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

Диссертация на соискание ученой степени
кандидата технических наук

Научный руководитель:
Никитин Олег Рафаилович
д.т.н., профессор

Владимир 2016

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

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 соответ-

ствии 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 технической политики ИБ.

2. Разработка методики формирования множества существенных факторов возникновения инцидентов ИБ, определяющих параметры контроля.

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 их группового ранжирования 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 показателей 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 «Завод «Электроприбор»» г. Владимир, Администрации Владимирской области, а также были использованы при разработке учебных курсов 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.

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» (Украина, 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.

1 ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОРПОРАТИВНЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ. АНАЛИЗ ОБЪЕКТА ИССЛЕДОВАНИЯ

В главе описываются объект и предмет исследования. Анализируются стандарты и руководящие документы, средства автоматизации, связанные с вопросами управления инцидентами информационной безопасности. Предложена формальная модель инцидента ИБ в корпоративной телекоммуникационной сети, как специфичного ее состояния идентифицируемого по отклонениям параметров ее функционирования от их эталонных значений, задаваемых технической политикой ИБ сети. Уточняется задача исследования.

1.1 Объект и предмет исследования

Объектом исследования настоящей диссертации является подкласс телекоммуникационных сетей – корпоративные телекоммуникационные сети (КТС) [13, 35]. КТС – сети масштаба предприятия, особенности которых, принципиальные в данной работе, следующие [3, 6, 11, 13, 19, 28, 39, 50, 102]:

1. КТС является вычислительной сетью, используемой для соединения имеющихся на предприятии информационных систем (ИС).

2. КТС является сетью передачи данных. Режим работы сети, как правило, круглосуточный. Основным транспортным протоколом для передачи данных является протокол TCP/IP.

3. В КТС используются разные типы приложений: клиент-серверные, на основе эмуляции терминала, WEB приложения и др.

4. Для адресации КТС используется адресное пространство разрешенного частного адресного пространства Интернет.

5. В пределах КТС имеются каналы связи (КС) с другими сетями для получения доступа к информационным ресурсам (ИР) и сервисам сторонних организаций.

6. В целях обеспечения удаленного доступа пользователей к информационно-техническим сервисам КТС допускается наличие КС удаленного доступа.

7. Все сетевые компоненты КТС идентифицированы и учтены в базе данных сетевого администрирования.

8. Все активное сетевое оборудование (АСО) КТС синхронизировано с сервером синхронизации времени.

9. Доступ и удаленное управление АСО разрешено только системному администратору после прохождения аутентификации и авторизации. Параметры аутентификации и авторизации АСО отконфигурированы.

10. На всех портах АСО установлен режим управления доступом к среде, должен быть режим STP (Spanning Tree Protocol). Все неиспользуемые порты АСО отключены.

11. Трафик, генерируемый системами управления сетью, не создает препятствия для передачи данных в КТС.

12. В системе в качестве структурных элементов присутствуют ярко выраженные система защиты информации (СЗИ) и система административного управления (САдУ). Их функции разграничены и обеспечиваются различными структурными подразделениями. СЗИ включает технические (аппаратные), программные и другие средства защиты, а также организационные мероприятия, исключающие или существенно затрудняющие разрушение, уничтожение, искажение и/или противоправный, несанкционированный доступ к конфиденциальной информации. Основной целью САдУ является приведение сети в соответствие с целями и задачами, для которых она предназначена. Достигается эта цель путём управления сетью, позволяющего минимизировать затраты времени и ресурсов, направляемых на управление системой, и в тоже время максимизировать доступность, производительность и продуктивность системы.

13. СЗИ построена и функционирует в соответствии со стратегией и тактикой защиты, определяемой Политикой обеспечения информационной безопасности (ПИБ). ПИБ является основным документом, регламентирующим процессы обеспечения ИБ на предприятии, утверждена руководством и является докумен-

том обязательного исполнения.

Данный набор особенностей характерен для крупных организаций, в которых обеспечением ИБ занимается специализированный отдел. Для полноценного функционирования, подобным организациям необходимо иметь в структуре КТС серверное оборудование, системы защиты, виртуальные приватные сети. На основе анализа подходов ведущих фирм (Cisco, Dlink) к построению КТС, сформирована типовая схема КТС, которая представлена на рисунке 1.1.

