приложения
16 – 17-я недели семестра	Сдача пояснительной записки. Защита курсовой работы

2.2. Последовательность выполнения

Последовательность выполнения, рекомендации по выполнению разделов проекта:

1. Содержательный анализ задачи.

2. Формализация задачи.

2.1. Определить характеристики анализируемой системы, топологию, структуру и состав сети.

2.2. Построить четырехуровневые иерархические модели риска для каждого элемента беспроводной сети.

3. Адаптировать типовой алгоритм решения задачи к текущим условиям. (Описание можно проводить либо в виде блок-схемы, либо на псевдоязыке).

4. Разработать программу, реализующую алгоритм оценки.

4.1. Описать переменные (как основные, так и промежуточные).

4.2. Реализовать ввод исходных данных и вывод.

4.3. Реализовать полный алгоритм решения.

5. Провести отладку программы.

5.1. Составить контрольный пример.

5.2. Отладить программу.

6. Оформить отчет по курсовому проекту.

2.3. Критерии оценки курсовой работы

Оценка за курсовую работу складывается из оценки за предоставленный отчет, полноту выполненной работы, работоспособность программы, защиту (ответы на вопросы по теме проекта) и составляет от 2 до 5 («неудовлетворительно», «удовлетворительно», «хорошо», «отлично»).

3. ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Четырехслойная риск-модель

Применение иерархической структуры для разработки моделей беспроводных сетей (БС) является крайне полезным в связи с динамичностью протекающих в них процессов, поскольку при обнаружении изменений в сети в оценке меры риска участвуют только связанные слои. Риск-модели разрабатываются для отдельных устройств, которые являются элементами рассматриваемой БС. Мера риска БС, опираясь на модель, также должна учитывает взаимосвязи между устройствами, влияние атак, и степень защищенности, обеспечиваемую с помощью настроек средств защиты. Таким образом, методика анализа и регулирования риска, состоящая из риск-модели и меры оценки, позволяет эффективно оценивать интегральный риск системы с учетом ключевых зависимостей в БС. Адекватность получаемых в результате применения методики оценок может быть легко подтверждена соответствующими практическими экспериментами.

Для моделирования рисков в сетях традиционно применяются модели, основанные на методе анализа иерархий (МАИ) [2]. Верхний слой отражает цель – оценку риска. Средний слой вводит правила для взвешивания факторов риска с аспектами вероятности и величины ущерба. Нижний слой перечисляет факторы риска в области сетевой безопасности, к которым относятся сетевые атаки, отказы устройств или несанкционированные действия, и т.д. Эти иерархии, состоящие из важнейших факторов для оценки риска ССМС с ИФ, полезны для систематических измерений сетевой безопасности. Тем не менее, неправильная настройка системы защиты является основной причиной уязвимости системы для БС, и известная трехслойная структура неполноценна при моделировании рисков сети.

Для моделирования риска БС предлагается применить методику МАИР с четырьмя слоями: риск, требования, атаки, и настройки.

1) Слой риска: первый слой содержит только корневой узел, представляющий величину риска ССМС с ИФ, который возникает в случае, если требования к безопасности сети не достигнуты.

2) Слой свойств информации: на втором слое МАИР определяются требования к безопасности информации: конфиденциальность, целостность и доступность:

– конфиденциальность оказывается под угрозой, когда информация становится доступна или передается неавторизованному пользователю. Разнообразные атаки направлены на достижение множества целей. Например, атаки прослушивания реализуются с целью нарушения конфиденциальности трафика сети, в то время как атака получения несанкционированного доступа приводит к нарушению конфиденциальности данных, которые находятся в памяти и не участвуют в непосредственном обмене. В данной работе, потеря конфиденциальности может произойти вследствие разнообразных причин, которые зависят от типов реализуемых атак;

– нарушение целостности происходит, если данные или сообщения были выполнены, изменены, приостановлены, скопированы, повторены или удалены нелегальным пользователем. Поскольку нарушители могут быть заинтересованы в атаке различных объектов, таких как сетевой трафик или сохраненные данные, целостность, рассматриваемая в рамках модели, меняет содержание в зависимости от типа атаки;

– доступность в первую очередь определяется тем, зависит ли от потенциальных атак функционирование услуги или возможность доступа авторизованного пользователя к сетевой услуге, которая ему необходима. Считается, что доступность находится под угрозой, если услуга или сервер были фальсифицированы, взломаны или приостановлены, и не могут

функционировать, как ожидается.

3) Слой атак: третий слой (слой атак) в МАИР представляет атаки, которые могут нарушить требования безопасности, перечисленные во втором слое. Атака может представлять разнообразные воздействия на рассматриваемые требования к безопасности, которые имеют конкретные особенности при воздействии на различные объекты, такие как полоса пропускания, сетевой трафик, приложения или ПК. Соответственно различные объекты могут быть подвержены различным рискам, даже если они подвержены одной и той же атаке. Например, атака эффективная при воздействии на пропускную способность сети, очевидно, терпит неудачу при попытке атаковать приложения. В предлагаемой модели, в слое атак рассмотрены атаки, не только с точки зрения их поведения, но и воздействия в отношении объектов атаки, и требований безопасности. Поскольку, ущерб от атак варьируется в зависимости от последовательности их применения, определим два типа воздействия: прямые, и косвенные, чтобы выразить зависимость от последовательности реализации атак:

– прямой эффект: воздействие направленно на конкретное требование к безопасности, которое первоначально является целью атаки;

– косвенный эффект: воздействие является побочным эффектом, сопровождающим прямое воздействие от реализованной атаки.

Например, атака прослушивания реализует угрозу конфиденциальности трафика путем несанкционированного анализа трафика сети. Она предназначена для прямого влияния на конфиденциальность трафика и других целей, например, файлов или приложений, но вместе с тем, пакеты, перехваченные нарушителем, могут быть необходимы для последующей атаки ретрансляции пакетов, которая ставит под угрозу целостность трафика. Таким образом, результаты атаки прослушивания оказывают косвенное влияние на целостность трафика. При оценке воздействия, вызванного атакой, должны совместно рассматриваться прямое и косвенное воздействие.

Анализ существующих атак на БС позволяет классифицировать их на пять типов по поведению и намерениям [2], в том числе атаки сканирования или мониторинга, ложной идентификации, отказа в обслуживании (DoS), взлома ключей и атаки НСД:

– Тип I: Атаки сканирования или мониторинга. Атаки сканирования реализуют попытки поиска доступных БС и направлены на получение полезной информации из сети жертвы путем перехвата пакетов и анализа сетевого трафика БС. Данный тип атак включает в себя подслушивание, атаки активной разведки и т.д. Поскольку атаки типа I пытаются получить важную информацию, большинство атак этого типа напрямую влияют на конфиденциальность трафика.

