В.Б. Щербаков, С.А. Ермаков, Н.С. Коленбет

РИСК-АНАЛИЗ АТАКУЕМЫХ БЕСПРОВОДНЫХ СЕТЕЙ

Монография

Под редакцией члена-корреспондента РАН
Д.А. Новикова

Воронеж
Издательство «Научная книга»
2013

УДК 004.056.5: 004.75
ББК 55.6
Щ 61

Рецензенты:

Белоножкин В.И., д-р техн. наук (Аппарат уполномоченного представителя Президента по правам человека в Воронежской области);
Зарубин С.В., д-р. техн. наук, профессор (Воронежский институт МВД России)

Щ 61 Щербаков, В.Б. Риск-анализ атакуемых беспроводных сетей: Монография/ В.Б. Щербаков, С.А. Ермаков, Н.С. Коленбет; под ред. чл.-корр. РАН Д.А. Новикова. – Воронеж: Издательство «Научная книга», 2013. – 160 с.

ISBN 978-5-98222-847-5

Книга посвящена разработке методической базы для прогнозной оценки эффективности систем защиты информации в современных беспроводных сетях на основании аналитических риск-моделей отдельных элементов и системы в целом.

Монография ориентирована на специалистов осуществляющих проектирование, развертывание и администрирование беспроводных сетей в условиях необходимости обеспечения конфиденциальности, целостности и доступности обрабатываемой информации. Она будет также полезна студентам и аспирантам соответствующих специальностей.

УДК 004.056.5: 004.75
ББК 55.6
Щ 61

ISBN 978-5-98222-847-5

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Беспроводные сети (БС) становятся все более важным ресурсом в условиях развития корпоративных технологий. Необходимость расширения существующих сетей за счет пользователей подвижной связи и невысокие затраты на эксплуатацию привели к принятию стандарта во многих отраслях, практической деятельности [12].

Интенсивное развитие беспроводных сетей закономерно ведет к увеличению интереса к ним со стороны нарушителей. В связи с чем следует ожидать роста числа компьютерных атак на них с использованием различных средств., Данное обстоятельство делает актуальной проблему обеспечения информационной безопасности (ИБ) данных объектов с использованием адекватных средств и методов защиты информации.

В настоящее время [1,2,9] управление рисками в области ИБ рассматривается как обязательная составляющая процесса защиты информационной системы. С одной стороны, это связано с тем, что на различных стадиях жизненного цикла системы имеют место разнообразные угрозы, с другой, в рамках разрозненных методик анализа и управления отдельными типами рисков трудно учтесть корреляции между отдельными риск-факторами, то есть затруднено выявление позитивной или негативной зависимостей между ними.

Таким образом, 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 [3,4,5].

При этом внедрение беспроводных технологий идет гораздо быстрее, чем приобретение профессиональных знаний и опыта, необходимых для адекватного управления ими, что обуславливает необходимость борьбы с угрозами нового поколения с помощью частичного использования решений и инструментов, первоначально разработанных для инфраструктуры проводной связи [10].

Каждая станция в сети потенциально является уязвимой и должна подчиняться установленным правилам, чтобы избежать возникновения проблем с безопасностью и эксплуатационными характеристиками. Эти проблемы наряду с параллельной эволюцией множества стандартов дополнительно усложнили задачу управления сетью.

Кроме того, вопрос физической безопасности в технологиях беспроводного доступа выходит на новый уровень, ибо невозможно четко описать периметр сети. Следовательно, сложнее организовать разграничение доступа авторизованных и несанкционированных пользователей и устройств, трудно локализовать такие устройства [12].

Специфика современных беспроводных сетей отражается в используемых подходах к анализу рисков. Особенностью ИБ беспроводной сети, является то, что в результате атак, использующих ее уязвимости, ущерб наносится как ресурсам самой беспроводной сети, так и активам организации в целом [7,12].

Многие активы не имеют четкого денежного выражения, например, потеря репутации. Это затрудняет, а в большинстве случаев делает невозможной более или менее точную количественную оценку ущерба. Тот факт, что статистические данные о вероятностях реализации угроз и ущербах от них в беспроводных сетях в настоящее время отсутствуют, говорит о невозможности получения объективной информации о вероятности этих параметров.

В настоящее время рынок беспроводной связи испытывает радикальные изменения, обусловленные ростом спроса со стороны абонентов на комплексные мультимедийные услуги, а также экспоненциальным ростом трафика и требований к скорости передачи данных. Сотовые сети нового четвертого поколения, основанные на технологии LTE, позволяют за счет повышения эффективности сети и сокращения эксплуатационных расходов решить эти вопросы путем применения инновационных технологии улучшения качества связи с использованием общего канала Интернет [13].

Вопросы обеспечения безопасности в сетях четвертого поколения решаются на нескольких структурных уровнях: на физическом, так называемом

воздушном интерфейсе, на уровне внутренней сети оператора, а также на уровне взаимодействия различных операторов. Каждый уровень представляет собой распределенную систему взаимосвязанных компонентов, каждый из которых может подвергаться внешним деструктивным воздействиям [93].

Таким образом, к беспроводным сетям стандарта LTE как к объекту исследования в контексте разработки риск-моделей отдельных элементов, могут быть адаптированы и применены экспертные подходы, рассмотренные в монографии. Ограничивающим фактором в применении этой методологии является необходимость анализа, систематизации и обработки большого количества экспертных данных, что требует существенных материальных и временных ресурсов. Кроме того принципиальным отличием сетей LTE от Wi-Fi является значительно больший масштаб их зоны покрытия и как следствие усложнение структуры сети, что в свою очередь усложняет процесс получения согласованных экспертных оценок и минимизации их субъективности.

