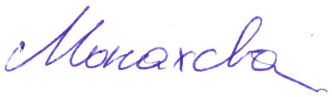
Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»

На правах рукописи



Монахова Мария Михайловна

МОДЕЛИ И АЛГОРИТМЫ КОНТРОЛЯ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОРПОРАТИВНОЙ ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ

Специальность: 05.12.13 – Системы, сети и устройства телекоммуникаций

Автореферат
диссертации на соискание ученой степени
кандидата технических наук

Владимир 2016

Работа выполнена в ФГБОУ ВО «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»

Научный руководитель: **Никитин Олег Рафаилович**
Заслуженный деятель науки РФ,
доктор технических наук, профессор, заведующий кафедрой радиотехники и радиосистем ФГБОУ ВО «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»

Официальные оппоненты: **Цимбал Владимир Анатольевич**
Заслуженный деятель науки РФ,
доктор технических наук, профессор, профессор кафедры «Автоматизированные системы управления» Военной академии РВСН имени Петра Великого, г. Серпухов
Ложников Павел Сергеевич
кандидат технических наук, доцент,
заведующий кафедрой «Комплексная защита информации» ФГБОУ ВО «Омский государственный технический университет», г. Омск

Ведущая организация: ФГБОУ ВО «Рязанский государственный радиотехнический университет», г. Рязань

Защита диссертации состоится « 23 » июня 2016 г. в « 16 » часов в ауд. 301-3 на заседании диссертационного совета Д 212.025.04 при Владимирском государственном университете имени Александра Григорьевича и Николая Григорьевича Столетовых по адресу: 600000, г. Владимир, ул. Горького, 87, ВлГУ, ФРЭМТ.

С диссертацией можно ознакомиться в библиотеке ФГБОУ ВО «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых» и на сайте http://diss.vlsu.ru.

Автореферат разослан «18» апреля 2016г.

Отзывы на автореферат, заверенные печатью, просим направлять по адресу: 600000, г. Владимир, ул. Горького, 87, ВлГУ, ФРЭМТ

Ученый секретарь диссертационного совета,
доктор технических наук, профессор Самойлов А.Г.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. Содержание проблемы информационной безопасности (ИБ) в системах и сетях телекоммуникаций интерпретируются следующим образом. По мере развития и усложнения средств, методов и форм автоматизации процессов обработки и передачи информации повышается уязвимость системных процессов и ресурсов, напрямую влияющая на возможность уничтожения, блокирования или искажения информации и появления в системе «нештатных» процессов, создающих ситуацию невозможности эффективного выполнения основных функций. Политики обеспечения ИБ, и создаваемые на их основе системы защиты информации (СЗИ), не могут полностью гарантировать защиту информационно-телекоммуникационной сети. После внедрения защитных мер и средств всегда остаются уязвимые места в сети, которые могут сделать обеспечение ИБ неэффективным. Кроме того, могут быть сбои и отказы самой СЗИ, выявляться новые, ранее не идентифицированные угрозы. Ситуации, связанные с «замеченными» нарушениями политики ИБ и отказы СЗИ в выполнении своих функций, определяют понятие «инцидента ИБ». Причинами возникновения инцидентов ИБ являются архитектурные просчеты, ошибки реализации программных и аппаратных компонентов, преднамеренные информационных воздействия, ошибки пользователей (операторов), старение оборудования и т.д. Несмотря на интеграцию в телекоммуникационные сети современных аппаратно-программных средств защиты и управления сетями, процессы контроля инцидентов ИБ автоматизированы лишь частично, отсутствуют эффективные модели и алгоритмы их обнаружения и идентификации в составе единой системы, что часто является основной причиной продолжительному снижению эффективности функционирования телекоммуникационной сети. Таким образом, исследования, направленные на создание моделей и алгоритмов контроля инцидентов, актуальны и имеют практическое значение в решении проблемы обеспечения качества функционирования сетей телекоммуникаций предприятий.

Степень разработанности темы. Проблема ИБ и защиты информации в системах и сетях телекоммуникаций исследовалась в трудах ведущих российских ученых Белова Е.Б., Галкина А.П., Герасименко В.А., Грушо А.А., Домарева В.В., Завгороднего В.И., Зегжды П.Д., Лося В.П., Лукацкого А.В.,

Малюка А.А., Медведковского И.Д., Молдовяна А.А., Никитина О.Р., Петракова А.В., Полушина П.А., Самойлова А.Г., Соколова А.В., Торокина А.А., Шаньгина В.Ф., Шелухина О. И., Хорева А.А., Ярочкина В.И. Значительный вклад в решение выделенной проблемы внесли зарубежные исследователи Р. Брэтт, К. Касперски, С. Норкатт, В. Столингс, К. Лендвер, M. Howard, R. Graham, D. Sanai, S. Manwani, M. Montoro, F. Cohen, J. Jung , D.Moore, C.Zou и другие.

