На правах рукописи

Липатов Алексей Леонидович

МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КЛЮЧЕВЫХ СИСТЕМ С ИСПОЛЬЗОВАНИЕМ ДЕРЕВЬЕВ АТАК

Специальность 05.13.19 «Методы и системы защиты информации, информационная безопасность»

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Санкт-Петербург
2009

Работа выполнена на кафедре Проектирования компьютерных систем Санкт-Петербургского государственного университета информационных технологий, механики и оптики

Научный руководитель:
доктор технических наук, профессор, Ю.А. Гатчин

Официальные оппоненты:
доктор технических наук, профессор, В.В.Григорьев
кандидат технических наук С.Н. Новаковский

Ведущая организация: Закрытое акционерное общество «ОТКРЫТЫЕ ТЕХНОЛОГИИ 98», Москва

Защита состоится « 22 » декабря 2009 г. в 15 часов 50 минут на заседании диссертационного совета Д212.227.05 в Санкт-Петербургском государственном университете информационных технологий, механики и оптики по адресу: 197101, г. Санкт-Петербург, Кронверкский пр., д. 49.

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

Автореферат разослан « 20 » ноября 2009 г.

Учёный секретарь
диссертационного совета Д212.227.05
кандидат технических наук, доцент В.И. Поляков

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность проблемы. Актуальность проблемы обеспечения информационной безопасности (ИБ) ключевых систем информационной инфраструктуры (КСИИ) Российской Федерации (РФ), обуславливается современными условиями ведения деятельности на критически важных объектах информационной и телекоммуникационной инфраструктуры РФ: наличием растущей зависимости бизнес-процессов от инфокоммуникационных технологий (ИКТ), сложностью используемых технологий, а также большим количеством потенциальных угроз ИБ, как случайного, так и преднамеренного характера, включая терроризм, реализация которых может приводить к значительным негативным последствиям для безопасности государства в информационной сфере и препятствовать реализации РФ своих целей во внутренней/внешней политике.

Однако, несмотря на всю важность и значимость данной проблемы, резко возросшей в последнее время в связи с бурным внедрением ИКТ на критически важных объектах информационной и телекоммуникационной инфраструктуры РФ, имеющиеся в настоящее время и применяемые на практике подходы к обеспечению ИБ КСИИ, модели построения систем информационной безопасности (СИБ) КСИИ имеют ряд существенных недостатков, среди которых необходимо выделить следующие:

- при решении задачи обеспечения ИБ КСИИ недостаточное внимание уделяется вопросам управления ИБ в целом, а оценке и обработке рисков ИБ в частности, также не уделяется должного внимания вопросам, связанным с обеспечением целостности и доступности информации, обрабатываемой в КСИИ;
- разработанные ФСТЭК России и применяемые в настоящий момент методики оценки защищенности информации от её утечки по каналам побочных электромагнитных излучений и наводок (ПЭМИН) не позволяют проводить корректную оценку защищенности КСИИ при использовании средств/методов активной и/или пассивной защиты информации;
- построение СИБ КСИИ осуществляется с использованием целого ряда неэффективных защитных мер, которые, как это было отмечено в «Доктрине информационной безопасности Российской Федерации», не в полной мере соответствуют современным потребностям общества и государства;
- существующие модели и методы, на основе которых осуществляется построение СИБ КСИИ, недостаточно формализованы;
- в полном объеме подходы к оценке уровня соответствия КСИИ установленным требованиям по ИБ в настоящий момент на практике де-факто не используются;
- при создании СИБ КСИИ, как правило, не используется общепринятый в мире процессный подход, а также ролевые модели СИБ КСИИ.

Анализ существующих и применяемых в настоящее время подходов к обеспечению ИБ КСИИ продемонстрировал, что СИБ КСИИ, создаваемые на их основе, являются недостаточно эффективными и не позволяют обеспечивать должный уровень ИБ КСИИ. Таким образом, разработка методов обеспечения ИБ КСИИ с использованием, в том числе методологии деревьев атак, которые позволят создавать зрелые СИБ КСИИ, способные адекватно противостоять актуальным угрозам ИБ, является важной научной задачей, имеющей существенное значение для обеспечения безопасности государства в сфере ИКТ.

Исходные положения для диссертационного исследования. КСИИ – территориально-распределенная сложная гетерогенная информационно-телекоммуникационная система (ИТС), входящая в состав критически важного объекта информационной и телекоммуникационной инфраструктуры РФ, относящегося к органам государственной власти (ОГВ) РФ. Технические средства ИТС: серверы, рабочие станции, сетевое коммуникационное оборудование, системы хранения данных и т.д. образуют локальные вычислительные сети (ЛВС), входящие в состав КСИИ,

расположены на нескольких площадках в различных субъектах РФ (для ОГВ федерального уровня) либо в одном субъекте РФ (для ОГВ уровня субъекта РФ). Сетевое взаимодействие между ЛВС организовано при помощи сети передачи данных (СПД), в состав которой могут входить в т.ч. и арендованные каналы связи. Архитектурно КСИИ разделяется на открытый и закрытый сегменты.

В КСИИ осуществляется обработка, передача и хранение открытой и конфиденциальной информации. Пользователи КСИИ имеют различные полномочия по доступу к информации и сервисам КСИИ.

Методологической основной диссертационного исследования являются работы Корченко А.Г., Хорева А.А., Ярочкина В.И., Домарева В.В., Кулакова В.Г., Курило А.П., Полаженко С.В., Колегова Д.Н., Котенко И.В., С. Камтепе, Б. Енера, Б. Шнайера, Х. Комона, М. Дауча и других ученых и специалистов, специализирующихся на вопросах обеспечения ИБ современных автоматизированных систем (АС), включая вопросы защиты от утечки информации по каналам ПЭМИН и использования методологии деревьев атак (ДА) для управления рисками ИБ КСИИ.

Цель диссертационной работы. Разработка методов управления и обеспечения ИБ КСИИ с использованием теории ДА, процессно-ролевого подхода к построению СИБ КСИИ, которые позволят эффективно решать задачи защиты обрабатываемой в КСИИ информации от нарушения ее конфиденциальности (в т.ч. путем применения технических средств разведки ПЭМИН), целостности и доступности и выполнения КСИИ своих функций без неприемлемого ущерба для безопасности государства в сфере ИКТ.

Основными задачами, решаемыми в процессе достижения цели проводимого исследования являются:

1. Проведение анализа моделей и методов, используемых для обеспечения ИБ КСИИ, выявление их недостатков и ограничений в применении.
2. Развитие методов управления и обеспечения безопасности КСИИ путем применения расширенной модели управления ИБ на базе PDCA-подхода Шухарта-Дёминга к планированию, реализации, проверке и совершенствованию и теории деревьев атак, которая должна быть использована при разработке формализованного подхода к моделированию и обнаружению реализации в отношении КСИИ угроз ИБ.
3. Разработка методики оценки защищенности информации обрабатываемой в КСИИ от утечки за счет ПЭМИН при использовании средств/методов активной (генераторы пространственного или линейного шума, сетевые помехоподавляющие фильтры) и/или пассивной (экранирование помещений КСИИ) защиты.
4. Формирование процессно-ролевой модели СИБ КСИИ применительно к ключевым процессам управления ИБ.
5. Разработка методики оценки уровня соответствия КСИИ установленным требованиям по ИБ с учетом предлагаемых к внедрению в рамках СИБ КСИИ эксплуатационных процессов ИБ.

Объекты исследования. Структура КСИИ органов государственной власти (ОГВ) в техническом аспекте, схемы информационных потоков, циркулирующих в КСИИ, активы КСИИ ОГВ, организационная структура обеспечения ИБ КСИИ ОГВ, модели обеспечения ИБ КСИИ ОГВ и методики оценки эффективности защищенности КСИИ ОГВ, методы и средства обеспечения ИБ КСИИ ОГВ.