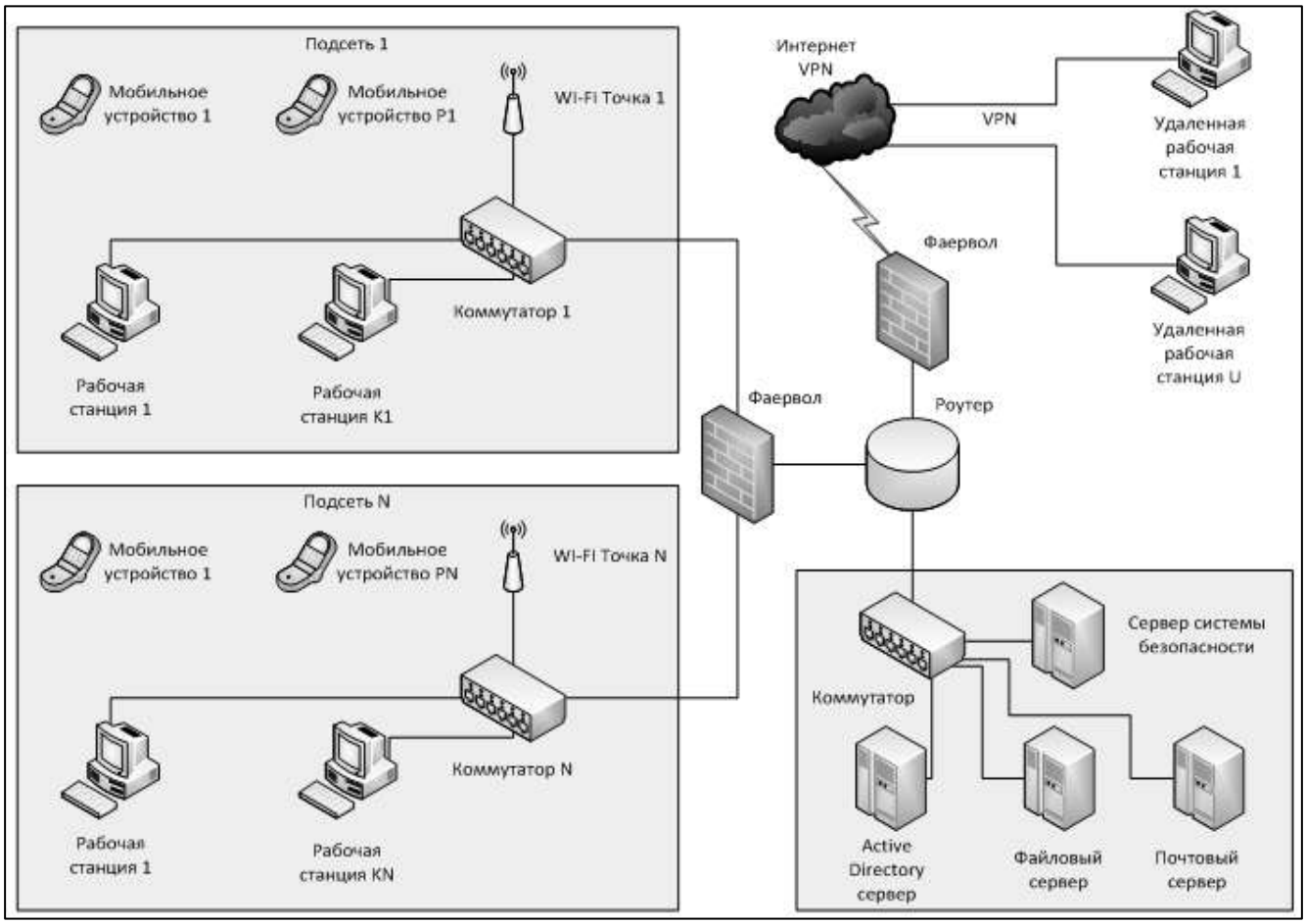


Рисунок 1.1- Типовая схема КТС

Типовая КТС [26, 30, 32] включает несколько подсетей, выделяемых для изоляции трафика, точки беспроводного доступа, защитные межсетевые экраны (МСЭ), оборудование маршрутизации и коммутации, VPN каналы, мобильные устройства, канал доступа в Интернет и сервера.

Технические средства обеспечения ИБ, составляющих типовую СЗИ,

сведены в таблицу 1.1.

Таблица 1.1 - Средства защиты, используемые в КТС

Общее название совокупности средств защиты	**Типовые средств защиты**
Штатные средства ОС	Авторизация в ОС Windows на основе доменных записей [23, 80], система разграничения доступа к файлам и каталогам в Linux [75].
Средства антивирусной защиты	Антивирус Касперского [124], ESETNOD32 [78], AvastPro [77].
Средства защиты от НСД	Dallas Lock[76], Secret Net[134], смарт-карты[17] и USB-ключи eToken [137].
Средства шифрования	КриптоПРО [31], CyberSafe Enterprise [114], Symantec (PGP) [100].
Средства аутентификации пользователей	Сервер аутентификации Kerberos[104], RSA SecurID [105].
VLAN	Cisco Catalyst 4500E Series Switches, Cisco Catalyst 3850 Series Switches [111, 112].
МСЭ экран	Межсетевой экран Cisco ASA5505 [109], Межсетевой экран Cisco ASA5510 [110].
Системы обнаружения вторжений	Security Studio Endpoint Protection [37], IDS Snort [24].
VPN	OpenVPN [132], ShadeYou VPN [135].

Анализ типовых решений КТС [3-6, 8-10, 13, 22, 27, 28, 30, 35, 36, 58, 68, 69, 72, 79] позволяет выделить принципиальные для настоящего исследования особенности:

1. Распределенная структура. КТС включает множество сегментов сети передачи данных, расположенных на обширной территории, наличие большого числа информационных каналов взаимодействия с «внешним миром» (источниками и потребителями информации), необходимость обеспечения непрерывности функционирования, что затрудняет оперативное решение задач сетевого управления, требует участия высококвалифицированных специалистов и/или специального инструментария автоматизации процессов управления.