Анализируя результаты исследований, можно сделать вывод, что существующие методы и средства обеспечивают существенное повышение защищенности телекоммуникационных сетей. Тем не менее, выработка решений по большинству функций защиты производится по-прежнему человеком (администратором сети), несмотря на интеграцию в телекоммуникационные сети современных аппаратно-программных средств администрирования и управления сетями, наличие отечественных (ГОСТ Р ИСО/МЭК ТО 13335-5-2006, ГОСТ Р ИСО/МЭК 7498-4-99, ГОСТ Р ИСО/МЭК 10164-1-99) и международных (ITU-T X.700, ISO 7498-4 FCAPS, ISO/IEC TR 18044, CMU/SEI-2004-TR-015) стандартов, процессы контроля инцидентов ИБ автоматизированы лишь частично, отсутствуют эффективные модели и алгоритмы их обнаружения и идентификации в составе единой системы, что часто является основной причиной продолжительному снижению эффективности функционирования телекоммуникационной сети.

Объект исследования - корпоративные телекоммуникационные сети (КТС).

Предмет исследования - методы и средства, позволяющие обеспечить контроль инцидентов ИБ в КТС, обусловленных нарушением политики ИБ.

Цели и задачи работы. Целью работы является решение научно-технической задачи разработки новых моделей, алгоритмов и процедур контроля инцидентов ИБ, направленных на повышение эффективности обеспечения информационной безопасности в системах и сетях телекоммуникаций. В соответствии с целью были поставлены и решены следующие научные задачи:

1. Анализ процессов, методов и средств обеспечения контроля инцидентов ИБ в КТС, классификация инцидентов по характеру нарушения техниче-

ской политики ИБ.

2. Разработка методики определения множества существенных факторов возникновения инцидентов ИБ.

3. Разработка моделей и алгоритмов формирования пакетов контролируемых параметров, процедур обнаружения инцидентов ИБ в КТС.

4. Синтез структурной схемы системы контроля инцидентов ИБ в КТС. Реализация функциональных модулей системы контроля и их практическое внедрение в КТС предприятий и организаций.

Научная новизна. В работе получены следующие научные результаты:

1. Предложена формальная модель инцидента ИБ, как специфичного состояния КТС, идентифицируемого по отклонениям параметров ее функционирования от эталонных значений, задаваемых технической политикой ИБ.

2. Разработана методика определения существенных факторов возникновения инцидентов ИБ, в основе которой использован способ группового ранжирования факторов при обеспечении согласованности экспертов.

3. Разработан алгоритм формирования пакета контроля инцидентов ИБ в КТС, основанный на анализе статистических характеристик обнаружения событий ИБ по значениям контролируемых параметров, выделении комбинаций, обеспечивающих допустимые вероятностные характеристики обнаружения.

4. Предложена структурная схема автоматизированной системы контроля инцидентов ИБ, как основа для практической реализации систем данного класса.

Практическая значимость работы. Разработано информационное и программное обеспечение системы контроля инцидентов ИБ, включающее: программный комплекс для расчета значимости элементов корпоративной сети передачи данных (св-во о гос. регистрации программы для ЭВМ №2012612368); программный комплекс администрирования корпоративной сети передачи данных DTNAM v1.0 (св-во о гос. регистрации программы для ЭВМ №2012660376); автоматизированную систему расчета статических характеристик инцидентов информационной безопасности КСПД АСУП (св-во о гос. регистрации программы для ЭВМ №2012660377); программный модуль СППР административного управления корпоративной АСУ расчета показате-

лей значимости ресурсов программно-технической инфраструктуры (св-во о гос. регистрации программы для ЭВМ №2013613706); программный модуль имитационного моделирования процессов администрирования СППР административного управления корпоративной АСУ (св-во о гос. регистрации программы для ЭВМ №2013613706); автоматизированную систему анализа защищенности объекта информатизации SaNaS 1.0 (св-во о гос. регистрации программы для ЭВМ №2014610966) и ее базу данных (св-во о гос. регистрации базы данных №2014620496); автоматизированную систему расчета статистических характеристик инцидентов информационной безопасности КСПД (св-во о гос. регистрации программы для ЭВМ №2015618341); автоматизированную систему регистрации инцидентов информационной безопасности КСПД (св-во о гос. регистрации программы для ЭВМ №2015618785).

Использование разработанных средств позволяет снижать общее количество анализируемых параметров для выявления инцидентов в 1.5 – 2,5 раза; уменьшать среднее время ожидания заявки пользователей, обнаруживших проявление инцидента ИБ, на обработку - на 33%, среднее время выполнения функции устранения инцидента - на 25**%.** Кроме того, в корпоративной сети уменьшается общее количество инцидентов. Результаты исследований внедрены в корпоративной телекоммуникационной сети ОАО ВЗ «Электроприбор» г. Владимир, сети передачи данных администрации Владимирской области, использованы в технических мероприятиях по обеспечению ИБ ООО «НПП «ИНПРОКОМ» г. Балакирево Владимирской обл., а также были использованы при разработке учебных курсов на кафедре радиотехники и радиосистем во Владимирском государственном университете.

Методология и методы исследования. При решении поставленных задач применялись: анализ процессов контроля инцидентов, синтез и моделирование алгоритмов и процедур обработки информации в сетях телекоммуникаций. Научные положения работы теоретически обосновываются с помощью аппарата теории множеств, теории графов, теории вероятностей, алгебры логики, теории статистического обнаружения, математической статистики.