– Тип II: Атаки ложной идентификации. Нарушитель маскируется под законного пользователя с целью: доступа к БС, генерации несанкционированного трафика, отключения функционирования БС. Как только атакующий успешно завладевает идентификатором потерпевшего, жертва не может уже получить доступ в сеть, а атакующий способен предоставлять услуги сети для других незаконных пользователей. Этот тип атаки непосредственно влияет на доступность. Замаскированный пользователь с поддельным идентификатором может легко перехватить или получить личную информацию пользователя, так что, как правило, затрагиваются и конфиденциальность и целостность.

– Тип III: DoS-атаки. Атаки типа отказ в обслуживании (DoS) нацелены на достижение состояния временной недоступности услуг для легальных абонентов. Нарушители используют этот период временной парализации для реализации других атак, которые могут серьезно нарушить сетевую безопасность. Поскольку после реализации атак этого вида запросы пользователей на обслуживание отклоняются, то можно сделать вывод о том, что прямое воздействие осуществляется на доступность.

– Тип IV: Взлом ключа. Атаки взлома ключей пытаются выявить ключи шифрования, путем анализа

многочисленных пакетов сети. После взлома ключа шифрования, нарушаются все требования безопасности (конфиденциальность, целостность и доступность).

– Тип V: Атаки НСД. Атаки типа НСД – это попытки не санкционированного доступа в систему жертвы через уязвимости системы. После успешной реализации такой атаки, нарушитель получает доступ ко всем услугам и таким образом нарушается конфиденциальность данных, целостность или доступность.

4) Уровень настроек: Для реализации некоторых атак на БС, нарушитель должен предварительно получить определенную информацию о сети или настройках устройств. В МАИР, четвертый слой (слой настроек) представляет конфигурации устройств и БС. При необходимости этот слой можно расширить.

Интегрированная метрика истории уязвимости

Предлагаемая методика оценки риска определяет новую меру уязвимости – интегрированную метрику истории уязвимости (ИМИУ), которая позволяет оценить степень уязвимости устройства.

Метрика истории уязвимости (МИУ) отражает степень уязвимости и представляет собой оценку уязвимости с точки зрения ее возраста [1]. Предполагается, что уязвимости, обнаруженные давно, должны иметь небольшой вес, потому что с течением времени с большой вероятностью уязвимость может быть выявлена и исправлена. Таким образом, возраст уязвимости представляется с помощью убывающей экспоненциальной функции (1)

$$hvm(s) = \ln\left(1 + \sum_{i=1}^{n_v} \alpha_i \cdot e^{-\beta \cdot \lambda_i}\right). \qquad (1)$$

где s – анализируемое приложение;

n_v – количество анализируемых уязвимостей;

α_i – весовой коэффициент i-ой уязвимости;

β – интенсивность атак через i-ую уязвимость;

λ_i – возраст i-ой уязвимости.

Величина *hvm(s)* имеет смысл вероятности того, что услуга будет иметь данные уязвимости в будущем.

Соответственно в рассмотрение могут браться не все уязвимые службы, поскольку эффективность уязвимостей с возрастом обычно снижается. Таким образом, если учитывать только последние *n* уязвимостей услуг, то из $hvm(s)$ может быть получен показатель $\overline{hvm}(s)$, как представлено в формуле (2):

$$\overline{hvm}(s) = \frac{hvm(s)}{\ln(1+10n)}, \tag{2}$$

где $0 \le \overline{hvm}(s) \le 1$.

Комбинация *hvm* для всех служб, работающих на некотором устройстве *dev* определяется с помощью агрегированной МИУ (АМИУ) [1]. АМИУ полезна для оценки уязвимостей угрожающих устройству *dev*:

$$ahvm(dev) = \ln\left(\sum_{i=1}^{n_s} e^{hvm(s_i)}\right), \tag{3}$$

где s_i – приложения, запущенные на устройстве *dev*;

n_s – количество приложений запущенных на устройстве *dev*.

Однако если уязвимости не обнаружены в *dev*, АМИУ принимает неопределенное значение ln(0). Для устранения этой неопределенности, предлагается новая интегрированная метрика

(ИМИУ) основанная на рассмотренной четырехуровневой модели оценки риска.

В ИМИУ предлагается обеспечить наличие граничных значений. Метрика, рассчитанная по ИМИУ, обозначена как *ihvm* (формула 4), а ее нормированное значение обозначено через $\overline{ihvm}$ и рассчитывается по формуле (5)

$$ihvm(dev) = \ln\left(1 + \sum_{i=1}^{n_s} e^{\overline{hvm}(s_i)}\right). \quad (4)$$

где s_i – приложения, запущенные на устройстве *dev*;

n_s – количество приложений, запущенных на устройстве *dev*.

Чем выше значение *ihvm*, тем больший ущерб потенциально может быть нанесен устройству запущенными службами. Если службы не запущены на устройстве *dev*, то показатель *ihvm(dev)* будет равен 0. После ранжирования $\overline{hvm}(s_i)$, $\forall s_i$ приложения запущенного на устройстве *dev*, можно рассматривать только *m* наибольших значений $\overline{hvm}(s_i)$, при этом максимальным значением *ihvm(dev)* будет $\ln\ 1 + me^1$.

Таким образом, можно вычислить меру уязвимости $\overline{ihvm}(dev)$ для одного устройства в соответствии с уязвимостями запущенных на нем приложений по формуле (5):

$$\overline{ihvm}(dev) = \frac{ihvm(dev)}{\ln(1 + me^1)}. \quad (5)$$

В результате, гарантируется, что величина $\overline{ihvm}(dev)$ попадает в диапазон [0, 1].

Предложенную метрика используется для численной оценки мер уязвимости настроек СЗ для приложений запущенных на каждом устройстве, необходимых для формирования соответствующих векторов приоритетов в иерархической модели исследуемой системы.

Алгоритм численной оценки риска

Рассмотрим алгоритм расчета предлагаемой меры оценки риска БС, который представляет собой пошаговый процесс. Ниже подробно рассмотрен каждый шаг, необходимый для расчета численной величины.

Шаг 1. Формирование модели риска.

Первоначально, необходимо создать МАИР. Для создания четырехслойной иерархической структуры в контексте оценки риска, необходимо сформировать и проанализировать множество возможных угроз объекту защиты и атак, реализующих эти угрозы. В соответствие с классификацией [1], выделяются классы угроз, и в каждом классе рассматриваются наиболее актуальные атаки, реализующие данные угрозы. Тогда на основании этих сведений может быть разработана риск-модель. Целью является получение оценки риска нанесения ущерба элементу сети, которая учитывает настройки системы защиты в условиях воздействия наиболее актуальных на текущий момент атак. На основании представленных результатов анализа данных формируется иерархическая структура, а также оценивается размерность матрицы, которая формируется для каждого устройств подверженного атакам N видам атак на M свойств информации. В результате могут быть получены матрицы размером $N \times 3$, поскольку анализируются три основных свойства информации.

Шаг 2. Разработка таблиц соответствия.