Методы исследований. Для решения поставленной задачи использовались: методы теории вероятностей, теории графов, теории конечных автоматов, теории распространения радиоволн, теории классификации и систематизации, математическое моделирование, технологии и стандарты на ИТС и ИБ. Для проектирования процессно-ролевой модели СИБ КСИИ использовались методы UML-моделирования.

Научная новизна:

1. Впервые проведена разработка расширенной модели управления ИБ КСИИ на базе PDCA-подхода Шухарта-Дёминга и теории деревьев атак, используемой при моделировании и обнаружении реализации при возникновении инцидентов ИБ в отношении КСИИ угроз ИБ.
2. При разработке расширенной модели управления ИБ КСИИ на базе PDCA-модели и теории деревьев атак произведен синтез отечественных и зарубежных подходов к управлению ИБ, в результате чего осуществлено создание оригинальных перечней угроз и уязвимостей, произведено определение соотношения угроз ИБ к типам активов, применительно к КСИИ.
3. Осуществлена разработка оригинальной методики оценки защищенности обрабатываемой в КСИИ информации от утечки по каналам ПЭМИН, позволяющей учитывать на этапе планирования реализации СИБ КСИИ использование средств/методов активной и/или пассивной защиты.
4. Сформирована методика оценки уровня соответствия КСИИ установленным требованиям по ИБ с учетом предлагаемых к внедрению в рамках СИБ КСИИ эксплуатационных процессов (процессов обеспечения ИБ).

Основным результатом проведенных исследований является внесение существенного вклада в решение проблемы, отмеченной в Доктрине информационной безопасности Российской Федерации, связанной с необходимостью совершенствования методов и способов защиты КСИИ, позволяющих создавать СИБ КСИИ, эффективно решающие задачи обеспечения ИБ КСИИ и выполнения КСИИ своих функций без неприемлемого ущерба для безопасности государства в информационной сфере.

Достоверность научных результатов и выводов обусловлена корректным применением математического аппарата, корректной оценкой адекватности математических, информационных, процессно-ролевых моделей, сопоставлением полученных общих результатов с частными случаями, приведенными другими авторами, а также успешным практическим использованием разработанных методов обеспечения ИБ КСИИ с использованием деревьев атак.

Практическая значимость. В рамках диссертационного исследования произведен анализ и систематизация накопленного в РФ в период с 1992 г. по 2008 г. опыта обеспечения ИБ КСИИ, выявлены недостатки (в т.ч. по результатам анализа лучших мировых практик обеспечения у управления ИБ) и ограничения в применяемых в настоящий момент подходах и моделях защиты КСИИ, предложены методы обеспечения ИБ, способные повысить эффективность решения задач обеспечения ИБ, в т.ч. обеспечения конфиденциальности, целостности и доступности, обрабатываемой в КСИИ информации, а также оценки и управления рисками ИБ с использованием теории деревьев атак, в рамках создаваемых/введенных в промышленную эксплуатацию СИБ КСИИ. Положения диссертационного исследования могут использоваться на всех этапах жизненного цикла КСИИ: при подготовке к эксплуатации, при вводе в эксплуатацию, непосредственно при эксплуатации, а также при снятии КСИИ с эксплуатации.

Положения диссертационного исследования могут использоваться также для совершенствования нормативно-методической базы, устанавливающей требования государственных регулирующих органов РФ к обеспечению ИБ КСИИ, с целью повышения эффективности СИБ КСИИ, создаваемых на их основе.

Практическая значимость работы подтверждена в результате успешной эксплуатации результатов диссертационного исследования на ряде критически важных объектов информационной и телекоммуникационной инфраструктуры РФ, что подтверждается Актами о внедрении результатов диссертации.

Основные положения, выносимые на защиту:

1. Расширенная модель управления ИБ КСИИ на базе PDCA-подхода Шухарта-Дёминга и теории деревьев атак, используемой при моделировании и обнаружении реализации при возникновении инцидентов ИБ в отношении КСИИ угроз ИБ.
2. Методика оценки защищенности информации от утечки по каналам ПЭМИН, позволяющей учитывать использование, предпринятых на объектах информационной и телекоммуникационной инфраструктуры РФ дополнительных защитных мер.
3. Методика оценки уровня соответствия КСИИ требованиям по ИБ, с учетом предлагаемых к внедрению в рамках СИБ КСИИ процессов обеспечения ИБ.

Реализация результатов исследования. Основные результаты исследования реализованы при проведении в 2007-2008 г. научно-исследовательской работы (НИР) по развитию информационной системы органов прокуратуры (НИР по развитию ИСОП. Заказчик: Генеральная прокуратура Российской Федерации (государственный контракт № 10/76-337-07 от 30 ноября 2007 г.), при создании в 2007 г. системы управления информационной безопасностью системы управления магистральной IP-сетью ЗАО «Компания ТрансТелеКом», при проведении в 2008 г. НИР (шифр: «ПВДНП»), в интересах Минкомсвязи России, ФСБ России, ГИАЦ и ИЦ/ВЦ МВД России, МО РФ, МИД России, ФМС России и др., а также в производственной деятельности ЗАО «ОТКРЫТЫЕ ТЕХНОЛОГИИ 98», ЗАО «Лаборатория противодействия промышленному шпионажу», и в учебном процессе кафедры проектирование компьютерных систем (ПКС) факультета компьютерных технологий и управления (КТиУ) СПб ГУ ИТМО.

Апробация работы. Основные результаты, полученные в ходе диссертационного исследования, докладывались на 9 международных и российских научных конференциях/семинарах/совещаниях: ежегодном совещании органов по аттестации Управления ФСТЭК России по СЗФО, Санкт-Петербург, 2006 г., III межвузовской конференции молодых учёных СПбГУ ИТМО, Санкт-Петербург, 10-13 апреля 2006 г., IV Международной научно-практической конференции «Инфокоммуникационные технологии Глобального информационного общества», Казань, 6-7 сентября 2006 г., IV межвузовской конференции молодых учёных СПб ГУ ИТМО (Санкт-Петербург), семинаре «Обеспечение информационной безопасности прикладных систем» (компания ЗАО «ОТКРЫТЫЕ ТЕХНОЛОГИИ 98»), Москва, 29 мая 2007 г., семинаре «Обеспечение информационной безопасности ОАК в условиях реорганизации» в рамках VIII международного авиационно-космического салона МАКС-2007, Москва, 21-26 августа 2007 г., IV Международной специализированной выставке-конференции по информационной безопасности Infosecurity Russia 2007, Москва, 26-28 сентября 2007 г., конференции информационная безопасности 2008 г. в рамках конференции студенческая весна МГТУ им. Н. Э. Баумана, V Всероссийской межвузовской конференции молодых учёных, Санкт-Петербург, 15-18 апреля 2008 г.

Диссертационные исследования поддержаны грантом 2007 года для студентов и аспирантов вузов и академических институтов, расположенных на территории Санкт-Петербурга, проведенного в соответствии с приказом председателя Комитета по науке и высшей школе Правительства Санкт-Петербурга от 16.01.2007 г. № 3 (номер гранта: 03/3.11/15-03/12, диплом победителя конкурса грантов Санкт-Петербурга для студентов, аспирантов 2007 г.: серия ПСП № 070306).

Публикации. По теме диссертации опубликовано 9 статей (из них 2 – в изданиях из перечня ВАК РФ).

Структура и объем диссертации. Диссертация состоит из введения, четырех глав, заключения, перечня литературы (108 наименований) и 2 приложений. Содержит 121 страниц текста (из них: 106 страниц основного текста, 15 страниц текста приложений). В диссертации приведено 29 рисунков, 14 таблиц.