2. Большое разнообразие решаемых задач и типов обрабатываемых данных, сложные режимы автоматизированной обработки информации с широким совмещением выполнения информационных запросов различных пользователей, обеспечение автоматизации целых направлений деятельности предприятия (бухгалтер-

ский учет, управление финансами, капитальное строительство и управление проектами, материально-техническое снабжение, управление производством и персоналом, внешнеэкономические связи и ряд других направлений), представленных множеством взаимосвязанных процессов. Заметим, что данные процессы, как правило, детерминированы (как минимум, в течение цикла управления сетью).

3. Гетерогенность. Разнообразие парка СВТ, сетевого оборудования и, в особенности, базового ПО на предприятии, что определяет требования к наличию в штате обслуживающего персонала различной специализации и профессиональной квалификации.

4. Участие в процессе автоматизированной обработки информации большого количества пользователей, большинство из которых имеют низкую квалификацию, что приводит к большому количеству инцидентов ИБ, связанных с человеческим фактором.

5. Объединение в единых базах данных информации различного назначения, принадлежности и уровней конфиденциальности делает ИР уязвимыми ко многим типам атак.

6. Большое количество сбоев в работе КТС связано с:

- широким использованием ОС Microsoft Windows с базовыми настройками безопасности как на РС пользователей, так и на корпоративных серверах;

- использованием слабо защищенных протоколов Ethernet и протоколов стека TCP/IP в качестве основы взаимодействия информационных процессов КИТС;

- использованием в прикладных задачах уязвимых протоколов HTTP, SNMP, FTP, DHCP, OPC, DCOM, ActiveX.

Политики ИБ, и создаваемые на их основе СЗИ, не могут полностью гарантировать защиту КТС. После внедрения защитных мери средств всегда остаются уязвимые места в КТС, 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 в КТС являются архитектурные просчеты, ошибки реализации программных и аппаратных компонентов, преднамеренные информационных воздействия, ошибки пользователей (операторов), старение оборудования и т.д. Наиболее распространенные причины возникновения инцидентов:

- сетевые атаки злоумышленников [68, 70, 102, 103, 107, 108, 119, 125]. Сетевым атакам подвержены такие элементы КТС, как корпоративные сервера, РС пользователей, среда передачи данных;

- вредоносные программы [2, 5, 12, 20, 29, 106] - компьютерные вирусы, черви, троянские программы. Таким видам угроз подвержены преимущественно РС пользователей. Заражение элементов КТС может сопровождаться нарушением СЗИ, ошибками или отказами элементов КТС, и, в результате, снижением системной производительности [22, 26];

- выход из строя аппаратных компонентов КТС, связанный с нарушением правил их эксплуатации (ошибки подключения, перегрев оборудования, деструктивные механические воздействия), а также связанный с их старением (эксплуатация аппаратных компонентов с превышением допустимых/гарантийных сроков);

- выход из строя компонентов КТС вследствие ошибок пользователей (человеческий фактор);

- архитектурные просчеты и ошибки реализации программных компонентов КТС.

По результатам исследований European Network and Information Security Agency за 2013 год [116], наиболее частыми причинами возникновения инцидентов ИБ в КТС являются естественные (природные) причины - 12%, ошибки пользователей - 12%, вредоносные атаки - 6%, ошибки ПО- 47%, другие причины – 33%. Процент от общего времени, затраченный на устранение каждого из типов инцидентов: естественные (природные) причины - 25%, ошибки пользователей - 20%, вредоносные атаки - 20%, ошибки ПО- 25%, другие причины - 10%. Здесь же приводятся данные о том, что в среднем 45% инцидентов происходит из-за проблем с ПО, 25% - связаны с человеческими ошибками и 30% - с аппаратными

отказами.

Методы и средства, позволяющие обеспечить контроль инцидентов ИБ в КТС, обусловленных нарушением политики ИБ, составляет предмет исследования диссертационной работы.

1.2 Контроль инцидентов информационной безопасности

ГОСТ Р ИСО/МЭК ТО 18044-2007 [18] дает следующие определения: «Инцидент ИБ – появление одного или нескольких нежелательных, или неожиданных событий КТС, с которыми связана значительная вероятность … угрозы КТС». «Событие КТС – идентифицированное появление определённого состояния системы, сервиса или сети, указывающего на возможное нарушение политики безопасности или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности». В международной практике разработано большое количество нормативных документов, регламентирующих вопросы управления инцидентами ИБ [18, 113, 120-122].

В [18] выдвигаются общие требования к построению системы управления ИБ, в частности, относящиеся и к процессам управления инцидентами. Документ [120] описывает инфраструктуру управления инцидентами в рамках циклической модели процессов Шухарта - Деминга [38] - модель PDCA. Стандарт [120] описывает модель PDCA как основу функционирования всех процессов системы управления ИБ. Даются подробные спецификации для стадий планирования, эксплуатации, анализа и улучшения процесса. Стандарт [121] основной упор делает на организацию работы CISRT (Critical Incident Stress Response Team) - подразделения, обеспечивающего поддержку предотвращения, обработки и реагирования на инциденты. Вводится ряд критериев, на основании которых можно оценивать эффективность данных сервисов, приводятся процессные карты. Сборник «лучших практик» по построению процессов управления инцидентами приведен в [113]. Подробно разбираются вопросы реагирования на разные типы угроз, такие как распространение вредоносного ПО, НСД и другие. Документ [122] определяет

формальную модель процесса реагирования на инциденты ИБ.