Поскольку БС имеют определенную область применения, то требования к безопасности и риски могут существенно от нее зависеть. Целью этого шага является анализ имеющихся данных, которые учитывают одновременно множество факторов для получения сценарийно-адаптивной оценки. Чтобы обеспечить

адекватную или близкую к адекватной оценку, необходимо проводить опрос группы экспертов. В предлагаемой методике, отображение опыта в таблицы соответствия осуществляет студентом самостоятельно, учитывая доступный в открытых источниках мировой опыт. На этом этапе формируются таблицы соответствия для:

1) отображения опыта эксперта в численные оценки,

2) определения мер уязвимости настроек СЗ для каждого устройства,

3) определение вероятности раскрытия параметров настроек СЗ,

4) сопоставление каждой мере численного значения.

Данный шаг включает в себя следующие этапы:

- задание численно-лингвистического преобразования;
- определение мер уязвимости настроек СЗ на устройстве по одному из критериев:

1) Нестандартность конфигурации. Устройство уязвимо, если оно использует значения конфигурации принятые по умолчанию. Если администратор оставляет стандартные настройки, и не меняет их периодически, то злоумышленник может легко их скомпрометировать. Следовательно, такие настройки рассматриваются как уязвимые.

2) Количество эффективных атак. Злоумышленник для успешной реализации атаки нуждается в определенных настройках на целевом устройстве. Такую атаку можно охарактеризовать как эффективную при данной конфигурации. Степень уязвимости настройки СЗ возрастает с сростом количества априори эффективных против нее атак.

3) Значение ИМИУ.

Шаг 3. Оценка риска сети.

1) Оценка векторов приоритетов $\hat{p}$, и $\hat{r}$.

В соответствии с сетевыми настройками, опытом экспертов, и базой данных уязвимостей, оцениваются векторы приоритетов $\hat{p}$, и $\hat{r}$, где $\hat{p}$ – определяется экспертно на основании используемого в БС метода шифрования, а $\hat{r}$ определяется тремя аспектами описанными выше.

2) Вычисляется вектор приоритетов конфигураций $\hat{w}_g$.

Мы можем вычислить *i*-й элемент вектора $\hat{w}_g$ для атаки A_i по формуле (6):

$$w_{g_i} = \frac{\sum_{j=1}^{n_a} r_j \cdot p_j}{n_a}. \qquad (6)$$

где n_a – количество атак.

Если не требуется какая-либо особая настройка для реализации, w_{g_i} устанавливается в 1, которая является максимальным приоритетом.

2) Вычисляется вектор приоритетов свойств информации $\hat{w}_r$.

Значение каждого элемента $\hat{w}_r$ определяется с точки зрения функциональных возможностей устройства. Например, вес показателя доступности ИФ должен быть больше, чем показателей конфиденциальности и целостности, потому что основной задачей ИФ является предоставление мобильным устройствам доступа к услугам, таким образом, для ИФ $w_r = 1/4, 1/4, 1/2^T$.

4) Оценка показателя риска для каждого элемента *I(dev).*

Так как в случае возрастания количества атак направленных на устройство снижается уровень его защищенности, размерность *I(dev)* была задана на основе размерности матрицы $\widehat{w}_g$, которая зависит от количества атак, направленных на устройство *dev*. Тогда получим оценку риска отдельного устройства в следующем виде:

$$I(dev) = w_g^T \times D \times w_r. \tag{7}$$

Поскольку все элементы матриц $\widehat{w}_g$, *D*, и $\widehat{w}_r$ находятся в диапазоне [0, 1], а сумма всех элементов $\widehat{w}_r$ равна 1, то *I(dev)* подпадает в диапазон $0, n_a$, где n_a – количество атак.

5) Вычисление интегрального показателя *Risk.*

Так как любое устройство в сети может поставить под угрозу безопасность всей сети, мы учитываем вклад каждого устройства в интегральной оценке риска (8).

$$Risk = \log_{10}\left(\sum_{i=1}^{n_d} 10^{I(dev_i)}\right), \tag{8}$$

где n_a – количество анализируемых элементов сети.

Ненадежное устройство или устройство с уязвимыми настройками системы защиты обычно рассматривается нарушителем как трамплин для реализации атак, поэтому максимальный из показателей $I(dev_i)$ доминирует в результирующей оценке (8), в то время как остальные меньшие по модулю значения также учитываются.

Методика построена таким образом, что значение *Risk* увеличивается, если риски сети возрастают. Показатель *Risk* зависит от количества устройств в сети, их настроек и

варьируется в зависимости от различных сетевых топологий. Если устройств в сети становится больше, максимально достижимое значение *Risk* становится больше. Таким образом, если в БС имеется n_d^{ap} точек доступа и n_d^{sta} беспроводных устройств, то показатель *Risk* будет находиться в следующем диапазоне $\left[\log_{10}(n_d^{ap}+n_d^{sta}),\ \log_{10}(n_d^{ap}10^{n_a^{ap}}+n_d^{sta}10^{n_a^{sta}})\right]$. Однако, показатель *Risk* очень чувствителен к изменениям параметров $n_d^{ap}, n_d^{sta}, n_a^{ap}$ и n_a^{sta}, так что задача интерпретации численных значений *Risk* может стать затруднительной.

Для упрощения интерпретации численных значений *Risk*, и анализа рисков в сети, предлагается таблица соответствия между численными значениями *Risk* и лингвистическими термами. Прежде всего, необходимо вычислить максимальный уровень риска для устройств в сети, а затем определить пороговые значения для низкого, среднего и высокого риска сети. В приведенном выше случае с n_d^{ap} точек доступа и n_d^{sta} беспроводных устройств, можно получить максимальные значения риска $I(AP_i)=n_a^{ap},\ \forall 1\le i\le n_d^{ap}$ и, $I(STA_j)=n_a^{sta},\ \forall 1\le j\le n_d^{sta}$ по формуле (8). Если все устройства имеют максимальное значение уровня риска, то в этой ситуации предполагается, что сеть, несомненно, является ненадежной, и абсолютно небезопасной. Тем не менее, не для каждой беспроводной сети требуются такие строгие условия. Если установлены очень жесткие условия, неожиданные события можно игнорировать, и не отслеживать в реальном времени неправильные настройки устройств. Таким образом, предлагается соответствие, приведенное в табл. 2, между численными значениями риска и логическими уровнями риска. Таблица соответствия отображает, как соотносятся максимальный уровень риска с количеством устройств в сети.