СОДЕРЖАНИЕ ДИССЕРТАЦИОННОЙ РАБОТЫ

Введение посвящено обоснованию актуальности и значимости проводимых диссертационных исследований, описанию подхода к разработке адекватных актуальным угрозам ИБ методов защиты КСИИ с использованием теории ДА. Кратко рассмотрены результаты исследований и наработок по проблематике обеспечения ИБ КСИИ, изложенные в работах других авторов. Изложены цели, задачи и направления исследований. Сформулированы исходные положения работы, объекты и методы исследований.

В первой главе производится исследование сложившейся системы взглядов на защиту КСИИ, исследование особенностей решения задачи обеспечения ИБ КСИИ и роли отечественной нормативной базы, регламентирующей вопросы защиты информации. Кроме того, производится критический анализ существующих подходов, моделей и методов обеспечения ИБ КСИИ с выявлением их недостатков и ограничений в применении, а также формулируется подход к разработке методов обеспечения ИБ, адекватных актуальным угрозам ИБ КСИИ с использование теории деревьев атак, осуществляется постановка задачи.

Объектом диссертационного исследования является КСИИ ОГВ, однако, результаты настоящего диссертационного исследования в целом могут быть использованы и при организации СИБ ГАС «Выборы», спутниковых систем, используемых для обеспечения органов управления и в специальных целях и т.д.

В настоящий момент в соответствии с установленными требованиями активы КСИИ подлежат обязательной защите. Режим обеспечения ИБ активов КСИИ устанавливается соответствующим предприятием/организацией (применительно к настоящему диссертационному исследованию – ОГВ) на основе положений нормативно-правовых документов и подзаконных актов (ОРД и НМД РФ), регламентирующих вопросы обеспечения ИБ.

Обеспечение ИБ КСИИ, является составной частью работ по созданию и эксплуатации критически важных объектов информационной и телекоммуникационной инфраструктуры и осуществляется в рамках СИБ.

Построение СИБ должно осуществляться в соответствии с подходами и принципами, описанными в соответствующих руководящих документах ФСТЭК России, ФСБ России.

При этом, положения действующих нормативно-правовых документов, ОРД и НМД по ИБ играют важную роль при решении задачи обеспечения ИБ КСИИ. Это связано с тем, что в отличие случаев защиты АС, не отнесенных к КСИИ, в соответствии с базовыми положениями, изложенными в СТР-К, в случае обеспечения ИБ КСИИ, вне зависимости от того являются ли активы государственными или не являются таковыми, требования государственных регулирующих органов в сфере обеспечения ИБ КСИИ будут носить обязательный для выполнения характер.

Основной целью обеспечения ИБ в рамках СИБ КСИИ должно являться обеспечение безопасного использования ИКТ, то есть обеспечение функционирования КСИИ в соответствии с установленными требованиями без неприемлемого ущерба для критически важного объекта информационной и телекоммуникационной инфраструктуры РФ (в рамках настоящего диссертационного исследования – для ОГВ), а как следствие для государства в информационной сфере.

При разработке эффективных методов обеспечения ИБ КСИИ с использованием теории деревьев атак необходимо учесть следующие требование. СИБ КСИИ должны быть комплексными и включать в своей состав процессы ИБ (организационные меры), технические, программные (программно-технические) средства ИБ, а также персонал критически важного объекта информационной и телекоммуникационной инфраструктуры РФ.

Кроме того, при разработке формальной методологии моделирования и обнаружения реализации угроз ИБ, направленных на активы КСИИ, следует стремиться к формированию подхода, на основе которого возможно будет осуществлять обнаружение сложных (многоэтапных) атак на КСИИ (что невозможно осуществить с применением имеющихся и применяемых для обеспечения ИБ КСИИ методик).

Во второй главе приводятся общесистемные решения по модели СИБ КСИИ. Приведена расширенная модель управления ИБ, реализуемая в рамках СИБ КСИИ, базирующаяся на основе EPDCA-модели, разработанной на базе PDCA-модели Шухарта-Дёминга, а также перечень угроз ИБ с указанием типов активов КСИИ, на которые данные угрозы ИБ могут воздействовать, перечень угроз ИБ КСИИ с указанием уязвимостей при помощи которых данные угрозы могут быть реализованы, необходимые для эффективного управления ИБ в рамках разработанной расширенной модели управления ИБ КСИИ. Также осуществлена разработка расширенного дерева атак (ДА), расширенных автоматов деревьев атак, расширенного параллельного автомата, используемых для эффективного моделирования и обнаружения инцидентов ИБ в рамках расширенной модели управления ИБ КСИИ.

ИБ КСИИ должна обеспечиваться на комплексной и системной основе в масштабах всего критически важного объекта информационной и телекоммуникационной инфраструктуры РФ, в рамках СИБ КСИИ.

СИБ КСИИ образуется комплексом технических, программных и программно-технических средств обеспечения ИБ, процессов и персонала, объединенных на основе модели расширенной управления ИБ.

Расширенная модель управления ИБ (EPDCA-модель: Extended «Plan – Do – Check – Act»-модель; расширенная «Планирование – Реализация – Проверка – Улучшение»-модель), реализуемая в рамках СИБ КСИИ, должна базироваться на основе PDCA-цикла Шухарта-Деминга, так как это показано на рисунке 1.