Особенностью походов, принципиальной для настоящего исследования, является следующее: стандарты [18, 113, 120, 122] описывают процедуры управления – менеджмента инцидентов, практически не затрагивая технических вопросов. Из данных публикаций не понятно, каким образом обнаружить инцидент ИБ, какие события могут быть причинами инцидента. Не конкретизированы понятия «нарушение политики безопасности» и «неизвестная ситуация». В дальнейшем будем рассматривать ряд функций менеджмента инцидентов, связанный только с техническими вопросами контроля инцидентов и не в ИС предприятия в целом, а только в ее технологической основе – КТС. Соответствующую политику ИБ будем называть технической политикой ИБ.

Цикл контроля инцидентов ИБ в КТС включает шесть этапов.

Этап 1. Измерение параметров инцидентов. КТС функционирует в штатном режиме с требуемой (например, номинальной) производительностью $E_{ном}$, оцениваемой средними задержками передачи информационных пакетов или числом информационных пакетов (байтов) по всем маршрутам [59 - 60]. Данный этап сопровождается контролем значений параметров инцидентов всех элементов КТС. Данный процесс должен быть организован таким образом, чтобы не приводить к существенному повышению средних задержек. Процесс контроля может осуществляться по наперед составленному расписанию, циклически или разово. Этап заканчивается при возникновении инцидента ИБ. Возникновение инцидента обнаруживается, например, по выходу средних задержек за пределы допустимых значений. Предпосылки этому резкое повышение сетевого трафика, что может быть связано с DOS-атакой, или снижение трафика, что связано, например, с выходом из строя линии связи, сервера или ряда рабочих станций.

Этап 2. Обнаружение инцидента. На данном этапе происходит обнаружение инцидента, поиск элементов КТС с нарушениями требований политики, сбор информации об инциденте и его последствиях. В течение данного этапа производительность КИТС может продолжать уменьшаться.

Этап 3. Идентификация инцидента. Производится анализ собранной инфор-

мации об инциденте (идентификация инцидента и его классификация), анализ возможных решений инцидента. Выбирается подходящее решение инцидента - возможно оперативное (временное), обеспечивающее частичное восстановление производительности.

Этап 4. Формирование программы «решения» инцидента. Происходит формирование объема и последовательности необходимых работ по восстановлению требований технической политики на «инцидентных» элементах. Кроме того, под конкретные работы подбираются исполнители.

Этап 5. Исполнение программы «решения» инцидента. Происходит выполнение конкретных работ по восстановлению требований действующей политики безопасности. Если восстановить работоспособность КТС не удается (по девствующей политике), то необходимо политику пересмотреть. На данном этапе эффективность КТС должна достигнуть $E_{ном}$.

Этап 6. Завершение инцидента. Формируется отчет по результатам контроля.

Составляющие времени цикла контроля:

T_1 – время измерения параметров инцидентов;

T_2 -время обнаружения инцидента;

T_3 - время идентификации инцидента;

T_4 - время формирования программы «решения» инцидента;

T_5 - время выполнения программы «решения» инцидента;

T_6 - время завершения инцидента.

Далее время цикла будет рассматриваться как основной показатель эффективности процессов контроля инцидентов в КТС.

Для эффективного контроля инцидентов ИБ необходимо:

1. Выполнить классификацию инцидентов ИБ. Состояния КТС, которые не войдут в указанный перечень, будут рассматриваться как штатные.

2. Разработать методику обнаружения типа и места инцидента. Нарушение

ТПИБ может заметить пользователь, системный администратор КТС, администратор безопасности или автоматизированная система сетевого мониторинга. Администратор по «рекомендации» автоматизированной системы контроля, анализирующей совокупность событий ИБ, должен принять окончательное решение об обнаружении конкретного типа инцидента ИБ.

3. Разработать процедуры устранения последствий и причин инцидента ИБ, выполнить действия, предупреждающие (или, по крайней мере, ослабляющие) повторное возникновение инцидента ИБ.

В настоящее время существует ряд коммерческих продуктов, потенциально способных автоматизировать ряд системных процессов контроля инцидентов ИБ. Выделим системы управления элементами сети (Cisco View, Optivity, RAD View), сканеров сети (AdRem Net Crunch, Manage Engine Op Manager, Service Keeper, nmap, xspider, maxpatrol, LanScope) [97, 98], программы инвентаризации аппаратных компонентов и ПО (EVEREST Ultimate Edition, WinAudit, ASTRA32 – Advanced System Information Tool, Network Asset Tracker, Network Inventory Monitor, Network Inventory Navigator) [117, 118]. Применение данных средств позволяет автоматизировать процессы:

- создания и поддержки шаблона безопасности - специальной базы профилей, содержащих значения параметров эталонных состояний КТС. Типичными примерами систем такого класса являются CA Unicenter TNG, Sun Net Manager, HP OpenView, IBM/Tivoli [99];

- поддержки пользователей (Technical support, Helpdesk, Service Desk), позволяющей пользователям оперативно информировать о возникающих проблемах [133];

- анализа журналов событий средств защиты информации КТС - систем обнаружения вторжений, систем межсетевого экранирования, антивирусных комплексов и т.д.;

- создание автоматизированных средств административного управления восстановления работоспособности КТС в случае обнаружения инцидентов ИБ, связанных со сбоями и отказами в функционировании элементов сети [41 - 47, 52 -

56].