Положения, выносимые на защиту:

- формальная модель инцидента ИБ в КТС, обеспечивающая теоретическое обоснование построения систем контроля инцидентов ИБ;

- методика определения множества существенных факторов возникновения инцидентов ИБ, позволяющая снижать количество контролируемых параметров для выявления инцидентов;

- алгоритм формирования пакетов контролируемых параметров, обеспечивающий повышение производительности системы контроля;

- структурная схема и результаты внедрения программных модулей системы контроля инцидентов, позволяющие разрабатывать системы данного класса.

Степень достоверности результатов исследований. Достоверность полученных в диссертационной работе результатов подтверждается с помощью исследований КТС, выполненных на экспериментальной установке, воспроизводящей условия возникновения инцидентов в КТС, а также в ходе практического использования разработанных средств.

Апробация работы. Материалы диссертационной работы докладывались и обсуждались на XXIX, XXX и XXXIII Всероссийской НТК «Проблемы эффективности и безопасности функционирования сложных технических и информационных систем» (Серпухов, 2010, 2011, 2014); IX Международном симпозиуме «Интеллектуальные системы, INTELS 2010» (Владимир, 2010); XXIII Международной НТК «Математические методы в технике и технологиях - ММТТ-23» (Смоленск, 2010); XVI Международной НТК «Проблемы передачи и обработки информации в сетях и системах телекоммуникаций» (Рязань, 2010); XII Международной конференции «Региональная информатика (РИ-2010)» (Санкт-Петербург, 2010); XVII Международной НТК «Информационные системы и технологии ИСТ-2011» (Нижний Новгород, 2011); IX Международной НТК «Перспективные технологии в средствах передачи информации» (Владимир, 2011); V, VI VII Всероссийской научно-практической конференции «Имитационное моделирование. Теория и практика ИММОД» (Санкт-Петербург, 2011, Казань, 2013, Москва, 2015); X Российской НТК «Новые информационные технологии в системах связи и управления» (Калуга, 2011); Всероссийской с международным участием молодежной научно-практической конференции «Молодежная математическая наука-2012» (Саранск, 2012); XIX Міжнародноі науково-практичноі конференціі «Інформаційні технологіі: наука, техніка, технологія, освіта, здоров'я» (Ук-

раина, Харьков, 2011); XI Міжнародноі науково-технічноі конференціі «Проблеми інформатики і моделювання» (Украина, Харьков-Ялта, 2011); Международной научно-практической конференции «The Strategies of Modern Science Development» (Yelm, WA, USA, 2013); IV Международной научно-практической конференции «Вопросы науки: Современные технологии и технический прогресс» (Воронеж, 2015).

Публикации: опубликовано 28 работ, 5 в изданиях из перечня ВАК, из них 1 проиндексирована в международной базе Scopus. Получено 9 свидетельств о государственной регистрации программ для ЭВМ.

Личный вклад. Все результаты, изложенные в диссертации, получены автором лично или при его непосредственном участии. Постановка цели и задач, обсуждение планов исследований и результатов выполнены совместно с научным руководителем.

Структура и объем диссертационной работы. Диссертация состоит из введения, четырех глав, заключения, списка использованных источников из 138 наименования, приложений и содержит 108 страниц основного текста, иллюстрированного 9 рисунками, содержит 25 таблиц.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** формулируется цель и задачи исследования, обосновывается актуальность, научная новизна работы и практическая значимость результатов.

В **главе 1** «*Инциденты информационной безопасности в корпоративных информационно - телекоммуникационных сетях. Анализ объекта исследования*» рассматриваются аспекты контроля инцидентов в КТС, обусловленных нарушением технической политикой ИБ (ТПИБ).

Формальная модель инцидента ИБ в КТС

Пусть наблюдаемая КТС может находиться в одном из N состояний $S=\{S_n\}, n=\overline{1,N}$. Каждое состояние описывается вектором из M параметров $S_n=(p_1,p_2,\ldots,p_m,\ldots,p_M)_n$. Задачей контроля является определение текущих значений параметров, и по ним - обнаружение состояний $S^* \in S$, которые сопоставляются с наличием инцидента. Пусть известно $M^* \leq M$ параметров, по которым возможно идентифицировать состояния S^*. Эти параметры назовем

параметрами инцидентов (ПИн). В каждом множестве возможных значений параметров выделим подмножества значений, установленных ТПИБ. Такое подмножество назовем *шаблоном безопасности.* Отклонение значения параметра от шаблона связывается с возможностью реализации угрозы ИБ. Введем простое высказывание «Значение ПИн отличается от шаблона». Поставим ему в соответствие логическую переменную X_m и назовем ее *событием информационной безопасности* (СоИБ). Инцидент ИБ – это сложное логическое высказывание, состоящее из многих СоИБ, истинность которого проверяется системой контроля. Для каждого вида инцидента v поставим в соответствие логическую функцию Y_v , истинность которой по текущим значениям X_m показывает факт наличия инцидента.

Каждый раз при осуществлении контроля производить сравнение шаблонов и значений всех параметров во всех узлах КТС не рационально: на проведение такого контроля требуются существенные вычислительные и временные ресурсы, которые отнимаются у КТС, что может приводить к существенному снижению ее производительности. Поэтому в процедурах контроля, оптимизируемых по временным критериям, среди всех параметров проверки выделяется подмножество наиболее критичных, только они подлежат контролю. В связи с этим вводится понятие пакета контроля (ПК) с $M_k \le M^*$ контролируемых параметров.