Поэтому крайне актуальным представляется исследование альтернативных подходов к разработке риск-моделей современных беспроводных сетей, в том числе и сетей стандарта LTE.

В ряде случаев удается накопить емкие статистические данные в условиях воздействия на такие сети определенных деструктивных факторов, позволяющие применить концепцию вероятностного риск-анализа распределенных систем. Однако имеет право на жизнь и другой подход [12], когда для обработки экспертных данных применяется аппарат теории нечетких множеств и нечеткой логики.

Целью данной книги является демонстрация возможностей практического применения разработанных авторами подходов к прогнозной оценке эффективности механизмов защиты беспроводных сетей на основе вероятностных риск-моделей программно-определяемых элементов беспроводных сетей, подвергающихся различным видам атак.

Авторы ставили перед собой следующие задачи:

– провести обзор и классификацию наиболее актуальных на текущий момент технологий беспроводной связи;

– создать формальную модель угрозы безопасности современным беспроводным сетям;

– выбрать наиболее подходящую методику для построения риск-моделей современных беспроводных сетей [3,6,10,11];

– разработать методику прогнозной оценки эффективности средств защиты беспроводных сетей WLAN [1-5,8,9];

– проанализировать архитектуру системы безопасности в сетях LTE и этапы ее развития;

– проанализировать характерные уязвимости и типовые атаки в LTE;

– разработать аналитические вероятностные риск-модели отдельных элементов и отдельной соты сети LTE;

– применить теорию массового обслуживания для разработки модели обслуживания абонентов в сетях LTE;

– провести имитационное моделирование предлагаемых моделей.

Фактически объектом исследования являются современные беспроводные сети в контексте комплексного обеспечения их информационной безопасности. Предметом выступают методики оценки и прогнозирования рисков информационной безопасности беспроводных телекоммуникационных систем в условиях реализации направленных на них деструктивных воздействий.

Практическая ценность работы заключается в перспективах обобщения рассмотренных моделей на более широкий класс элементов современных беспроводных сетей, а также – на более широкий класс реализуемых на них деструктивных воздействий.

Первая глава знакомит читателя с современными беспроводными сетями. Предлагается подход к созданию формальной модели угрозы безопасности, включающий источники угроз, уязвимости и типовые атаки, с подробными примерами на основе сетей стандарта IEEE 802.11. Выбирается наиболее подходящая методика для построения риск-моделей рассматриваемых

беспроводных сетей с перспективой оценки эффективности применяемых средств защиты.

Во второй главе беспроводные сети рассматриваются как объекты реализации угроз информационной безопасности. Разрабатывается методика оценки эффективности средств защиты беспроводных сетей WLAN и демонстрируется ее практическое применение на примере беспроводных сетей стандарта IEEE 802.11.

В третьей главе подробно рассматривается архитектура системы безопасности в сетях LTE, приводятся требования к системе безопасности LTE и анализируются ее основные элементы. Анализируются характерные уязвимости и типовые атаки. Разрабатываются аналитические вероятностные риск-моделей отдельных элементов и отдельной соты сети LTE.

В четвертой главе проводится анализ существующих численных мер оценки рисков. Обосновывается структура методики оценки риска на основе метода анализа иерархий, а также представляются оригинальная мера оценки и алгоритм ее вычисления.

В приложении приводятся примеры, демонстрирующие на практике возможности предлагаемой методики.

Авторы выражают благодарность сотрудникам кафедры «Системы информационной безопасности» Воронежского государственного технического университета за поддержку инициативы настоящего издания и помощь в подготовке рукописи.

Авторы будут благодарны за отзывы и пожелания, а также конструктивные предложения о сотрудничестве в области безопасности информационных технологий, которые следует отправлять по адресу:

394049, Воронеж, Ватутина 1, Региональный учебно-научный центр по проблемам информационной безопасности.

Тел./факс: (4732) 52-34-20, 78-59-90

E-mail: mnac@comch.ru

(3,1911, низкий риск). Второй пример показывает, что методика позволяет учитывать изменения в топологии беспроводной сети. Когда устройство подключается или выходит из беспроводной сети, методика позволяет повторно эффективно оценить риск всей беспроводной сети, не повторяя лишние шаги. Этот пример также показывает, что методика оценки рисков позволяет получать результаты с высокой детализацией, с помощью которых можно выявить различия в конфигурациях различных беспроводных сетей.

Научное издание

Владимир Борисович Щербаков
Сергей Александрович Ермаков
Николай Сергеевич Коленбет

РИСК-АНАЛИЗ АТАКУЕМЫХ БЕСПРОВОДНЫХ СЕТЕЙ

Монография

Под ред. чл.-корр. РАН Д.А. Новикова

Издание публикуется в авторской редакции

Дизайн обложки С.А. Кравец

Подписано в печать 30.12.2013. Формат 60x84 1/16.
Усл. печ. л. 10,0. Заказ 000. Тираж 1000 экз.

ООО Издательство «Научная книга»
394077, Россия, г. Воронеж, ул. 60-й Армии, 25-120
http://www.sbook.ru/

Отпечатано с готового оригинал-макета
в ООО «Цифровая полиграфия»
394036, г. Воронеж, ул. Ф. Энгельса, 52.
Тел.: (473)261-03-61