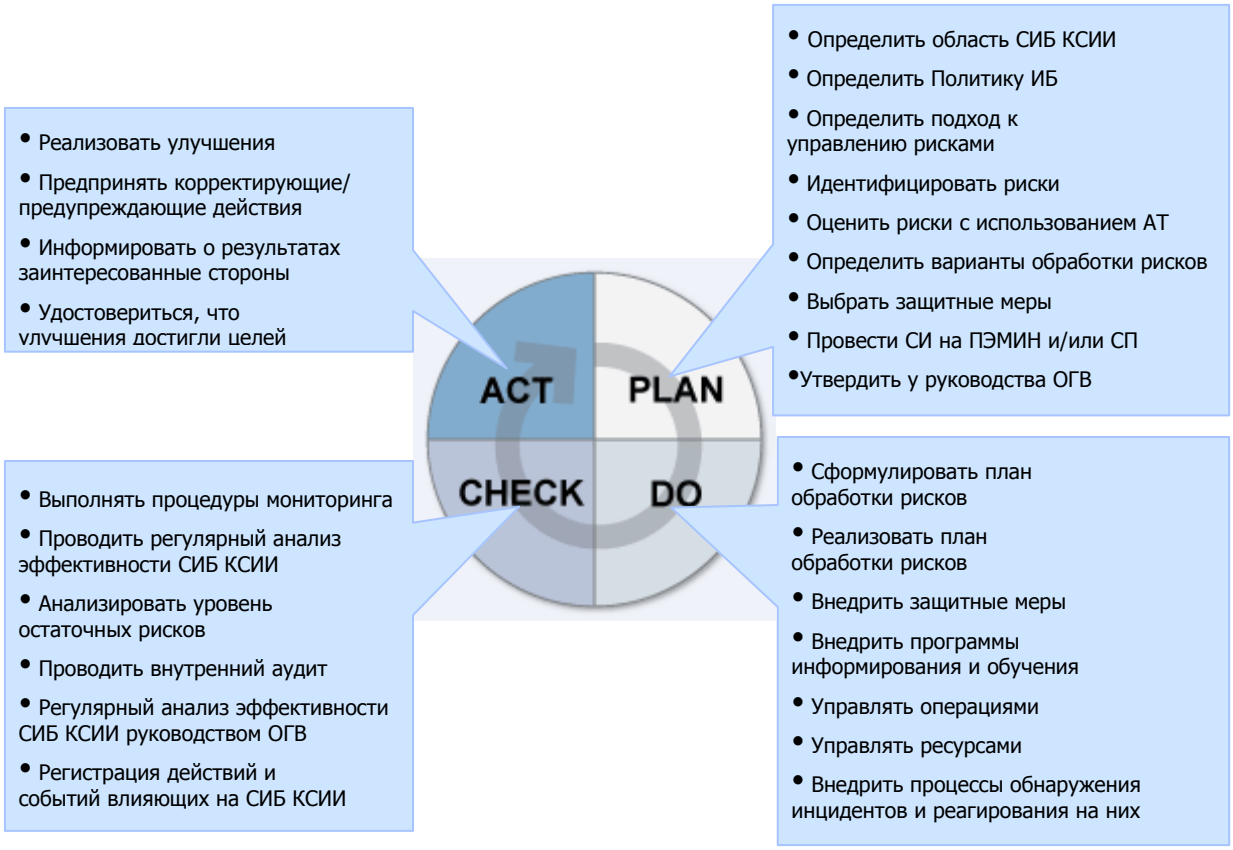

Рисунок 1 – Расширенная модель управления ИБ (EPDCA-модель) СИБ КСИИ

Для осуществления эффективного управления ИБ КСИИ в рамках расширенной модели управления, приведенной в подразделе, необходимо осуществить разработку перечня угроз ИБ с указанием типов активов КСИИ, на которые данные угрозы ИБ могут воздействовать. Данная информация и позволяет при оценке рисков ИБ (с использованием методологии деревьев атак) КСИИ в процессе управления ИБ КСИИ учитывать факт того, что в целом каждая конкретная угроза ИБ воздействует только на определенные типы активов КСИИ.

В диссертационном исследовании в контексте методологии деревьев атак были использованы следующие сокращения: И ($\wedge$) – Операция «логическое И», РДА – Расширенное дерево атак, ($\vec{\wedge}$) У-И – Операция «упорядоченное И», НКАД – недетерминированный конечный автомат деревьев, ИЛИ ($\vee$) – Операция «логическое ИЛИ», РНКАД – расширенный недетерминированный конечный автомат деревьев, ВЖ – время жизни, РПА – расширенный параллельный автомат, СК – степень конфиденциальности.

Деревья атак являются формальным методом моделирования реализации угроз ИБ в отношении КСИИ (атак). Атаки представляются в виде деревьев, где корнем является цель атаки, ближайшие узлы – подцелями, а листья – способами достижения подцелей и реализации атаки на основную цель. Дочерние узлы в дереве могут быть двух типов: И и ИЛИ. Для реализации атаки необходимо обойти все дочерние узлы типа И или хотя бы один узел типа ИЛИ. Дерево атак при этом формируется следующим образом:

1. Определяются потенциальные цели атаки. Каждая цель атаки является корнем собственного дерева атак.
2. Рассматриваются все возможные атаки на заданные цели.
3. Эти атаки формируют дочерние узлы И и ИЛИ.
4. Каждая из атак рассматривается как цель и формирует ее дочерние узлы.
5. Данный процесс продолжается рекурсивно.

При такой структуре дерева сценарий атаки является поддеревом, которое включает узел – цель, а так же все его дочерние узлы И и хотя бы один узел ИЛИ. Подобным образом определяются все поддеревья для дочерних подцелей. Дерево атак является законченным, если оно содержит поддеревья для всех возможных атак, ведущих к достижению главной цели. Для каждого узла можно назначить атрибут (например, ВЖ и др.). Используя такие атрибуты, возможно выявить атаки с определенными параметрами, что может быть полезно для определения угроз и требуемых защитных мер.

Автомат деревьев обрабатывает входное дерево, начиная от листьев и заканчивая корнем.

Определение 1. Недетерминированным конечным автоматом деревьев (НКАД) является кортеж $A = (Q, F, Q_f, \Delta)$, где

Q – множество состояний;

$Q_f \subseteq Q$ – множество финальных состояний

F – множество n-арных значений (a - лист, $f()$ - узел с одним потомком, $g(,)$- узел с двумя потомками и т.п.)

Δ - множество функций переходов в виде

$f(q_1(x_1),\ldots,q_n(x_n)) \rightarrow q(f(x_1,\ldots,x_n))$

где $f \in F$, $q, q_1, \ldots, q_n \in Q$ и $x_1, \ldots, x_n$ - все переменные, которые принимают значения из множества F.

Входом НКАД является дерево, которое выражается последовательностью n-арных значений входного алфавита F. Автомат обрабатывает дерево от листьев к корню. Когда корень обработан, автомат принимает входное дерево, если одно из финальных состояний Q_f достигнуто.

Разработка расширенного дерева атак. В данной диссертационной работе предлагается несколько улучшений дерева атак для повышения его эффективности при оценке рисков реализации угроз ИБ в отношении активов КСИИ. Во-первых, существуют деревья атак, в которых цели или подцели могут быть достижимы, если все потомки типа И обходятся в заданной последовательности. В этом случае невозможно использовать потомков И или ИЛИ для формирования заданного порядка. Например, «Отключение клиента» в сети WLAN можно реализовать, выполнив атаки типа «Подслушивание MAC-адреса точки доступа», «Подмена AP» и «Отправление сообщения об отключении MAC-адреса жертве» в заданной последовательности. Такие типы потомков назовем У-И и обозначим символом $\vec{\wedge}$.

Следующее улучшение - время жизни и атрибут конфиденциальности узла. Атрибут ВЖ определяет время жизни для событий на листьях и для подцелей. В примере «Отключение клиента» клиент получает сообщение «отключен» от точки доступа, но пытается восстановить соединение. Клиент осуществляет последовательность определенных операций для восстановления

соединения. Эти операции включают поиск точки доступа с лучшим сигналом, выбор способа аутентификации и подключение к выбранной точке доступа. Атакующий имеет ограниченное время на завершение атаки до того, как жертва восстановит подключение. Таким образом, если с момент достижения подцели прошло время больше, чем ВЖ, то подцель становится неактуальной. ВЖ позволяет снизить количество ложных срабатываний, что является одной из основных проблем систем обнаружения вторжений, применяемы в том числе в КСИИ.

Атрибут СК (степень конфиденциальности) определяет вероятность достижения цели (реализации атаки), когда подцель достигнута. Возможно сообщить об атаке до того, как она завершится.

Атрибуты подцели в расширенном дереве атаки приведены в таблице 1.

Таблица 1. Атрибуты подцели в расширенном дереве атак

Подцели	Сценарии атак	Атрибут ВЖ
B	*A(B(C(D(a), b, c), d))*	4/4 = 1
C	*A(B(C(D(a), b, c), d))*	3/4 = 0,75
D	*A(B(C(D(a), b, c), d))*	1/4 = 0,25
E	*A(E(F(e),f,g))*	3/3 = 1
F	*A(E(F(e),f,g))*	1/3 = 0,33

Для вычисления атрибута подцели необходимо рассмотреть все возможные сценарии атак, включающие данную подцель. Из всех значений выбирается максимальное. СК является отношением всех рассмотренных событий до подцели к общему количеству событий в сценарии. Этот атрибут может быть использован для создания системы раннего оповещения и предсказания атаки до ее реализации.

Определение 2. Расширенное дерево атак (РДА) – это дерево атак, в котором дочерние узлы могут быть типа И, У-И или ИЛИ, узлы имеют атрибуты ВЖ и СК.

Определение 3. Путь атаки стартует от цели расширенного дерева атаки и выбирает один из потомков ИЛИ или все потомки И и У-И рекурсивно, пока не достигнет всех листьев. Каждый такой путь называется сценарием атаки.