Задача контроля - определить значения Y_v за минимальное время, что означает нахождение минимальных ПК по каждому виду инцидента, определения минимального времени на контроль каждого параметра пакета, которые в совокупности обеспечат требуемое качество обнаружения инцидента. Так как определение значений ПИн подвержено случайным воздействиям в узлах КТС, и требуется минимизировать время контроля, то для каждого «измерителя» параметра задаются характеристики обнаружения X_m за время не более t_j: функции $p_m(t \le t_j)$, $q_m(t \le t_j), t_j = \overline{1,T}$ вероятностей корректного и «ложного» обнаружения. Вследствие этого качество обнаружения инцидента связывается с граничными вероятностями корректного и «ложного» обнаружения инцидента.

В **главе 2** «*Разработка методики определения множества существенных факторов возникновения инцидентов информационной безопасности*» на **первом этапе** выделяются виды инцидентов, с ними связываются совокупность нарушенных мер защиты (НМЗ). Факторы возникновения инцидентов рассматриваются как причины нарушения профиля работы соответствующего средства защиты (СЗ), заданного шаблоном ИБ в ТПИБ (средства ОС, антивирусной защиты (АВЗ), защиты от НСД, шифрования (Ш), аутентификации (А), экранирования (Э), IDS, VLAN, VPN). В работе предлагается пять видов инцидентов ИБ, 7 НМЗ и 30 факторов. В таблице 1 приведены СЗ, нарушение профиля работы которых приводит к НМЗ и, соответственно, к инциденту определенного вида.

Таблица 1 – Соответствие «Вид инцидента – Нарушенные меры защиты»

Вид инцидента / Нарушенная мера защиты	«Не устранены условия возникновения угроз»	«Не обнаружена реализация угрозы»	«Нет защиты от реализованной угрозы»	«Реализация неизвестной угрозы»	«Не устраняется воздействие реализации угрозы»
«Нарушены механизмы идентификации и аутентификации»	ОС, НСД, А, Э, VPN VLAN	ОС, СД, А,VLAN, Э, VPN	-	-	-
«Нарушены механизмы контроля и разграничения доступа к защищаемым ИР»	ОС, НСД, А, IDS	ОС, А, НСД, IDS	ОС, А, НСД, IDS	-	ОС, НСД, А, IDS
«Нарушены механизмы контроля и разграничения доступа к сетевым ресурсам»	ОС, НСД, А, Э, VPN VLAN,	-	-	-	ОС, НСД, А, Э, VLAN, VPN
«Нарушены механизмы защиты от вредоносных программ»	-	АВЗ, IDS	АВЗ. IDS	-	-
«Нарушены механизмы защиты внутренних каналов связи»	-	Ш, VLAN	Ш, VLAN	Ш, VLAN	Ш, VLAN
«Нарушены механизмы защиты внешних каналов связи»	Ш, Э, VLAN	Ш, Э, VLAN	Ш, Э, VLAN	Ш, Э, VLAN	Ш, Э, VLAN
«Нарушены механизмы защиты от удаленных атак»	-	АВЗ, НСД, Э, VLAN, VPN	АВЗ, НСД, Э, VLAN, VPN	АВЗ, НСД, Э, VLAN, VPN	АВЗ, НСД, Э, VLAN, VPN

На **втором этапе** в соответствии с нижеследующим алгоритмом выполняется экспертный анализ факторов с целью уменьшения их числа и распределения по видам инцидентов (для простоты рассматривается один вид инцидента)

Шаг 1. Сформировать $\Phi = \{\phi_k\}, k = \overline{1,K}$ - множество факторов нарушения действующей ТПИБ. Выделить НМЗ в соответствии с таблицей 1.

Шаг 2. По каждой НМЗ:

- получить матрицу рангов $\|\chi_{kz}\|$ факторов группой из Z экспертов ($z = \overline{1,Z}$), $\chi_{kz} \in \{1,\ldots,K\}$, чем меньше ранг, тем существеннее фактор;

- по каждому фактору вычислить медиану ($\tilde{\chi}_k = med\{\chi_{kz}\}$) их рангов, ранжировать факторы по $\tilde{\chi}_k$;

- проверить степень согласованности мнений экспертов (по коэффициенту конкордации), если согласованность не соблюдена, то изменить исходные факторы и/или группу экспертов, переход к шагу 1.

Шаг 3. По каждой НМЗ выделить факторы с максимальным рангом ($\tilde{\chi}_k \le 2$) - множество существенных факторов (СФ) $\Phi_{C\Phi}$.

Шаг 4. Объединить множества СФ по всем НМЗ. Конец алгоритма.

Практическое применение методики позволяет уменьшить количество факторов по каждому виду инцидентов в 1.5 – 2,5 раза. Данный «выигрыш» зависит от особенностей конкретной КТС и действующей технической политики.