Таблица 2

Таблица соответствия численных оценок уровня риска и логических интерпретаций

Численная оценка риска беспроводной сети	**Логические значения**
$\left[\log_{10}\left(\frac{2n_d^{ap}}{3}\times 10^{\frac{n_a^{ap}}{2}}+\frac{2n_d^{sta}}{3}\times 10^{\frac{n_a^{sta}}{2}}\right),\log_{10}\left(n_d^{ap}\times 10^{n_a^{ap}}+n_d^{sta}\times 10^{n_a^{sta}}\right)\right]$	Высокий (незащищенная сеть)
$\left[\log_{10}\left(\frac{n_d^{ap}}{3}\times 10^{\frac{n_a^{ap}}{2}}+\frac{n_d^{sta}}{3}\times 10^{\frac{n_a^{sta}}{2}}\right),\log_{10}\left(\frac{2n_d^{ap}}{3}\times 10^{\frac{n_a^{ap}}{2}}+\frac{2n_d^{sta}}{3}\times 10^{\frac{n_a^{sta}}{2}}\right)\right]$	Средний
$\left[\log_{10}\left(n_d^{ap}+n_d^{sta}\right),\log_{10}\left(\frac{n_d^{ap}}{3}\times 10^{\frac{n_a^{ap}}{2}}+\frac{n_d^{sta}}{3}\times 10^{\frac{n_a^{sta}}{2}}\right)\right]$	Низкий (безопасная сеть)

6) Обновление текущего состояния топологии.

Если обнаружены новые устройства или новые настройки, необходимо обновить текущее состоянии сети. В предлагаемой методике, не требуется пересчитывать соответствующие показатели для всех устройств. Лицу, принимающему решение просто необходимо выполнить вспомогательные шаги с 1 по 5, чтобы определить уровень риска для нового устройства $I(dev_i)$, где dev_i – представляет собой новое устройство, вошедшее в сеть, или устройство, настройки которого были изменены. Тогда, интегральное значение риска БС может быть получено путем повторного выполнения шага 6 предложенного алгоритма.

Программная реализация алгоритма

Алгоритм оценки риска может быть реализован программного. На рис. 1 показана структура программной системы инструмента оценки рисков, состоящая из трех основных компонентов:

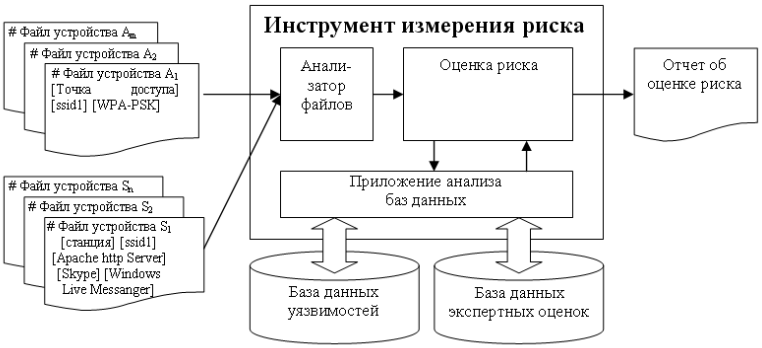

Рис. 1. Структура программной реализации алгоритма оценки рисков сети

– «Анализатор файлов устройств» предварительно обрабатывает файлы с перечнями настроек устройств и предоставляет параметры для модуля «Оценка риска», который вычисляет значение риска, и создает отчет об оценке риска. Файл настроек устройств содержит конфигурацию каждого устройства в сети, включая тип устройства, методы шифрования, запущенные службы;

– «Оценка риска», основа данного прикладного инструмента, и отвечает непосредственно за оценку риска;

– «Приложение анализа баз данных» отвечает за взаимодействие с базой данных и др. Оно предоставляет необходимую информацию об актуальных атаках на беспроводные сети, степени уязвимости настроек, вероятностях раскрытия настроек системы и других уязвимостях опубликованных в открытых источниках.

4. ПРИМЕР ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ

В данном разделе рассматривается несколько примеров. В каждом примере: формируется иерархическая структура, отражающая специфику сети в контексте обеспечения ее безопасности, задаются таблицы соответствия, необходимые для последующей оценки риска при использовании заданных настроек системы защиты, а также определяются вероятности раскрытия злоумышленником параметров настроек безопасности применяемой системы защиты.

Далее подробно рассматриваются все шаги составляющие процесс численной оценки риска на примере локальных беспроводных сетей.

Шаг 1: Разработка иерархической структуры

В соответствии с изложенным выше подходом, а также на основании сведений о классификации атак [2] может быть разработана риск-модель. Результаты анализа угроз и их проявлений для выбранного объекта защиты приведены в табл. 3. На основании представленных данных формируется иерархическая структура для рассматриваемых примеров (рис. 2).

Шаг 2: Разработка таблиц соответствия

Для расчета показателей риска необходимо использовать реальный мировой опыт, отражающий практическую специфику в области беспроводных технологий.

• Численно-лингвистические преобразования.

В табл. 4 продемонстрирован пример отображения 9 лингвистических термов в числовые значения из интервала [0, 1]. Величины, приведенные в табл. 4, могут быть скорректированы в зависимости от имеющегося опыта, условий функционирования и конфигурации сети.

• Меры уязвимости настроек системы защиты (СЗ) на устройстве.

Таблица 3

Анализ атак

Класс	**Атака**	**Объект атаки**	**Необходимые параметры**	**Прямое воздействие**	**Косвенное воздействие**
I	Вардрайвинг (A_1^{ap})	ТД	Нет	-	Д
	Перехват трафика (A_1^{sta})	БК	Нет	К	Ц, Д
	Активное сканирование(A_2^{ap})	ТД	Нет	К	Ц, Д
II	Фишинг (A_2^{sta})	БК	SSID (G_1)	К, Ц, Д	-
	MAC-спуфинг (A_3^{ap})	ТД	MAC-адрес БК (G_4)	Д	-
	IP-спуфинг (A_4^{ap})	ТД	IP-адрес БК (G_5)	Д	-
	«Человек посередине» (A_3^{sta})	БК	IP-адрес БК (G_5), IP-адрес ТД (G_3), открытые порты (G_6)	К, Ц, Д	-
III	Beacon-флуд (A_4^{sta})	БК	Нет	Д	-
	Флуд аутентификации (A_5^{ap})	ТД	SSID (G_1), MAC-адрес ТД (G_2)	Д	-
	Флуд деаутентификации(A_5^{sta})	БК	MAC-адрес БК (G_4)	Д	-
IV	Взлом WEP/WPA (A_6^{ap} , A_6^{sta})	БК, ТД	SSID (G_1), MAC-адрес ТД (G_2), канал (G_7)	К, Ц, Д	-
V	Атака НСД (A_7^{sta})	БК	IP-адрес БК (G_5), открытые порты (G_6), запущенные приложения (G_8)	К, Ц, Д	-

К: конфиденциальность; Ц: целостность; Д: доступность
ТД: точка доступа; БК: беспроводной клиент