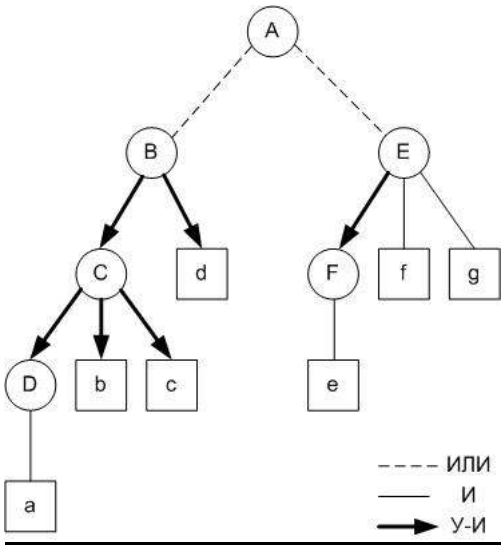

Рисунок 1 – Дерево атаки "Bypassing 802.1x"

Рисунок 2 демонстрирует расширенное дерево атаки «Обход 802.1x». Механизм аутентификации протокола 802.1x можно обойти путем перехвата сеанса аутентификации или с использованием атаки типа «Человек посредине», чтобы получить аутентификационную информацию пользователя. Каждое событие имеет атрибут ВЖ, каждая подцель имеет атрибуты СК и ВЖ, а каждое ребро имеет тип И, У-И или ИЛИ. В таблице выше представлены значения СК для

всех подцелей. Корень дерева является целью атаки «A - Обход 802.1x». Для достижения цели атакующий должен выполнить атаку «B - Перехват сеанса аутентификации 802.1x» или «E – Человек посредине в сеансе 802.1x». Подцель «B - Перехват сеанса аутентификации 802.1x» в свою очередь может быть достигнута за счет подцели «C – Отключение клиента» и «d – Подмена аутентифицированного клиента 802.1x» в заданном порядке (У-И). Построение дерева продолжается пока не будут созданы все листья, описывающие все возможные события. Данное дерево имеет два возможных пути атаки, что означает два сценария атаки для достижения цели: *A(B(C(D(a),b,c),d))* и *A(E(F(e),f,g))*.

Дерево атаки создается таким образом, чтобы разделить подцели на максимально определяемые события. Но существующие системы сетевого мониторинга могут сообщать как о событиях, так и о подцелях, используемых в дереве атак. Когда часть из потомков подцели не достигнута, можно рассматривать и другие способы достижения подцели, т.о. дерево атак не является законченным. Если дерево атак не закончено, то системному администратору нужно отправить сообщение о необходимости перестроения дерева. В примере расширенного дерева атак на рисунке выше может быть обнаружено, что клиент отключен, но событие «c – Отправить сообщение отключения MAC-адреса» не произошло. В этом случае можно ожидать других способов перехвата сеанса аутентификации с помощью отключения клиента.

В качестве другого примера рассмотрим ситуацию, когда пользователь проходит процесс аутентификации 802.1x, используя аутентификационную информацию другого активного пользователя. В этом случае можно сделать вывод, что дерево атак не полностью построено, так как атакующий перехватывает сеанс и легальный пользователь пытается подключиться или атакующий уже получил аутентификационную информацию пользователя с использованием атаки «Человек посредине» (например, подобрав слабый пароль, используя шпионское ПО, методы социальной инженерии и т.п.). Таким образом, дерево не только моделирует атаку, но и является средством самодиагностики для проверки законченности моделей известных атак.

Существует несколько недостатков недетерминированных конечных автоматов деревьев, в связи с чем они не подходят для использования с расширенными деревьями атак. Во-первых, НКАД предполагает дерево в качестве входа, обрабатывая его, когда достигается финальное состояние. В нашей системе входом является поток сообщений, среди которых ищутся конкретные деревья.

Наиболее важной особенностью расширенных деревьев атак является то, что входной поток передает только события на уровне листьев дерева. Так как ряд подцелей могут никогда не появиться во входном потоке, НКАД может никогда не достигнуть финального состояния. Улучшить НКАД можно с использованием деривационных правил, когда логическая переменная ассоциируется с каждым событием.

Определение 4. Логическая переменная *x* принимает значение true, если соответствующее событие *x* появляется во входном потоке не позже, чем ВЖ(*x*). Переменная принимает значение false, если событие не появляется или если появляется ранее, чем ВЖ(*x*).

В данной диссертационной работе предлагается новая методология и показывается как она может быть использована для определения расширенных деревьев атак в потоке сообщений. Расширенный автомат атак обеспечивает следующую функциональность: обнаружение атак, обнаружение частей атак, проверку законченности дерева атак. Расширенный автомат атак основан на НКАД, но улучшен путем ведения состояний частей атак наряду с финальными состояниями, деривационных правил для подцелей и правил обратных переходов для отката автомата, когда истекает время жизни для события или подцели.

Определение 5. Расширенный недетерминированный конечный автомат деревьев (РНКАД) – это кортеж $A=(Q, F, Q_{PA}, Q_A, D, \Delta_F, \Delta_B)$, где

Q – множество состояний

$Q_{PA} \subseteq Q$ – множество состояний частей атак.

$Q_A \subseteq Q$ – множество состояний атак

F – входная последовательность, состоящая из n-арных значений

D – множество деривационных правил для цели и подцелей в форме логических выражений, представляющих события, связанные операциями И, У-И, и ИЛИ.

Δ_F – множество правил прямых переходов в форме

$f(q_1(x_1),\ldots,q_n(x_n)) \rightarrow q(f(x_1,\ldots,x_n))$

Δ_B – множество правил обратных переходов в форме

$q(f(x_1,\ldots,x_n)) \rightarrow f(q_1(x_1),\ldots,q_n(x_n))$

где $f \in F$, $q, q_1, \ldots, q_n \in Q$ и $x_1, \ldots, x_n$ - все переменные, которые принимают значения из множества F. Входом автомата является поток значений F. Когда автомат достигает одного из состояний части атаки Q_{PA}, он сообщает об атаке с атрибутом СК. Когда автомат достигает одного из состояний Q_A, он сообщает об атаке в совокупности с последовательностью событий, которые к ней привели. Автомат автоматически сбрасывается в начальное состояние, когда достигается финальное состояние и продолжает обрабатывать входной поток.

Подобно НКАД, РНКАД использует входную последовательность F n-арных значений, где константы (*a*, *b* и т.п.) представляют листья, *f*() представляет цель или подцель с одним потомком, а *g*() представляет цель или подцель с двумя и более потомками.

Часть подцелей могутнее появиться во входном потоке расширенного дерева атак. Но можно использовать логическое выражение для вычисления подцели и ее возникновения. Для этого в РНКАД используются деривационные правила для каждой подцели. Когда возникает событие, логическое выражение, включающее это событие, вычисляется. Если значение выражения, вычисленное для подцели, равно true, то делается вывод, что подцель достигнута, даже если ее нет во входном потоке.

Правила прямых переходов подобны правилам переходов в НКАД. Когда событие или подцель возникает, или когда подцель вычисляется с использованием деривационных правил, соответствующее значение используется в правиле прямых переходов для обработки дерева и изменения состояния.

Каждое событие или подцель имеет время жизни, которое определяется атрибутом ВЖ. Если время жизни события или подцели истекает, то деривационное правило должно быть пересчитано для проверки актуальности подцели. Далее для подцели и события с истекшим временем жизни применяется правило обратного перехода для отката назад от текущего состояния. Правила обратного перехода являются обратными правилам прямого перехода. На рисунке 3 представлена диаграмма всей системы РНКАД.