В **главе 3** «*Разработка математических моделей и алгоритмов оптимизации контроля инцидентов информационной безопасности*» разрабатываются модели формирования ПК. Пусть контролируется один вид инцидента. Исходные данные: i ($i = \overline{1,I}$) - номер узла КТС; j ($j = \overline{1,J}$) - номер контролируемого параметра; t_{ij} - затраты времени на определение СоИБ x_{ij}; функции вероятностей корректного и «ложного» обнаружения x_{ij}, заданные массивами $\|p_{kt}\|, \|q_{kt}\|, k = 1,\ldots,K; K = I \times J;\ t = 1,\ldots,T.$ Требуется - определить минимальный пакет контроля инцидента $M_{k\min}$, распределить контролируемые параметры по узлам.

Алгоритм формирования пакета контроля инцидента

Шаг 1. Задать матрицу $\|\eta_{ij}\|$ наличия контролируемого параметра j в узле i, P^* и Q^* - граничные вероятности корректного и «ложного» обнаружения инцидента; пусть $M_k = K$.

Шаг 2. Сформировать массивы $\|P_{lt}\|$ и $\|Q_{lt}\|, l = 0,...,(2^{M_k} - 1), t = \overline{1,T}$, вычисляя их значения по комбинации X_k в соответствии с номером набора событий l. Наборы будем обозначать $\Psi_{lt}^{M_k}$. Получить массив $\|\zeta_{lt}\|$, где $\zeta_{lt} = P_{lt} / Q_{lt}$.

Шаг 3. Отобрать множество наборов событий Ψ по правилу: $\psi_l^{M_k} \in \Psi$, если $\zeta_{lt} \geq P^* / Q^*$, $l = 0,...,(2^{M_k} - 1), t = \overline{1,T}$. Каждому набору из Ψ поставить в соответствие $P_{lt_{min}}$. Выполнить сортировку Ψ по убыванию $P_{lt_{min}}$.

Шаг 4. Если $\sum_{\psi} P_{lt_{min}} < P^*$, то конец алгоритма (задача не решена).

Шаг 5. Начиная с $l = |\psi|$ пока ($l \geq 0$ или $\sum_{\psi} P_{lt_{min}} \geq P^*$) $\Psi = \Psi \setminus \psi_l^{M_k}$ (удалять элементы с малыми значениями $P_{lt_{min}}$).

Шаг 6. Выполнить минимизацию логической функции, образованной дизъюнкцией термов в Ψ. Число оставшихся логических переменных определяет значение $M_{k\,min}$. Конец алгоритма.

Алгоритм назначения параметрам времени на контроль

Шаг 1. Для всех $t = \overline{1,T}$ вычислить $T_r = \sum_{k=1}^{K} t_r(X_k)$ и P_r, здесь $r = \overline{1,R}$ - номер набора, $t_r(X_k)$ - значение времени контроля при данном наборе.

Шаг 2. Отобрать множество $\hat{R}$ наборов $t_r(X_k)$ по правилу: $r \in \hat{R}$, если $P_r \geq P^*$. Оптимальный набор имеет номер минимального числа из $\hat{R}$. Конец алгоритма.

В **главе 4** «*Разработка и анализ эффективности системных средств контроля инцидентов информационной безопасности в корпоративной информационно-телекоммуникационной сети*» предлагается **структурная схема**

системы контроля инцидентов ИБ в ИТКС (рисунок 1), описывается алгоритм ее функционирования, рассматриваются подходы к ее практической реализации. На схеме выделены: блок управления измерителями (БУИ), блок хранения профиля (БХП), блок хранения статистических характеристик измерителей (БХСХИ), блок хранения дистрибутивов измерителей (БХДИ), блок управления (БУ) решающий блок (РБ), блок временного хранения данных (БВХД), блок хранения параметров архитектуры (БХПА), блок формирования программы «решения» инцидента (БФПРИ) блок администраторов (БА), блок формирования отчетов (БФО). На схеме обозначены: $U=\{u_1,...,u_U\}$- узлы КИТС; PK - множество контролируемых ПИн; V - множество дистрибутивов измерителей, V^*- множество «настроенных» измерителей; $PK^{изм}$ - множество результатов; $PK^{эт}$ - «профиль» ТПИБ.