Анализ возможных средств автоматизации контроля инцидентов позволяет сделать следующие выводы:

- инциденты, связанные с нарушением технической политики ИБ не систематизированы, так инциденты, обусловленные отказами и сбоями в функционировании элементов сети, а также авариями, как множественными отказами [58], не могут составлять полное множество нарушений технической политики ИБ;

- средства сетевого управления, как правило, имеют в своем составе возможности по обнаружению событий ИБ, но алгоритмы их работы «закрыты» - составляют коммерческую тайну, ими практически невозможно управлять программно. Часто декларируемые характеристики и функциональные особенности коммерческих средств отличаются от их реальных характеристик;

- мощные системы управления событиями, которые объявляют об анализе «всех» событий в ИС (более нескольких миллионов одновременно), требуют для их обработки супер-ЭВМ. Такие системы сильно «подсаживают» сеть и весьма дороги для большинства отечественных предприятий. Заметим, что эти системы анализируют события, связанные с информационным взаимодействием пользователей и системы, анализа событий, связанных мониторингом технической политики, не декларируется;

- ряд разработок в направлении автоматизации контроля инцидентов ИБ не выходят за рамки лабораторных исследований и далеки от практического применения.

1.3 Формальная модель инцидента ИБ в КТС

Пусть в процессе функционирования наблюдаемая КТС может находиться в одном из N состояний множества $S = (S_1, S_2, \dots, S_N)$. Согласно предлагаемой модели, каждое состояние (полностью) описывается вектором параметров. Мощность множества таких векторов совпадает с мощностью S. Запись $\overrightarrow{PAR} = (\overrightarrow{PAR}_1, \overrightarrow{PAR}_2, \dots, \overrightarrow{PAR}_N)$ означает, что в каждый момент времени существуют

вектора $(\overrightarrow{PAR_1},\overrightarrow{PAR_2},...,\overrightarrow{PAR_N})$ из одних и тех же параметров. Такими параметрами могут быть как количественные - изменяемые в процессе функционирования значения статических и динамических характеристик элементов КТС, так и качественные, отражающие экспертные оценки поведения элементов анализируемой системы.

Конкретные значения параметров текущего состояния S_N - вектора $\overrightarrow{PAR_n},(n=\overline{1,N})$ - будем обозначать $p_1,p_2,\ldots$. Пусть всего таких значений M. Таким образом, $\overrightarrow{PAR_n}=(p_1,p_2,...,p_M)_n,(n=1,...,N)$, и

$$S=(\overrightarrow{PAR_1},\overrightarrow{PAR_2},...,\overrightarrow{PAR_N})=\{(p_1,p_2,...,p_M)_1,...,(p_1,p_2,...,p_M)_N\} \qquad (1.1)$$

Параметры инцидентов ИБ. Принципиальной задачей контроля инцидентов ИБ является идентификация (обнаружение) (по значениям измеренных текущих значений параметров) некоторых состояний КТС - S^*, которые мы сопоставляем с наличием инцидента.

Пусть выявлено некоторое подмножество параметров, по которым возможно идентифицировать состояния из подмножества $S^*=(S_1,S_2,...,S_{N^*})\in S$, $N^*=|S^*|\le N$. Параметры объекта, позволяющие обнаруживать и распознавать состояния S^*, назовем параметрами инцидентов (ПИн) ИБ. Очевидно, что таких параметров меньше, чем M, описывающих все состояния КТС. Обозначим вектор ПИн как $\overrightarrow{PAR_{ПИн}}$, его длина $M_{ПИн}\le M$.

Параметры инцидентов разделим на опознавательные ПИн и ПИн, контролирующие деятельность. Опознавательные параметры описывают поведение элементов КТС в статическом состоянии (параметры принятой настройки). Параметры, контролирующие деятельность, характеризуют этапы и режимы функционирования КТС и представляют собой последовательность во времени событий или действий составных элементов КТС, а также значения их статистических характеристик.

Рассмотрим множества возможных (дискретных) значений измеряемых параметров инцидентов:

$$\begin{cases} p_1 = (p_{11}, p_{12}, \ldots, p_{1N^*}), \\ p_2 = (p_{21}, p_{22}, \ldots, p_{2N^*}), \\ \ldots\ldots \\ p_{M_{ПИн}} = (p_{M_{ПИн}1}, p_{M_{ПИн}2}, \ldots, p_{M_{ПИн}N^*}). \end{cases} \quad (1.2)$$

В каждом таком множестве выделим подмножества значений, «разрешенных» с точки зрения действующей политики ИБ:

$$\overrightarrow{PAR}^*_{ПИн} = (p^*_1, p^*_2, \ldots, p^*_m, \ldots, p^*_{M_{ПИн}}) \quad (1.3)$$

Такое подмножество (эталонных) значений параметров назовем *шаблоном безопасности* КТС по принятой (действующей) технической политике ИБ. Подмножества значений параметров, не разрешенных по технической политике ИБ, определяют состояние КТС, связываемое с инцидентом ИБ. Очевидно, для того, чтобы «обнаружить» инциденты ИБ по текущим значениям параметров инцидентов ИБ, необходимо их (значения параметров) сопоставить с шаблоном.