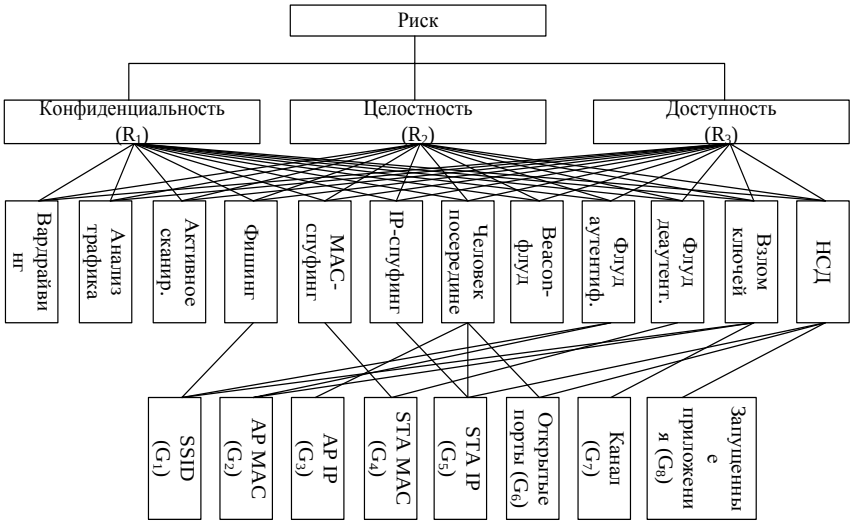

Рис. 2. Четырехуровневая иерархия оценки риска построенная для сетей из примера

Таблица 4

Таблица преобразования количества успешных реализаций атак в численные оценки уязвимости конфигурации средств защиты

Количество эффективных атак	**Лингвистический уровень уязвимости**	**Численная оценка уязвимости**
0	Самый низкий (СН)	0
0	Очень низкий (ОН)	0,1
0	Низкий (Н)	0,2
0	Довольно низкий (ДН)	0,3
1	Средний (С)	0,5
2-4	Довольно высокий (ДВ)	0,7
5-8	Высокий (В)	0,8
9-11	Очень высокий (ОВ)	0,9
12	Самый высокий (СВ)	1

Меры уязвимости настроек СЗ определяются по следующим критериям:

1) Нестандартность конфигурации. На рис. 2, конфигурации G_1 (SSID) и G_6 (открытые порты) – соответствуют «высокому» (В) уровню уязвимости, если используют настройки по умолчанию, в противном случае устанавливается «низкий» (Н) уровень уязвимости.

2) Количество эффективных атак. По данному критерию может быть определены меры уязвимости для настроек G_1, G_2, G_3, G_4, G_5, G_6, и G_7, представленных на рис. 2. В табл. 4 приведен пример отображения числа эффективных атак в численную оценку уязвимости.

3) Значение ИМИУ. Мера уязвимости конфигурации G_8 (запущенных приложений) может быть определена по формуле (4) предыдущего раздела.

Существует возможность изменения принципа преобразования числа эффективных атак в меры уязвимости настроек в соответствии с мировым опытом и динамикой процессов в конкретной беспроводной сети. В табл. 5 приведены уязвимости некоторых приложений, степень их опасности, и возраст, которые могут быть получены из открытых баз данных. В последнем столбце приведены вычисленные по формуле (1) значения *hvm(s)* при $\beta = 1$ для каждого приложения, которое может быть запущено на устройстве.

• вероятность раскрытия параметров настроек

Вероятность определения нарушителем параметров настроек системы защиты существенно зависит от метода шифрования используемого в беспроводной сети. Например, для расшифровки пакетов зашифрованных методом WEP или WPA требуются различные усилия. Тем не менее, в некоторых случаях, злоумышленник может определить некоторые настройки, которые не могут быть защищены применяемым методом шифрования.

Таблица 5

Уязвимости приложений по данным базы данных NVD

Запущенное приложение (s)	**Уязвимости**	**Тяжесть (α_i)**	**Возраст (λ_i)**	***hvm(s)***
Windows Live Messenger	CVE-2010-0278	4,3	0,32	2,3951
	CVE-2009-2544	6,8	0,81	
	CVE-2009-0647	5,0	1,24	
	CVE-2008-5828	5,0	1,37	
	CVE-2008-5179	5,0	1,49	
Wireshark	CVE-2010-0304	7,5	0,25	3,2299
	CVE-2009-4378	4,3	0,37	
	CVE-2009-4377	4,3	0,37	
	CVE-2009-4376	9,3	0,37	
	CVE-2009-4211	9,3	0,42	
Skype	CVE-2009-4741	10	0,11	2,8013
	CVE-2009-4567	3,5	0,33	
	CVE-2009-5697	4,2	1,37	
	CVE-2009-4875	6,8	1,51	
	CVE-2009-1805	9,3	1,92	
FireFtp	CVE-2009-3478	6	0,6	1,7242
	CVE-2008-2399	9,3	1,96	

На основании анализа конфигурации, представленной на рис. 2, в табл. 6 приводится пример оценки вероятности получения настроек при различных методах шифрования.

• степень воздействия.

Деструктивные воздействия на основные свойства циркулирующей в сети информации можно условно разделить на три уровня: прямые, косвенные, и отсутствующие. На основании имеющегося опыта каждому воздействию может быть назначено численное значение. В данном примере значения 1; 0,5; и 0 – назначены для прямого, косвенного, и отсутствующего воздействия соответственно. Тогда, в соответствии с табл. 2 формируются матрицы для всех устройств подверженных атакам. Поскольку 6 атак ориентированы на точки доступа, и 7 атак направлены против беспроводных клиентов, могут быть получены матрицы 6 × 3, и 7 × 3 соответственно, что представлено формулой 1.

Таблица 6

Вероятность получения нарушителем параметров настроек СЗ

Метод шифрования	**Вероятность**		**Уязвимые конфигурации**
	Лингвистическая	**Численная**	
Нет шифрования	СВ	1	G_1, G_2, G_3, G_4, G_5, G_6, G_7, G_8
WEP	СВ	1	G_1, G_2, G_4, G_7
	С	0,5	G_3, G_5, G_6, G_8
WPA-PSK, WPA2-PSK	СВ	1	G_1, G_2, G_4, G_7
	Н	0,2	G_3, G_5, G_6, G_8
WPA-EAP TLS, WPA-EAP AES	СВ	1	G_1, G_2, G_4, G_7
	ОН	0,1	G_3, G_5, G_6, G_8

По определению, каждый элемент матрицы представляет собой степень воздействия реализованной атаки на конкретное свойство информации. Так как в предлагаемом алгоритме рассматриваются три свойства информации:

конфиденциальность, целостность и доступность, то каждая строка матрицы состоит из трех элементов, как показано в формуле (9) . Например, вардрайвинг (A_1^{ap}) оказывает только косвенное влияние на доступность точки доступа, поэтому первая строка D_{AP} имеет вид [0 0 0,5]

$$D_{AP} = \begin{bmatrix} 0 & 0 & 0,5 \\ 1 & 0,5 & 0,5 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix} D_{STA} = \begin{bmatrix} 1 & 0,5 & 0,5 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \quad (9)$$

Шаг 3: Оценка риска сети

Пример I: Атака прослушивания

В первом примере, проводятся два эксперимента (Эк1-1 и Эк1-2) с одинаковыми по топологии беспроводными сетями: одной точкой доступа, и двумя беспроводными клиентами. Клиент STA_1 использует приложение Windows Live Messenger, а клиент STA_2 пытается анализировать трафик STA_1, с помощью Wireshark. В первом эксперименте Эк1-1 не применяются никакие механизмы защиты, а во втором эксперименте Эк1-2 вводится шифрование WPA2-PSK для защиты сетевого трафика. Благодаря различиям в конфигурациях, станция STA_2 успешно подслушивает трафик станции STA_1 в Эк1-1, но не в состоянии перехватить пакеты станции STA_1 по MSN в Эк1-2. На рис.3 продемонстрированы условия и результаты эксперимента для примера I.