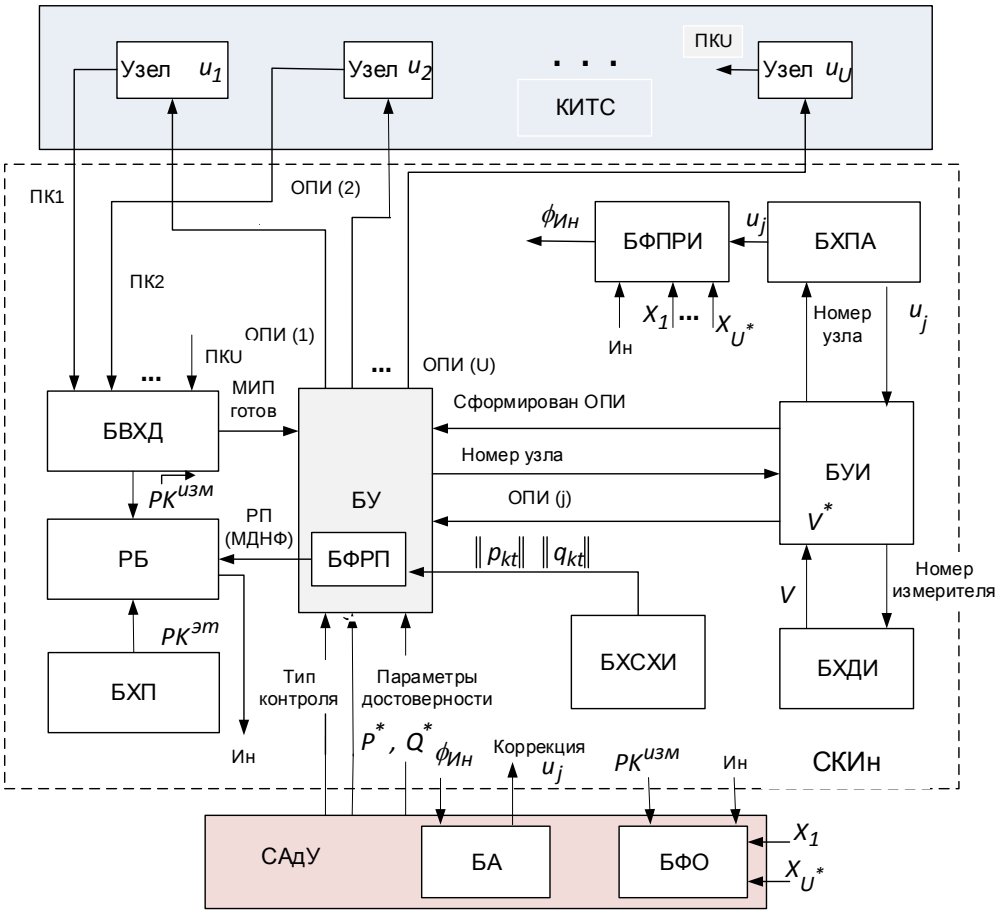


Рисунок 1 – Структурная схема системы контроля инцидентов

Алгоритм работы системы:

Шаг 1. Задание на контроль: вид инцидента, P^* и Q^*. Если требуется «тотальная» проверка, то на контроль определяются все M^* параметров.

Шаг 2. Выполнить процедуру формирования ПК (см. главу 3). В результате сформирован ПК с M_{kmin} в виде $\|t_{ij}\|, i=\overline{1,M_{kmin}}; j=\overline{1,U^*}; U^* \le U$ (U^* -

число узлов, отобранных для контроля, t_{ij} - время на контроль i-го ПИн в j -м узле). Если $t_{ij} = 0$, то параметр на конкретном узле не отобран для контроля.

Шаг 3. Процесс формирования массива «измеренных» параметров (МИП): сбросить «МИП готов»; отправить запрос на установление связи с узлом u_j; *time-out*. Если ответа нет, и истекло время ожидания, то сообщение «*Узел j не отвечает. Продолжить контроль?*». Если продолжение контроля возможно, то переход к шагу 4, иначе конец алгоритма.

Шаг 4. Процедура формирования общего пакета измерителей (ОПИ) для узла: «сбросить» «Сформирован ОПИ»; очистить предыдущий ОПИ; начиная с $i = 1$, пока ($i \le M_{kmin}$ и $t_{ij} \neq 0$) получать файлы дистрибутивов измерителей из БХДИ, «настраивая» их и добавляя в ОПИ. Выставить флаг «Сформирован ОПИ».

Шаг 5. Отправить ОПИ в u_j, *time-out*. Если продолжение контроля возможно, то переход к шагу 6, иначе конец алгоритма.

Шаг 6. Принять в БВХД файл результатов контроля ПК1, …, ПКU сохранить в j-й строке МИП. Если $j = U^*$, то выставить флаг «МИП готов», перейти к шагу 7; иначе перейти к анализу параметров следующего узла ($j = j + 1$) – к шагу 4.

Шаг 7. «Пуск РБ». Сравниваются $РК^{изм}$ с $РК^{эт}$, вычисляются логические функции Y_v по значениям $X_i, i \in M_{kmin}$; если $Y_v = 1$, то выставляется флаг «Обнаружен инцидент», прейти к шагу 8; иначе конец алгоритма.

Шаг 8. Инициировать процесс формирования программы «решения» инцидента. Выполняется БФПРИ: выбирается либо типовая программа, либо синтезируется новая - $\varphi_{ИН}$. Исполнить программу: передать программу в БА, ждать завершения. Сохранить исполненную программу. Конец алгоритма.

Измерители параметров инцидентов (ИПИ) – основные элементы системы контроля. Это программные модули, позволяющие определить значение параметра. ИПИ запускаются на удаленных устройствах (РС, сервер, АСО). Для определения характеристик обнаружения была создана экспериментальная установка

(рисунок 2). Принимались следующие соглашения: в процессе измерения используется «чистая» КТС (на систему не проводилось атакующих воздействий, ПО и аппаратные средства элементов функционируют без сбоев и т.п.); внешние условия (по отношению к наблюдаемому элементу) не изменяются (характер сетевого взаимодействия элемента неизменен на протяжении процесса функционирования); внутренние свойства системы, изменение которых может повлиять на показания измеряемых параметров, также оставались неизменными (списки пользователей и их права, набор установленного ПО и т.д.). Кроме того, необходимо выполнить требование того, чтобы компонент КТС, в отношении поведения которого проводится исследование, использовался достаточно интенсивно, чтобы выявление закономерностей в его работе стало возможным. На рисунке 3 в качестве примера приведены экспериментально полученные значения статистических характеристик обнаружения ИПИ №1 параметра «АВЗ не установлена и активирована на шлюзе доступа (HTTP, FTP трафик)» (а) и ИПИ №2 параметра «Имеется доступ к активному сетевому оборудованию не только у системного администратора» (б) (всего 12 ИПИ). Из других разработанных средств выделим программные комплексы для расчета значимости элементов КИТС, администрирования корпоративной сети, регистрации инцидентов ИБ, мониторинга состояния элементов КТС, АРМ диспетчера.