На всех множествах параметров инцидентов ИБ (1.2) введем функцию расстояния между двумя значениями (измеренным и шаблонным (разрешенным)). Пусть это будет вещественная неотрицательная симметричная функция, равная нулю исключительно в случае совпадения значений. Практически такую функцию ввести нетрудно, поскольку множества значений параметров инцидентов ИБ являются либо подмножествами множеств целых или вещественных чисел (числовые параметры элементов КТС, например, минимальная длина пароля), либо множествами строк определённой длины (строковые параметры элементов системы), либо массивами опять же чисел или строк (например, списки контроля доступа). Таким образом, мы имеем возможность определить, является ли текущее значение параметра разрешенным.

Замечание. На практике для некоторых параметров инцидентов невозможно «перечислить» все значения, соответствующие шаблону безопасности. Приходится вводить понятие «допустимого диапазона». Таким параметром может быть средняя загрузка процессора какого-либо сервера или рабочей станции в течение дня. Тогда значение функции приравнивается нулю при попадании значения пара-

метра в допустимый диапазон.

Событие информационной безопасности. Введем в рассмотрение простое логическое высказывание «Значение параметра инцидента отличается от значений, задаваемых шаблоном безопасности». Оно истинно при неравенстве нулю выше введённой функции расстояния, и ложно при равенстве. Поставим в соответствие высказыванию соответствующую логическую переменную, обозначим ее как X_m, и назовем в дальнейшем событием информационной безопасности (СоИБ).

Замечание. Такой поход включает идентифицированное появление определенного состояния КТС, которое свидетельствует либо о возможном нарушении политики ИБ, либо об отказе СЗИ, либо о возникновения ранее неизвестной ситуации, которая может быть связана с ИБ, что полностью соответствует принятому определению события, введенному в стандарте [18].

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.

1.4 Модель функционирования системы контроля инцидентов. Уточнение задачи исследования

Для обнаружения инцидентов необходимо анализировать значения многих параметров КТС (включая параметры СЗИ, как подсистемы КТС): например, параметров парольной защиты (минимальная длина пароля пользователя, период действия пароля и т.д.), параметров (настройки) системы управления доступом, специфические настройки, имеющие отношение к «профильному» функционированию КТС (характеристики производительности) и т.д. Эти и другие параметры, критичные с точки зрения возникновения инцидентов ИБ, были названы параметрами инцидентов ИБ (ПИн).

Система контроля инцидентов (СКИн) ИБ «запоминает» эталонные значения (настройки) ПИн (соответствующие действующему «профилю») в своей базе данных. Значения эталонных настроек определяются требованиями технической политики ИБ.

При осуществлении контроля инцидентов ИБ (ИнИБ) производится сравнение текущих значений ПИн с эталонными, и в случае выявления несоответствия принимается решение о возникновении ИнИБ.

Каждый раз при осуществлении проверки «на инцидент» производить сравнение эталонных настроек, сохранённых в базе данных, и «измеренных» значений абсолютно всех параметров во всех узлах КТС не рационально: на проведение такого мониторинга требуются существенные вычислительные и временные ресурсы, которые в процессе проведения проверки (мониторинга) отнимаются у КТС. Если число проверяемых параметров велико, то это может приводить к существенному снижению производительности КТС, и она не сможет обеспечить свою главную функцию - поддержку информационных процессов предприятия. Поэтому в процедурах контроля, оптимизируемых по временным критериям, среди всех параметров проверки выделяется некоторое подмножество наиболее критичных, они подлежат сравнению, остальные параметры остаются неконтролируемыми.

Одной из задач данного диссертационного исследования и является выявление наиболее критичных параметров КТС. «Сужение» множества параметров контроля, кроме выше названного, может достигаться, например, выявлением «инцидентной» подсети, тогда контролируемых параметров уже снизится во столько раз, сколько подсетей в КТС.

При отклонении параметра от «эталонного» значения имеет место потенциальный ущерб, связанный с возможностью реализации той или иной угрозы ИБ. Этот ущерб имеет место как для случая контролируемых параметров, так и для неконтролируемых. Разница лишь в том, что с отклонениями неконтролируемых параметров приходится «мириться», значения же отклонений контролируемых параметров могут быть востребованы для соответствующих корректировок и настроек средств и механизмов защиты в СЗИ (приведение к профилю техниче-

ской политики).

Приведённое описание логики работы СКИн является основой для создания формальной математической модели функционирования данной системы.

Пусть в анализируемой КТС определено $M_{ПИн} \leq M$ параметров, контролируемых СКИн, а также заданы функции определения расстояния между двумя значениями для каждого параметра.

В связи с тем, что контролируются не все параметры КТС, а лишь их часть, вводится понятие пакета контроля.

Определение. Подмножество ПИн с номерами $\{m_1\} \in \{1, \ldots, M_{ПИн}\}$ назовём пакетом контроля, обозначив его ПК(m_1).