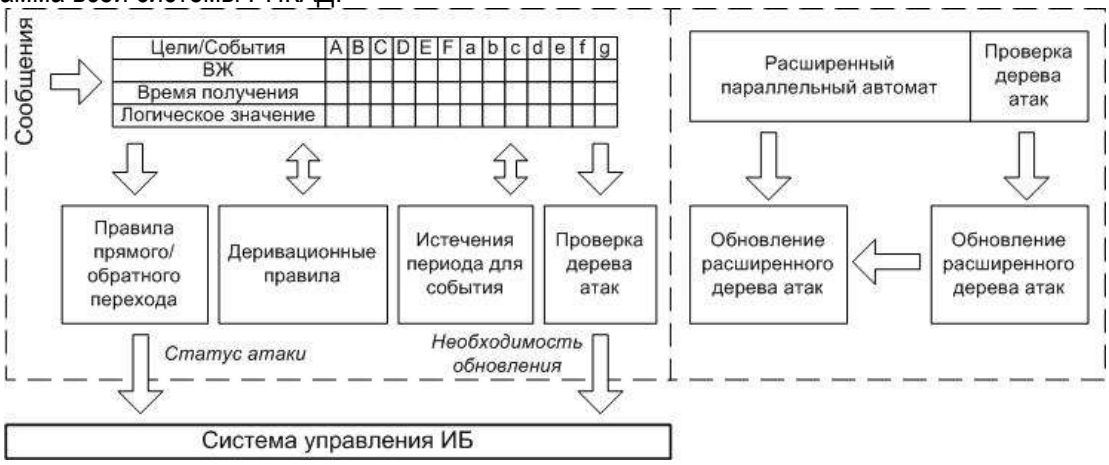

Рисунок 3 – Структура РНКАД

РНКАД существует для каждого дерева атак.

Разработка расширенного параллельного автомата. Расширенный автомат деревьев получается из расширенного дерева атак, т.о. он создается для обнаружения единственного дерева, формируемого из потока входных значений. Более сложные атаки, которые являются комбинацией нескольких расширенных деревьев атак, могут быть обработаны двумя способами. Во-первых, можно создать отдельный расширенный автомат деревьев атак для каждого расширенного дерева атак и передать копию входного потока в каждый автомат. Во-вторых, можно создать расширенный параллельный автомат (РПА), который является комбинацией расширенных деревьев атак и использует единый входной поток для параллельного обнаружения нескольких атак.

Построение расширенного параллельного автомата для множества *n* деревьев $T = \{T_1, T_2, ..., T_n\}$ состоит из двух шагов:

1. Для каждого дерева $T_i \in T$ строится РНКАД с общим входным алфавитом:
   $A^i = \left(Q^i, F, Q^i_{PA}, Q^i_A, D^i, \Delta^i_F, \Delta^i_B\right)$
   где $Q^1 \cap Q^2 \cap ... \cap Q^n = \varnothing$
2. Расширенный параллельный автомат определяется следующим образом:
   $A = A^1 \cup A^2 \cup ... \cup A^n$
   где
   $Q = Q^1 \cup Q^2 \cup ... \cup Q^n$
   $Q_{PA} = Q^1_{PA} \cup Q^2_{PA} \cup ... \cup Q^n_{PA}$
   $Q_A = Q^1_A \cup Q^2_A \cup ... \cup Q^n_A$
   $D = D^1 \cup D^2 \cup ... \cup D^n$
   $\Delta_F = \Delta^1_F \cup \Delta^2_F \cup ... \cup \Delta^n_F$
   $\Delta_B = \Delta^1_B \cup \Delta^2_B \cup ... \cup \Delta^n_B$

В третьей главе произведена разработка оригинальной методики, определяющей порядок проведения оценки защищенности конфиденциальной информации, обрабатываемой ОТС КСИИ, от ее утечки за счет ПЭМИ и позволяющей производить оценку эффективности принятых мер по активной/пассивной защите от утечки информации за счет ПЭМИ. Также произведена разработка оригинальной методики, определяющей порядок проведения оценки защищенности конфиденциальной информации, обрабатываемой ОТС КСИИ, от ее утечки за счет наводок, возникающих в ВТС под воздействием ПЭМИ ОТС, на линии электропитания и заземления (и другие токоведущие коммуникации), выходящие за границы КЗ, позволяющей производить оценку эффективности принятых мер по активной защите от утечки информации за счет наводок информативного сигнала на токоведущие коммуникации. Кроме того, - приведены данные о проведенном эксперименте – специальных исследований ПЭВМ по оригинальным методикам оценки защищенности информации, обрабатываемой ОТС за счет ПЭМИН.

Предотвращение утечки защищаемой информации, обрабатываемой в КСИИ, за счет ПЭМИ (технического канала утечки информации), является одной из задач обеспечения ИБ в рамках СИБ КСИИ (для тех случаев, когда в КСИИ обрабатывается конфиденциальная информация).

Защита от утечки конфиденциальной информации, обрабатываемой в КСИИ, за счет ПЭМИ от ОТС, должна достигаться на этапах «Реализация»/«Улучшение» цикла обеспечения и управления ИБ КСИИ за счет:

1. Использования ОТС КСИИ, удовлетворяющих требованиям, установленным в НМД ФСТЭК (Гостехкомиссии) России, по электромагнитной совместимости.
2. Размещения ОТС КСИИ на максимально возможном удалении от границ КЗ.
3. Реализации пассивных или активных методов защиты от утечки конфиденциальной информации за счет ПЭМИ.

Для определения необходимости реализации/усовершенствования мероприятий по защите информации, обрабатываемой ОТС КСИИ, от утечки за счет ПЭМИ на этапах «Планирование»/«Проверка» цикла обеспечения и управления ИБ КСИИ должна быть проведена оценка защищенности обрабатываемой ОТС КСИИ информации. Оценка защищенности обрабатываемой ОТС КСИИ информации проводится в соответствии с разработанной в данном подразделе диссертационной работы методикой. Использование для оценки рисков утечки конфиденциальной информации, обрабатываемой в КСИИ, по каналам ПЭМИ, методологии деревьев атак, разработанной в разделе 2 диссертационной работы, в соответствии с положениями действующих НМД ФСТЭК (Гостехкомиссии) России не представляется возможным.

Разработанная методика определяет порядок проведения оценки защищенности конфиденциальной информации, обрабатываемой ОТС КСИИ, от ее утечки за счет ПЭМИ и

базируется соответствующих НМД ФСТЭК (Гостехкомиссии) России, однако, в отличие от нее позволяет производить оценку эффективности принятых мер по активной защите от утечки информации за счет ПЭМИ.

Расчетная часть методики заключается в расчете возможных расстояний *R, (м)* распространения информативного сигнала от ОТС КСИИ для его каждой спектральной составляющей, а также в определении надлежащего радиуса КЗ $R_{2,}$ *(м)* для ОТС в целом.

Для оценки защищенности конфиденциальной информации, обрабатываемой ОТС КСИИ, от ее утечки за счет ПЭМИ соответствующие НМД ФСТЭК (Гостехкомиссии) России предусматривают расчет зоны $R_{2,}$ то есть требуемого радиуса КЗ вокруг ОТС КСИИ, на которых осуществляется обработка конфиденциальной информации. При обеспечении вокруг основных технических средств КЗ равной или большей R_2, считается, что ОТС КСИИ являются защищенными от утечки конфиденциальной информации за счет ПЭМИ.