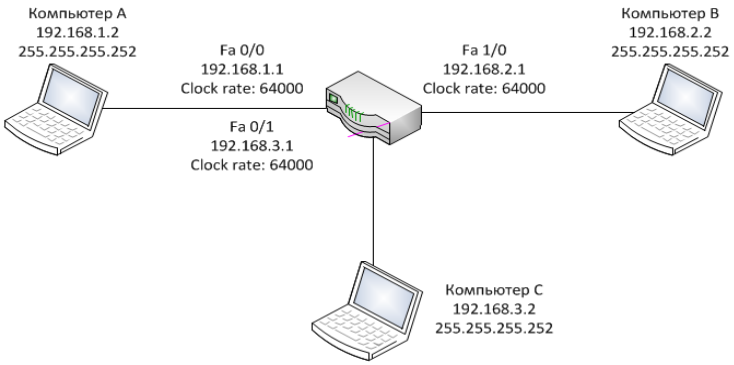


Рисунок 2 – Схема экспериментальной установки

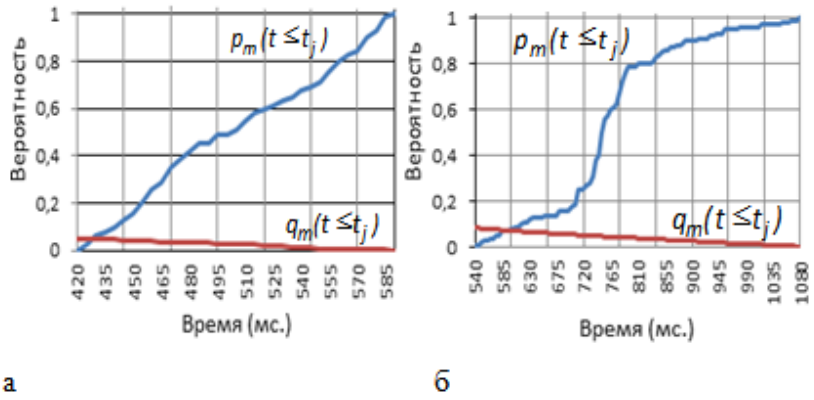


Рисунок 3 - Статистические характеристики обнаружения

Основные результаты диссертационного исследования:

1. Стандарты и руководящие документы, связанные с управлением инцидентами ИБ, не затрагивают технических вопросов построения систем контроля, не конкретизируют технических особенностей нарушений политики безопасности. Анализ средств автоматизации контроля инцидентов показал: инциденты, связанные с нарушением ТПИБ не систематизированы, средства сетевого управления имеют возможности по обнаружению событий ИБ, но алгоритмы их работы «закрыты», ими невозможно управлять.

2. Предложена формальная модель инцидента ИБ, как специфичного состояния КТС, идентифицируемого по отклонениям параметров ее функционирования от шаблонов, задаваемых ТПИБ. Задача эффективного контроля заключается в том, чтобы определить минимальный по количеству контролируемых параметров пакет, найти значения минимального времени на контроль каждого параметра.

3. Предложена классификация инцидентов ИБ по признаку «нарушение технической политики ИБ». Выделены характерные особенности инцидентов: «Не устранённая уязвимость», «Не обнаружена реализация угрозы», «Нет защиты от реализованной угрозы», «Реализация неизвестной угрозы», «Не устраняется воздействие реализации угрозы».

4. Разработана методика определения множества существенных факторов возникновения инцидентов ИБ. В основе методики использован способ «усечения» полного множества факторов нарушения ТПИБ. Выявляется взаимосвязь инцидентов разного типа с факторами нарушения конкретной технической политики, далее выполняется групповой экспертный анализ факторов, в основе которого использован способ группового ранжирования при обеспечении согласованности экспертов.

5. Разработан алгоритм формирования пакета контроля инцидентов ИБ, основанный на анализе статистических характеристик обнаружения событий ИБ по значениям контролируемых параметров, выделении комбинаций, обеспечивающих допустимые вероятностные характеристики обнаружения. Разработана процедура расстановки параметров оптимального пакета контроля по узлам КТС, что позволяет повысить производительность системы контроля.

6. Предложен алгоритм обнаружения инцидента, основанный на переборе всех возможных комбинаций событий ИБ, имеющих вид бинарных сигналов. Преимуществом предлагаемого подхода является использование минимального количества анализируемых комбинаций событий, обеспечивающих обнаружение инцидента с вероятностью не хуже заданной.

7. Предложена структурная схема системы контроля инцидентов ИБ. Разработан алгоритм ее функционирования, что позволяет сформировать требования к практической реализации систем данного вида.