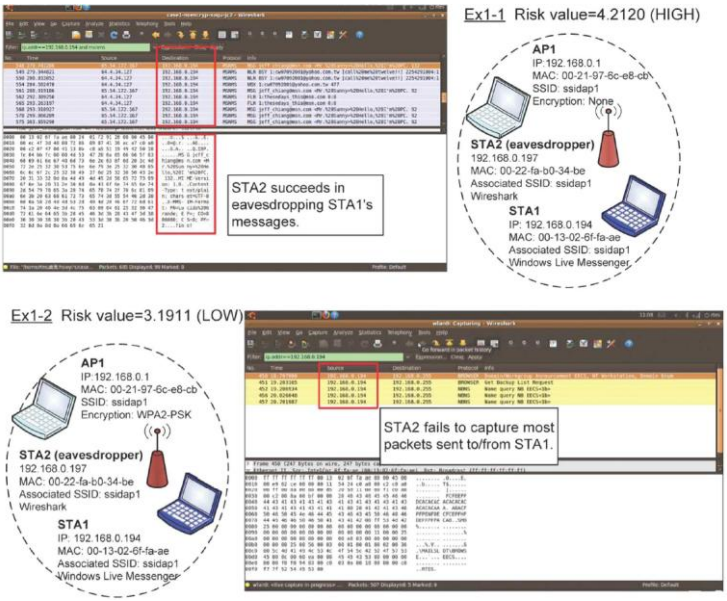

Рис. 3. Пример 1. В Эк1-1 не применяется никакого механизма обеспечения безопасности, а в Эк1-2 сеть защищена с помощью WPA2-PSK

Проведем оценку интегрального риска для каждой из анализируемых сетей с помощью, предложенного алгоритма.

1) Определение $\hat{r}$ и $\hat{p}$.

(a) Меры уязвимости для настроек G_1 и G_6 должны быть определены по критериям 1) нестандартности конфигурации и 2) количеству эффективных атак. В этом примере G_1 не принимает значения по умолчанию, и, следовательно, ей присваивается «Низкий» (Н) уровень уязвимости. Кроме того, конфигурация G_1 является необходимым условием для реализации трех видов атак, в том числе фишинговой атаки, атаки флуда аутентификации и атаки взлома ключа шифрования. Согласно таблице 3 может быть назначен «достаточно высокий» (ДВ) уровень уязвимости. В итоге, лингвистические уровни уязвимости преобразуются в численные оценки, из которых выбирается максимальное значение для G_1, max(0,2;0,7). Таким

же образом, может быть получен уровень риска G_6, max(0,8;0,7)=0,8 исходя из предположения, что настройки по умолчанию адаптированы для G_6.

(b) уровни уязвимости G_2, G_3, G_4, G_5 и G_7 определяются по количеству эффективных атак. Например, настройка G_2 необходима для реализации двух атак, и его уровень риска устанавливается в «ДВ», который эквивалентен величине 0,7.

(c) Уровень риска G_8 определяется по ИМИУ. В этом примере на STA_1 запущено приложение Windows Live Messenger (s_1), на $STA_{\backslash 2}$ запущено приложение Wireshark (s_2), а на точке доступа AP_1 приложения не запущены. Согласно сведениям из открытой базы данных NVD, известно 8 уязвимостей в Windows Live Messenger, и 93 уязвимости в Wireshark. В таблице 4 представлено по пять самых актуальных уязвимостей для каждого приложения. Если рассматривать только новейшие 5 уязвимостей для каждого приложения, и учитывает три самых высоких показателя $hvm(s_i)$ в *ihvm*, то в силу (1), (2), (4) и (5), можно оценить, что $\overline{ihvm}(AP_1)=0$, а $\overline{ihvm}(STA_1)$ и $\overline{ihvm}(STA_2)$ рассчитываются, как показано ниже.

s_1: Windows Live Messenger

$$\overline{hvm}(s_1)=\frac{2,3951}{\ln(1+10\cdot 5)}=0,6092,$$

$$ihvm(STA_1)=\ln\ 1+e^{\overline{hvm}(s_1)}\ =1,0434,$$

$$\overline{ihvm}(STA_1)=\frac{ihvm(STA_1)}{\ln(1+3\cdot e^1)}=0,4712.$$

s_2: Wireshark

$$\overline{hvm}(s_2)=\frac{3,2299}{\ln(1+10\cdot 5)}=0,8215,$$

$$ihvm(STA_2) = \ln\ 1 + e^{\overline{ihvm}(s_2)}\ = 1{,}1860,$$

$$\overline{ihvm}(STA_2) = \frac{ihvm(STA_2)}{\ln(1+3\cdot e^1)} = 0{,}5356.$$

Тогда получим меры уязвимости настроек СЗ для каждого элемента сети AP_1, STA_1, и STA_2 в обоих экспериментах Эк1-1 и Эк1-2.

$$r_1^{AP_1} = \begin{matrix} 0{,}7 & 0{,}7 & 0{,}5 & 0{,}7 & 0{,}7 & 0{,}8 & 0{,}5 & 0 \end{matrix}^T, \quad (10)$$

$$r_1^{STA_1} = \begin{matrix} 0{,}7 & 0{,}7 & 0{,}5 & 0{,}7 & 0{,}7 & 0{,}8 & 0{,}5 & 0{,}4712 \end{matrix}^T \quad (11)$$

$$r_1^{STA_2} = \begin{matrix} 0{,}7 & 0{,}7 & 0{,}5 & 0{,}7 & 0{,}7 & 0{,}8 & 0{,}5 & 0{,}5356 \end{matrix}^T. \quad (12)$$

Вероятность раскрытия конфигураций ($\hat{p}$) определяется путем анализа табл. 6 и 4. В итоге оценивается $\hat{p}_{11}$ для Эк1-1 (шифрование не применяется):

$$\hat{p}_{11} = \begin{matrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{matrix}^T, \quad (13)$$

Для Эк1-2 (применяется WPA2-PSK шифрование)

$$p_{12} = \begin{matrix} 1 & 1 & 0{,}2 & 1 & 0{,}2 & 0{,}2 & 1 & 0{,}2 \end{matrix}^T. \quad (14)$$

2) Вычисляется вектор приоритетов конфигураций $\hat{w}_g$ для AP_1, STA_1, и STA_2 по формуле (6).