Теоретически может быть $(2^{M_{ПИн}} - 1)$ пакетов. Каждому пакету контроля соответствует множество контролируемых параметров с номерами из множества m_1. Для ПК(m_1) параметры $par_i, i \in m_1$ (параметры перенумерованы) будем называть контролируемыми параметрами.

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 $p_m(t \leq t_j)$, $q_m(t \leq t_j), t_j = \overline{1,T}$ вероятностей корректного и «ложного» обнаружения. Вследствие этого качество обнаружения инцидента связывается с граничными вероятностями корректного и «ложного» обнаружения инцидента.

Исходя из вышеуказанных положений, цель исследования заключается в синтезе алгоритмов формирования оптимального контроля инцидентов ИБ в КТС. Для достижения этой цели необходимо решить следующие частные задачи:

- разработать методику зависимости возникновения инцидентов от факторов

нарушения технической политики ИБ;

- выявить контролируемые параметры КТС, по которым возможно оценить нарушение технической политики;

- разработать алгоритм формирования пакета контроля;

- разработать алгоритмы и экспериментальное программное обеспечение для практического определения ПИн КТС.

Выводы к главе 1

Стандарты и руководящие документы, связанные с вопросами управления инцидентами информационной безопасности, не затрагивают технических вопросов построения систем контроля, не конкретизируют технических особенностей нарушений политики безопасности, как основной причины инцидента.

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

Анализ известных средств автоматизации контроля инцидентов показал: инциденты, связанные с нарушением ТПИБ не систематизированы; средства сетевого управления, как правило, имеют в своем составе возможности по обнаружению событий ИБ, но алгоритмы их работы «закрыты», ими невозможно управлять программно.

Задача эффективного контроля инцидентов ИБ в КТС заключается в том, чтобы определить минимальный по количеству контролируемых параметров пакет, найти значения минимального времени на контроль каждого из составляющих пакет параметров.

2 РАЗРАБОТКА МЕТОДИКИ ОПРЕДЕЛЕНИЯ МНОЖЕСТВА СУЩЕСТВЕННЫХ ФАКТОРОВ ВОЗНИКНОВЕНИЯ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Основная проблема в синтезе математических моделей контроля инцидентов ИБ по параметрам КТС заключается в том, что появлению инцидента сопутствует множество различных причин - факторов и обнаружить их проявление можно в самых разнообразных компонентах КТС. В результате анализа типовой ТПИБ КТС было выявлено 30 таких факторов. Если связать факторы с параметрами функционирования элементов сети, то в реальной КТС (например, состоящей из 1000 узлов) для анализа нарушения должно анализироваться нескольких тысяч параметров. Такой анализ за приемлемое время и без снижения общей производительности КТС бесперспективен. Следовательно, процедура обнаружения инцидентов по параметрам функционирования КТС должна сопровождаться снижением множества факторов – выявлением существенных факторов, влияющих на возникновение инцидента.

В главе предлагается методика «усечения» полного множества факторов нарушения ТПИБ, основанная на систематизации инцидентов ИБ, выявлении взаимосвязи инцидентов с факторами нарушения технической политики КТС и групповом экспертном анализе. Приводятся практические примеры ее применения.

2.1 Выявление взаимосвязи инцидентов с факторами нарушения технической политики КТС

Политика ИБ [25, 87] определяет систему взглядов на проблему обеспечения ИБ и представляет собой систематизированное изложение целей и задач защиты, как набор правил, процедур и практических приемов в области обеспечения ИБ, которыми руководствуется организация. На основе политики ИБ строится управление, защита и распределение критичной информации в системе. Она (политика)

должна охватывать все особенности процесса обработки информации, определяя поведение КТС в различных ситуациях. Для конкретной КТС политика ИБ зависит от технологии обработки информации, используемых программных и технических средств, структуры организации и т.д. [25].

Анализ руководящих документов в области технической защиты информации, стандартов и «лучших» практик [1, 21, 81 - 85, 96] построения технической политики ИБ корпоративных сетей позволяет выделить ряд структурных и функциональных особенностей, принципиальных для настоящего исследования:

1. Стратегия и тактика построения СЗИ (политики ИБ) определяется через защитные функции (ЗФ): предотвращения причин возникновения угроз ($ЗФ_1$), их (угроз) сдерживания ($ЗФ_2$), обнаружения ($ЗФ_3$), предупреждения воздействия на элементы КТС проявившихся угроз ($ЗФ_4$), обнаружения воздействия необнаруженных угроз ($ЗФ_5$) и устранения обнаруженного воздействия угроз ($ЗФ_6$). В конкретных политиках могут присутствовать не все функции из перечисленных. Главное, чтобы в определенном сочетании они обеспечивали требуемый уровень ИБ (в пределах принимаемых рисков [38]). Предлагается нарушение ТПИБ, и соответственно *виды инцидентов* ИБ следует связать с невыполнением данных функций.

Выполним такую классификацию:

А). «Не устранённая уязвимость» ($Ин_1$) (конечно, при наличии источника угрозы, которая могла бы эксплуатировать данную уязвимость). Часть уязвимостей КТС может быть устранена при «хорошем» построении (конфигурировании) сети, другая часть, например, определяемая надежностью элементов, даже за счет резервирования, не устранится никогда. Сбой или отказ элементов – яркий представитель инцидента данного типа. Еще примеры – окончание лицензии на ПО и обнаружение несоответствия профилю.