На практике часто случается, что радиус КЗ значительно меньше зоны R_2 и организационными мерами обеспечить защищенности информации от утечки за счет ПЭМИ не представляется возможным. В таких случаях требуется обеспечить либо экранирование помещения(ий), в котором располагаются незащищенные ОТС КСИИ, либо обеспечить установку средств активной защиты (генераторов пространственного шума типа «ЛГШ-503», «Гном-3» и т.д.). Однако, соответствующие НМД ФСТЭК (Гостехкомиссии) России не предполагают оценки эффективности принятых мер по активной защите информации. Теоретически, возможно осуществить расчет отношения сигнал/шум на границе КЗ, которое нужно будет сравнить с нормами, которые, в неявном виде, приведены в виде параметра *К,* в формуле 1.

$$R = \frac{L}{П\sqrt{\frac{К\ E_ш}{E}}}, (м), \qquad (1)$$

где *П* – показатель степени затухания электромагнитного поля;

f, (МГц) – частота спектральной составляющей информативного сигнала;

L, (м) – расстояние от ОТС до границы ближней и промежуточной зоны распространения информативного сигнала либо расстояние от ОТС до границы промежуточной и дальней волновой зоны распространения информативного сигнала;

E_c и $E_ш$*, (мкВ/м)* – напряженности поля информативного сигнала и помех на *i*-й частоте

К – параметр, информация о значения которого является информацией ограниченного доступа и не может быть приведена в рамках настоящей диссертационной работы.

При расчете возможных расстояний распространения информативного сигнала за счет магнитной составляющей электромагнитного поля в формуле используют значения ρH_c и $\rho H_ш$, в мкА/м.

Таким образом, в формуле параметры *П* и *L* зависят от условий проведения измерений и свойств исследуемых ОТС КСИИ (частот излучения). Параметр *К* – величина зависящая от того, содержит ли исследуемые ОТС в своем составе монитор или нет. Так как коэффициент *К* непосредственно присутствует в дроби отношения сигнал/шум, можно сделать вывод, что это есть норма отношения сигнал/шум, при выполнении которой ОТС КСИИ считаются защищенными.

Следовательно, можно предположить, что при выполнении отношения сигнал/шум на границе КЗ с значениями *К* меньшими, чем значения приведенные в соответствующих НМД ФСТЭК (Гостехкомиссии) России, ОТС КСИИ будут защищены от утечки за счет ПЭМИ.

Теперь требуется рассчитать фактическое отношение сигнал/шум на границе КЗ. При установке средств активной защиты в непосредственной близости от защищаемого ОТС КСИИ, можно считать, что коэффициент затухания информативного сигнала и шума при распространении

до границы КЗ будет одинаковым. А, следовательно, отношение сигнал/шум будет постоянным на всей трассе распространения информативного сигнала.

Следовательно, в таком случае, достаточно измерить и рассчитать уровень информативного сигнала, а также измерить и рассчитать уровень шумовой помехи на каждой из частот ПЭМИ. Далее, по формуле 2, требуется определить отношение сигнал/шум на каждой из частот:

$$\Delta_i = \frac{E_{c_i}}{E_{ш_i}}, \qquad (2)$$

где E_c и $E_{ш}$, *(мкВ/м)* – напряженности поля информативного сигнала и помех на *i*-й частоте.

Теперь полученные величины требуется сравнить с нормами. Если на всех частотах обнаруженных ПЭМИ выполняется норма отношения сигнал/шум, то ОТС КСИИ можно считать защищенным (для случаев, когда генератор пространственного шума находится в непосредственной близости от ОТС КСИИ и не используется экранирование помещений КСИИ). Если хотя бы на одной из частот норма не выполняется – не защищены.

Что касается пространственного затухания сигнала (шума), то процесс его расчета может осуществляться в соответствии с положениями, приведенными в диссертационной работе.

Также в диссертационной работе приводится информация о разработанной оригинальной методике оценки защищенности ОТС от утечки информации за счёт наводок, возникающих во вспомогательных технических средствах (ВТС) КСИИ под воздействием информативного сигнала от ОТС, на токоведущие коммуникации: сеть электропитания, заземления или др. (технический канал утечки информации), выходящие за пределы КЗ. Разработанная методика в отличие от действующей и применяемой на практике методики, изложенной в документах ФСТЭК (Гостехкомиссии) России, позволяет осуществлять корректную оценку защищенности ОТС, защищенных с использованием средств активной защиты.

Корректность разработанных оригинальных методик была подтверждена в результате проведенного эксперимента – специальных исследований на ПЭМИН.

В четвертой главе осуществлена разработка UML-моделей для процессов управления ИБ, которые организованы на основе расширенной PDCA-модели обеспечения и управления ИБ КСИИ, разработанной во второй главе диссертационной работы. Также осуществлена разработка оригинальных предложений по реализации технических подсистем СИБ КСИИ. Кроме того, произведена разработка оригинальной методики оценки эффективности применения СИБ КСИИ.

Процессная (организационная) составляющая является одной из главных составляющих при создании эффективных СИБ КСИИ. В данном подразделе приводится процессно-ролевая модель СИБ КСИИ, разработанная с применением языка UML с помощью инструментального средства Enterprise Architector. Модель состоит из процессов управления ИБ и эксплуатационных процессов обеспечения ИБ СИБ КСИИ, которые организованы на основе EPDCA-модели обеспечения и управления ИБ КСИИ, разработанной в главе 2 диссертационной работы. Использование языка UML при моделировании процессов СИБ КСИИ позволяет представлять сложные процессы в наглядном, понятном и строго формализован виде.

В качестве примера приведем общую UML-модель для процессов домена «Совершенствование», разработанной EPDCA-модели обеспечения и управления ИБ КСИИ. Данная модель приведена на рисунке 4.

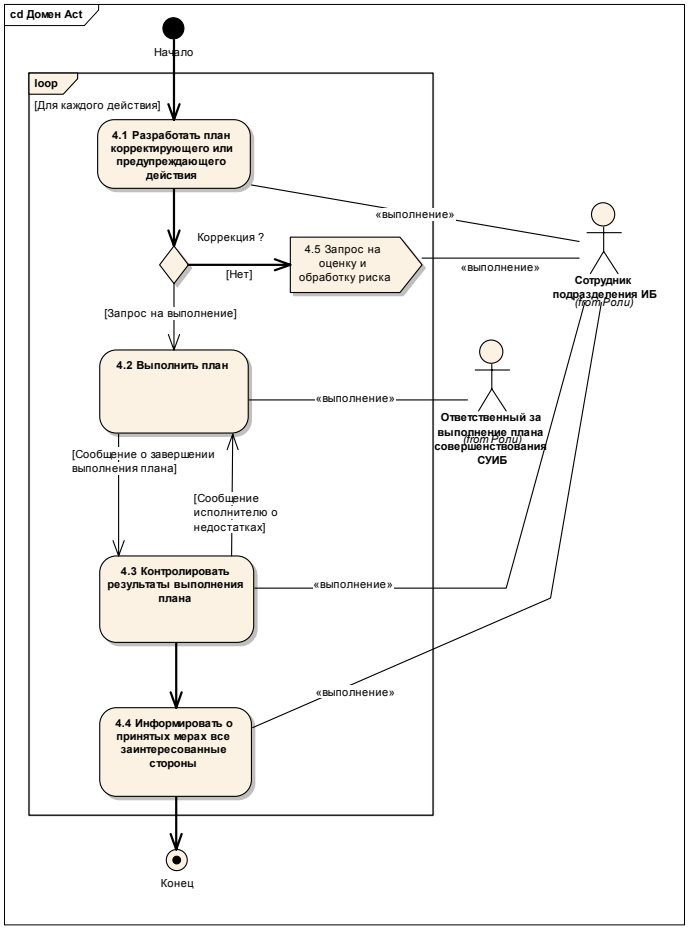

Рисунок 4 – Общая UML-модель процессов домена «Совершенствование»

Технические подсистемы, в состав которых включаются технические, программные и/или программно-технические средства защиты информации, являются неотъемлемой частью СИБ КСИИ. В главе 4 приводятся решения по реализации технических подсистем СИБ КСИИ, предназначенных для компенсации рисков реализации современных компьютерных атак, направленных на активы КСИИ, смоделированных с использованием методологии деревьев атак, разработанной в рамках главы 2 диссертационной работы.