В Эк1-1:

$$\hat{w}_{g_{11}}^{AP_1} = \begin{matrix} 1 & 1 & 0{,}7 & 0{,}7 & 0{,}7 & 0{,}6333 \end{matrix}^T,$$

$$\widehat{w}_{g_{11}}^{STA_1} = 1 \quad 0,7 \quad 0,6667 \quad 1 \quad 0,7 \quad 0,6333 \quad 0,6571^{T},$$

$$\widehat{w}_{g_{11}}^{STA_2} = 1 \quad 0,7 \quad 0,6667 \quad 1 \quad 0,7 \quad 0,6333 \quad 0,6785^{T} \quad (15)$$

В Эк1-2:

$$w_{g_{12}}^{AP_1} = 1 \quad 1 \quad 0,7 \quad 0,14 \quad 0,7 \quad 0,6333^{T},$$

$$w_{g_{12}}^{STA_1} = 1 \quad 0,7 \quad 0,1333 \quad 1 \quad 0,7 \quad 0,6333 \quad 0,1314^{T},$$

$$w_{g_{12}}^{STA_2} = 1 \quad 0,7 \quad 0,1333 \quad 1 \quad 0,7 \quad 0,6333 \quad 0,1357^{T}. \quad (16)$$

3) Вычисляется вектор приоритетов свойств информации $\widehat{w}_r$ для каждого сетевого устройства. Например, «доступность» точки доступа должна иметь больший приоритет, чем «конфиденциальность» и «целостность», потому что АР отвечает за предоставление доступа в интернет для беспроводных устройств. Следовательно, в Эк1-1 и Эк1-2, имеем

$$\widehat{w}_{r_1}^{AP_1} = \left[\frac{1}{4} \quad \frac{1}{4} \quad \frac{1}{2}\right]^{T}. \quad (17)$$

С другой стороны, конфиденциальности, целостность и доступность могут иметь одинаковые приоритеты для беспроводной станции, так что

$$\widehat{w}_{r_1}^{STA_1} = \left[\frac{1}{3} \quad \frac{1}{3} \quad \frac{1}{3}\right]^{T}. \quad (18)$$

4) Рассчитывается величины рисков для каждого элемента. По формулам (7), (9), (15-18), получаем

$$I_{11}(AP_1) = w_{g_{11}}^{AP_1} \times D_{AP} \times w_{r_1}^{AP_1} = 2,5583,$$

$$I_{11}(STA_1) = w_{g_{11}}^{STA_1} \times D_{STA} \times w_{r_1}^{STA_1} = 3{,}8904,$$
$$I_{11}(STA_2) = w_{g_{11}}^{STA_2} \times D_{STA} \times w_{r_1}^{STA_2} = 3{,}9118.$$

Аналогично, рассчитываются величины рисков для каждого устройства в Эк1-2: $I_{12}(AP_1) = 2{,}2783$, $I_{12}(STA_1) = 2{,}8313$, и $I_{12}(STA_2) = 2{,}8356$.

5) Определяется интегральное значение риска по формуле (8). Для Эк1-1 получается значение риска $Risk_{11} = \log_{10}(10^{2{,}5583} + 10^{3{,}8904} + 10^{3{,}9118}) = 4{,}212$, и $Risk_{12} = \log_{10}(10^{2{,}2783} + 10^{2{,}8313} + 10^{2{,}8356}) = 3{,}1911$ для Эк1-2 соответственно. Согласно табл. 3, показатель риска в Эк1-1 попадает в категорию высокого, потому что больше, чем верхний порог 3,6887. Аналогично, в Эк1-2 показатель риска попадает в категорию низкого, потому что меньше, чем средний порог 3,3877. Такой результат адекватен реальности, потому что в случае большего значения риска, атака анализа трафика была успешно реализована, а в случае с меньшим значением риска система защиты в сети эффективно противостояла атаке.

Пример II: Динамическая топология.

Во втором примере демонстрируется, как алгоритм оценки риска учитывает динамичность топологии беспроводной сети. В примере представлены состояния беспроводной сети в моменты времени τ_1, τ_2 и τ_3. Первоначально (в момент времени τ_1), сеть состоит из одной точки доступа, и двух станций STA. Затем в момент времени τ_2 новая станция STA_3 подключается к сети. И, наконец, в момент времени τ_3 станция STA_1, отключается от сети. На рис. 4 представлены топологии сети, и конфигурации устройств. С помощью предлагаемого подхода, становится возможным управление беспроводной сетью в динамике, а также эффективная оценка риска сети путем выполнения следующих шагов.

Первоначально, в момент времени τ_1 две сети в Эк1-2 и Эк2-1 в точности одинаковые, получаем интегральную оценку риска $Risk_{21}$=3,1911 равную $Risk_{12}$.

В момент τ_2: STA_3 присоединяется к беспроводной сети (как показано на рис. 4) в момент времени τ_2. Поскольку никаких изменений не было внесено в AP_1, STA_1 и STA_2, не требуется пересчитывать соответствующие показатели рисков, но необходимо выполнить следующие шаги.

1) определить уровень уязвимости конфигурации СЗ на STA_3, $\hat{r}_{22}^{STA_3}$. Предположим, что STA_3 использует приложение Windows Live Messenger (s_1), Skype (s_2), и FireFTP (s_3); и берутся в рассмотрение только последние пять уязвимостей каждого приложения.

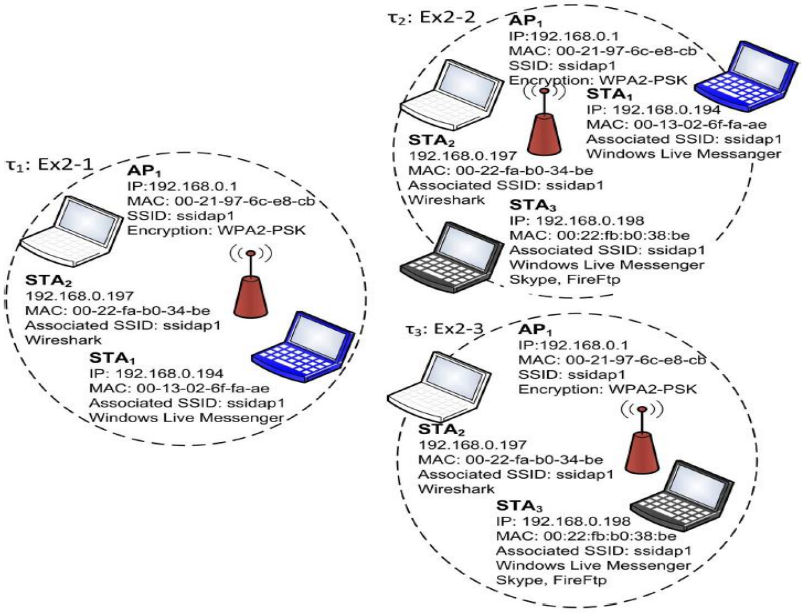

Рис. 4. Пример 2. Состояние параметров беспроводной сети в различное время

По данным об уязвимостях приложений перечисленных в табл. 5, вычисляется $\overline{hvm}(s_i)$, $i \in 1,3,4$, по (1) и (2), а затем вычисляется $\overline{ihvm}(STA_3)$ в соответствии с $\overline{hvm}(s_i)$ по формулам (2) и (4), как показано ниже.