8. Разработано информационное и программное обеспечение системы контроля инцидентов ИБ, включающее программные комплексы для расчета значимости элементов КТС, документированного обеспечения, администрирования корпоративной сети, регистрации инцидентов ИБ, мониторинга состояния элементов КТС, АРМ диспетчера. Результаты опытной эксплуатации на ряде предприятий модулей системы контроля инцидентов показали: среднее время ожидания заявки пользователей, обнаруживших проявление инцидента ИБ, на обработку снижается на 33%, среднее время выполнения функции устранения инцидента снижается до 25%, снизилось время назначения исполнителя на решения инцидента. Кроме того, уменьшается общее количество инцидентов.

ОСНОВНЫЕ ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

Статьи в изданиях рекомендованных ВАК РФ

1. Монахова, М.М. О применении алгоритма Куна-Манкреса и модели администратора в задачах восстановления производительности телекоммуникационных сетей / Д.В. Мишин, М.М. Монахова, М.Ю. Монахов // Радиотехнические и телекоммуникационные системы. - 2016. - №1. - С. 44-50.

2. Монахова, М.М. Автоматизированная система контроля целостности политики информационной безопасности сетевого оборудования // М.М. Монахова, С.Д. Лучинкин, Г.В. Путинцев, Д.В. Мазурок / Перспективы науки.- 2015. - № 8 (71). - С.76 - 80.

3. Монахова, М.М. Особенности контроля инцидентов информационной безопасности в корпоративной информационно-телекоммуникационной сети // М.М. Монахова / Известия высших учебных заведений. Технология текстильной промышленности. 2015, № 4 (358). - С.153 – 157 (*проиндексирована*

в международной базе Scopus).

4. Монахова М.М. Система администрирования корпоративной сети передачи данных АСУП / Д.В. Мишин, М.М. Монахова, А.А. Петров // Известия высших учебных заведений. Приборостроение. - 2012. - №8. - С.50-52.

5. Монахова, М.М. Система документированного обеспечения администрирования корпоративной сети передачи данных / Д.В. Мишин, М.М. Монахова // Вестник Костромского государственного университета им. Н.А. Некрасова. - 2010. - №1. - С. 70 - 72.

Публикации в других научных изданиях

6. Монахова, М.М. Автоматизированная система обнаружения инцидентов информационной безопасности корпоративных сетей передачи данных / М.М. Монахова, Г.В. Путинцев // Сборник трудов VII Всероссийской НТК «Имитационное моделирование. Теория и практика» ИММОД-2015. – Т.2. - М: ИПУ РАН, 2015. – С. 297 – 301.

7. Монахова, М.М. О формировании профиля телекоммуникационной сети / М.М. Монахова, О.Р. Никитин // Сборник трудов XXXIII Всероссийской НТК «Проблемы эффективности и безопасности функционирования сложных технических и информационных систем». – Серпухов: Филиал ВА РВСН, 2014. - С. 190-193.

8. Монахова, М.М. К вопросу о создании автоматизированной системы администрирования инцидентами безопасности телекоммуникационных сетей / Д.В. Мишин, М.М. Монахова, А.П. Кузнецова, С.Д. Лучинкин / Сборник трудов XXXIII Всероссийской НТК «Проблемы эффективности и безопасности функционирования сложных технических и информационных систем». – Серпухов: Филиал ВА РВСН, 2014. - С. 186-189.

9. Monakhova, M.M. The use of the priority model in optimization of corporate data network administrating / M. M. Monakhova, D. V. Mishin, A.V. Andreev // The Strategies of Modern Science Development: Proceedings of the International scientific–practical conference (Yelm, WA, USA, 29-30 March 2013). - Yelm, WA, USA: Science Book Publishing House, 2013. - P. 3-11.

10. Monakhova, M.M. Decision support system of dispatching the task to administrators of corporate area network / D. Mishin, M. Monakhova // Сборник материалов Всероссийской с международным участием молодежной НТК

«Молодежная математическая наука-2012». - Саранск, 2012. - С. 8-14.

11. Монахова, М.М. О модели администратора автоматизированной системы администрирования корпоративной сети передачи данных / Д.В. Мишин, М.М. Монахова // Материалы IX Международной НТК «Перспективные технологии в средствах передачи информации». - Владимир: ВлГУ, - 2011. - С. 76-79.

12. Monakhova, M.M. About the optimization of the administration corporate area networks of the data transmission under scarce administrative resources / D.V. Mishin, M.M. Monakhova // Information Science and Modelling. - Kharkov. - 2011. - №17. - P. 101-108.

13. Монахова, М.М. Модель автоматизированной системы администрирования корпоративной сети передачи данных / Д.В. Мишин, М.М. Монахова //Труды IX Международного симпозиума «Интеллектуальные системы». - М.: РУСАКИ. - 2010. - С. 268-271.

14. Монахова, М.М.. Алгоритмы распределенного администрирования корпоративных сетей передачи данных / Д.В. Мишин, М.М. Монахова // Материалы XIV Международной НТК «Проблемы передачи и обработки информации в сетях и системах телекоммуникаций». - Рязанский государственный радиотехнический университет. - 2010. - С. 131-134.

Подписано в печать
Формат 60×84/16. Усл. печ. л. . Тираж 100. Заказ
Издательство Владимирского государственного университета
600000, Владимир, ул. Горького, 87