Для эффективного обеспечения ИБ КСИИ в рамках СИБ КСИИ должны реализовываться следующие технические подсистемы ИБ: подсистема межсетевого экранирования, подсистема обнаружения и предотвращения вторжений, подсистема управления событиями ИБ, подсистема защиты от утечек конфиденциальной информации, подсистема антивирусной защиты и антиспам защиты.

Оценка соответствия СИБ КСИИ установленным требованиям должна осуществляться следующим образом.

Процессы ИБ разделяются на две группы: процессы управления ИБ КСИИ и процессы обеспечения ИБ КСИИ (эксплуатационные процессы). Рассмотрим КСИИ, в которой выделены 32 процесса управления и обеспечения ИБ.

Для оценки уровня ИБ организации используются групповые и частные показатели. Групповой показатель используется для каждой группы процессов ($K_{ГП(i)}$). Оценка конкретного процесса осуществляется с использованием частного показателя ($K_{П(i,j)}$), который детализирует общую оценку.

Оценка $K_{П(i,j)}$ частного показателя формируется по результатам экспертного оценивания степени реализации процесса. При этом частному показателю $K_{П(i,j)}$ присваиваются следующие значения:

0 – не реализовано;

0,25, 0,5 или 0,75 – частично реализовано;

1 – реализовано полностью.

Оценка группового показателя ($K_{ГП(i)}$) вычисляется из оценок входящих в него частных показателей ($K_{П(i,j)}$) с учетом коэффициентов значимости, $в(i,j)$ определяющих важность частного показателя для оценивания группового показателя:

$$K_{ГП(i)} = \sum_{j} в(i,j) \cdot K_{П(i,j)} ,$$

где

$j = 1 - N_i$,

N_i – количество частных показателей ИБ, входящих в групповой показатель.

При учете коэффициентов значимости показателя осуществляется нормировка в соответствии с условием:

$$\sum_{j=1}^{k} в(i,j) = 1 ,$$

где *k* – число частных показателей в *i*-ом групповом показателе.

При осуществлении оценивания выполняется анализ нормативных, распорядительных, программных и других документов организации, имеющих отношение к проверяемым областям ИБ, а также уточнение полученной информации с помощью опросов сотрудников организации и наблюдения за деятельностью.

Оценки $K_{ГП(i)}$, полученные в результате оценивания групповых показателей ИБ, отображаются на круговой диаграмме в соответствующих секторах *i*, отстающими от центра круговой диаграммы на величину, соответствующую значению оценок.

Результирующая оценка по направлению «процессы управления системой ИБ» ($P_{УИБ}$) или «процессы эксплуатации системы ИБ» ($P_{ОИБ}$) вычисляется как наименьшее значение из входящих в каждое направление групповых показателей.

На диаграмме значения $P_{УИБ}$ и $P_{ОИБ}$ отображаются в виде дуг, отстающих от центра диаграммы на величину, соответствующую вычисленным значениям.

Общий уровень реализации процессов ИБ (P) вычисляется как наименьшее из значений $P_{УИБ}$ и $P_{ОИБ}$ и приводится на круговой диаграмме, представленной на рисунке 5.

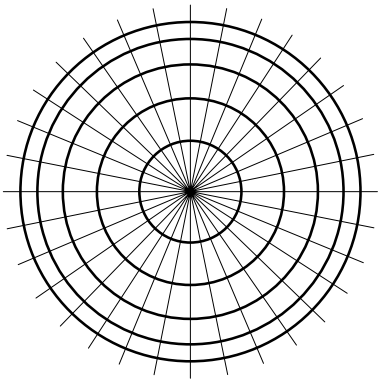

Рисунок 5 – Круговая диаграмма для отображения результатов оценивания

В заключении приводятся основные результаты проведенных исследований и вытекающие из них выводы, указаны направления дальнейших исследований. Описываются аспекты разработанных методов обеспечения ИБ КСИИ с использованием ДА.

Основные результаты диссертационной работы:

1. Проведен критический анализ существующих моделей и методов, используемых для обеспечения ИБ КСИИ, выявление их недостатков и ограничений в применении.
2. Осуществлена разработка оригинальной расширенной EPDCA-модели СИБ КСИИ, а также разработка расширенного параллельного автомата для моделирования и обнаружения фактов реализации атак на КСИИ (на этапе «Планирование» EPDCA-цикла управления и обеспечения ИБ КСИИ) на базе методологии деревьев атак.
3. Разработаны оригинальные методики оценки защищенности информации обрабатываемой в КСИИ от утечки за счет ПЭМИН при использовании средств/методов активной и/или пассивной защиты КСИИ.
4. Разработана оригинальная процессно-ролевая модель СИБ КСИИ применительно к ключевым процессам управления ИБ.
5. Разработана оригинальная методика оценки уровня соответствия КСИИ установленным требованиям по ИБ с учетом предлагаемых к внедрению в рамках СИБ КСИИ эксплуатационных процессов ИБ (процессов обеспечения ИБ).

Список публикаций по теме диссертации:

1. Липатов А.Л., Гирин С.Н. ТРЕБУЮТСЯ КОНТРОЛЕРЫ. Практические вопросы контроля защищенности корпоративных сетей. Защита информации. Инсайд. № 5 2005 г.
2. Липатов А.Л., Русинов А.Н., Салмин Е.А. Оценка и управление рисками ИТ-безопасности в информационных системах. Научно-технический вестник СПБГУ ИТМО. Выпуск 29. I сессия научной школы «Информационная безопасность, проектирование, технология элементов и узлов компьютерных систем» / Главный редактор д.т.н., профессор В.Н. Васильев – СПб: СПбГУ ИТМО, 2006. - 280 с. (**из перечня ВАК РФ**).
3. Липатов А.Л., Салмин Е.А., Русинов А.Н. Применение стандарта 802.1x для контроля доступа в локальную вычислительную сеть. Научно-технический вестник СПБГУ ИТМО. Выпуск 29. I сессия научной школы «Информационная безопасность, проектирование, технология элементов и узлов компьютерных систем» / Главный редактор д.т.н., профессор В.Н. Васильев – СПб: СПбГУ ИТМО, 2006. - 280 с. (**из перечня ВАК РФ**).
4. Липатов А.Л., Гирин С.Н. НАСТРОЙКА СЕРТИФИЦИРОВАННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ MICROSOFT. Защита информации. Инсайд. № 5 2006 г.
5. Липатов А.Л., Осломенко Д.В. Законодательные требования в области обеспечения информационной безопасности автоматизированных систем. Сборник тезисов IV межвузовской конференции молодых ученых. – СПб: СПбГУ ИТМО, 2007. - 165 с.
6. М.В. Масленников, А.Л. Липатов, Э.В. Белов. Особенности обеспечения информационной безопасности промышленных систем. Сборник тезисов IV межвузовской конференции молодых ученых. – СПб: СПбГУ ИТМО, 2007. - 165 с.
7. Липатов А.Л. Двенадцатая Санкт-Петербургская ассамблея молодых ученых и специалистов. Аннотации работ победителей конкурсов грантов Санкт-Петербурга 2007 года для студентов, аспирантов и молодых кандидатов наук. – СПб.: Изд-во РГГМУ, 2007. с. 70.
8. Липатов А.Л., Ершов В. В. Контроль критичных бизнес-процессов средствами информационной безопасности. – М.: ЭСКПО, № 4 (116) июль-август 2008. с. 6-7.
9. Липатов А.Л. Персональные данные: современные требования законодательства России в сфере обеспечения их безопасности. – М.: IT-Manager, сентябрь 2008.