$$\overline{hvm}(s_1) = \frac{2,3951}{\ln(1+10\cdot 5)} = 0,6092 \text{ s}_1\text{: Windows Live Messenger,}$$

$$\overline{hvm}(s_3) = \frac{2,8013}{\ln(1+10\cdot 5)} = 0,7125 \text{ s}_3\text{: Skype,}$$

$$\overline{hvm}(s_4) = \frac{1,7242}{\ln(1+10\cdot 5)} = 0,4385 \text{ s}_4\text{: FireFTP,}$$

$$ihvm(STA_3) = 1,8607,$$

$$\overline{ihvm}(STA_3) = 0,8403.$$

Таким образом, получаем

$$\hat{r}_{22}^{STA_3} = \begin{matrix} 0,7 & 0,7 & 0,5 & 0,7 & 0,7 & 0,8 & 0,5 & 0,8403 \end{matrix}^T.$$

Поскольку в Эк2-2 по-прежнему используется WPA2-PSK шифрование, вероятность раскрытия настроек остается той же, где $p_{22} = p_{21} = p_{12}$.

2) Определяется вектор приоритетов конфигураций STA_3, $\hat{w}_{g_{22}}^{STA_3}$ по формуле (6), и получается

$$\hat{w}_{g_{22}}^{STA_3} = \begin{matrix} 1 & 0,7 & 0,1333 & 1 & 0,7 & 0,6333 & 0,1560 \end{matrix}^T.$$

3) Формируется вектор приоритетов свойств информации. В этом примере применяется тот же, что и приведенный в примере I вектор $\hat{w}_r$.

4) Оценивается показатель риска для STA_3: $I_{22}(STA_3) = 2{,}8559$.

5) Рассчитывается интегральный показатель риска T_{22}, из $I_{22}(AP_1)$, $I_{22}(STA_1)$, $I_{22}(STA_2)$, и $I_{22}(STA_3)$. В силу (8), получается

$$Risk_{22} = \log_{10}(10^{2,2783} + 10^{2,8313} + 10^{2,8356} + 10^{2,8559}) = 3{,}3561.$$

В Эк2-2 по сравнению с экспериментом Эк2-1 имеется больше устройств и, следовательно, уязвимостей, а значит $Risk_{22}$ больше $Risk_{21}$.

В момент времени τ_3 STA_1 покидает сеть и для других устройств ничего не меняется. Соответственно можно определить величину риска в τ_3 путем перерасчета T_{23} с известными показателями $I_{22}(AP_1)$, $I_{22}(STA_2)$, и $I_{22}(STA_3)$. В результате получается

$$Risk_{23} = \log_{10}(10^{I_{23}(AP_1)} + 10^{I_{23}(STA_2)} + 10^{I_{23}(STA_3)}) = 3{,}2020,$$

где $I_{23}(AP_1) = I_{22}(AP_1)$, $I_{23}(STA_2) = I_{22}(STA_2)$, и $I_{23}(STA_3) = I_{22}(STA_3)$.

В результате получены интегральные оценки для Эк1-1, и Эк1-2: $Risk_{11}$=4,2120 (высокий риск), и $Risk_{12}$=3,1911 (низкий риск), соответственно. Поскольку в Эк1-1 нет механизма обеспечения безопасности, а атака подслушивания будет успешно реализована, то логично, что результат оценки подразумевает высокий риск. Кроме того, низкое значение риска также соответствует реальной ситуации, потому что атака прослушивания потерпит неудачу, когда сеть в Эк1-2 находилась под защитой.

Таким образом, предложенный алгоритм позволяет осуществлять практическую оценку риска беспроводной сети.

5. ЗАДАНИЯ КУРСОВОЙ РАБОТЫ

5.1. Общая часть

Выполнить программную реализацию инструмента для выполнения циклического анализа эффективности средств защиты информации беспроводной сети от угроз нарушения ее конфиденциальности, целостности и доступности, путем реализации предложенной методики оценки риска (на основе четырехслойного метода анализа иерархий и оригинального алгоритма оценки риска как расширенной метрики истории уязвимости).

5.2. Индивидуальные варианты заданий

Используя те же, что и в рассмотренном примере конфигурации беспроводных сетей выполнить расчет показателей риска, рассматривая только новейшие N mod 5 уязвимостей для каждого приложения, где N – первая цифра в номере зачетки, а mod – операция деления по модулю.

5.3. Контрольные вопросы

1. В чем преимущество структурной модели риска на основе метода анализа иерархий?
2. Из каких слоев состоит четырехслойная модель?
3. Что собой представляет метрика истории уязвимости?
4. Чем отличается интегрированная метрика истории уязвимости?
5. Каким образом определяется вектор приоритетов конфигураций?
6. Назовите наиболее опасные угрозы безопасности беспроводных сетей.
7. Перечислите средства защиты информации беспроводной сети от угроз нарушения ее конфиденциальности, целостности и доступности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Щербаков, В. Б. Риск-анализ атакуемых беспроводных сетей [Текст]: vонография / В. Б. Щербаков, С. А. Ермаков, Н. С. Коленбет; под ред. чл.-корр. РАН Д. А. Новикова. – Воронеж: Издательство «Научная книга», 2013. – 160 с.

2. Щербаков, В. Б. Безопасность беспроводных сетей: стандарт IEEE 802.11 [Текст] / В. Б. Щербаков, С. А. Ермаков; под ред. В. И. Борисова. – М. : РадиоСофт, 2010. – 256 с.

3. Защита беспроводных телекоммуникационных систем [Текст]: учеб. пособие [Электронный ресурс]/ В. Б. Щербаков, А. В. Гармонов, С. А. Ермаков, Н. С. Коленбет. – Воронеж: ФГБОУ ВПО «Воронежский государственный технический университет», 2013. – электрон. опт. диск.

СОДЕРЖАНИЕ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

к курсовому проектированию
по дисциплине «Беспроводные системы связи
и их безопасность»
для студентов специальности 090302
«Информационная безопасность
телекоммуникационных систем»
очной формы обучения

Составитель
Ермаков Сергей Александрович

В авторской редакции

Подписано к изданию 27.04.2015.

Уч.-изд. л. 2,3.

ФГБОУ ВПО «Воронежский государственный
технический университет»
394026 Воронеж, Московский просп., 14