Б). «Не обнаружена реализация угрозы» ($Ин_2$) (угрозы «известной», входящей в «Модель угроз» ТПИБ). Здесь рассматривается ситуация, при которой обнаружение не состоялось из-за либо некорректно настроенных средств обнаружения, либо длительность обнаружения угрозы выходит за рамки заданного времен-

ного промежутка.

В). «Нет защиты от реализованной угрозы» ($Ин_3$). Возможно, «силы» противодействия не хватило, чтобы полностью обеспечить защиту. Данная ситуация может возникнуть как при обнаружении известной угрозы, так и при ее не обнаружении. Типовая ситуация выглядит, примерно, следующим образом: мерами защиты от вредоносного ПО в КТС обнаружен «вирус» (т.е. известная угроза пропущена и реализована), поступило сообщение о «лечении» (удалении), а «вирус» все равно начал распространяться по всей системе – был обнаружен на других рабочих станциях. Защитных средств, устраняющих (или хотя бы ослабляющих) реализацию обнаруженной угрозы в системе явно недостаточно. Здесь налицо невыполнение соответствующей ЗФ, а, следовательно, ТПИБ. Заметим, что речь идет о невыполнении ЗФ за фиксированное время с требуемым качеством.

Г). «Реализация неизвестной угрозы» ($Ин_4$). Данная ситуация может быть обнаружена только косвенно, например, по аномальному функционированию элементов КТС. Например, подсистема обеспечения целостности может зафиксировать факт изменения содержимого конфиденциальных файлов в отсутствии «срабатывания» системы обнаружения вторжений. Заметим, что понятие «неизвестности» угрозы существует в рамках принятой политики ИБ (в разделе «Модель угроз»), «Модель угроз» (и политика ИБ) могут быть пересмотрены и «неизвестная» угроза станет «известной». Но это уже другой тип инцидента.

Д). «Не устраняется воздействие реализации угрозы» ($Ин_5$). Рассматривается ситуация, когда не удается локализовать и устранить реализацию угрозы во всех точках КТС ее проявления (в течение заданного времени с требуемой эффективностью). Данный инцидент может иметь место в случае обнаруженной угрозы и не срабатывания защиты.

Замечание. Защитная функция «Ликвидация последствий реализованной (пропущенной) угрозы» является обязательной функцией любой ТПИБ. Вряд ли следует связывать инцидент с тем, что не удается ликвидировать последствия пропущенной атаки. Здесь речь идет об аварии.

2. Политика ИБ в качестве обязательного структурного элемента содержит

«Модель угроз» - документ, в котором перечисляется полное множество угроз, противодействие которым реализовано в СЗИ, точки воздействия угроз в КТС, причины и источники их возникновения, а также механизмы (меры) защиты. Следовательно, нарушения ТПИБ (по ряду функций, обозначенных в п.1) следует искать в фактах недостаточной защиты конкретно против угроз, выделенных в Модели. В соответствии с [14 - 16], угроза – это обстоятельства или события, которые могут быть причиной нанесения ущерба. Ущерб может заключаться в нарушении свойств информации путем ее разрушения, искажения или несанкционированного ознакомления, либо в разрушении, искажении или несанкционированном использовании ресурсов системы. Источниками угроз могут быть различные объекты и явления, что затрудняет их учет при построении СЗИ. В связи с этим в мировой практике принято строить Модель угроз, в которой приводится классификация возможных угроз, их описание и средства возможной реализации.

Одним из лучших документов в этой области является IT-Baseline Protection Manual [123]. В этом стандарте угрозы разделены на группы, связанные: с форс-мажорными обстоятельствами, с недостатками организации и управления, с человеческим фактором, с техническими неисправностями, со спланированными действиями злоумышленников. Каждая из этих групп содержит большой перечень угроз, подробное рассмотрение которых выходит за пределы этой работы.

Замечание. Пропуск «необнаруженных» (неизвестных, или не вошедших в заявленное множество) угроз также является нарушением политики ИБ. Обнаружение и защита против них возможна только косвенно (по их проявлениям) дополнительными средствами системного администрирования.

3. В качестве защитных мер (ЗМ) реализации ЗФ, как правило, приводятся процедуры и механизмы: идентификации и аутентификации ($ЗМ_1$), контроля и разграничения доступа к локальным ($ЗМ_2$) и разделенным ($ЗМ_3$) ИР, защиты от вредоносных программ ($ЗМ_4$), защиты внутренних ($ЗМ_5$), и внешних ($ЗМ_6$) каналов связи, защиты от удаленных атак ($ЗМ_7$).

Связь ФЗ↔ЗМ представлена таблицей 2.1. Таблицей 2.2 задаются типовые средства реализации защитных мер в КТС.

Таблица 2.1 - Меры (подсистемы) ЗИ, обеспечивающие реализацию ФЗ

Меры (подсистемы) ЗИ	Предупреждение условий возникновения источников угроз	Сдерживание угроз	Обнаружение угроз	Предупреждение воздействия на элементы КТС проявившихся угроз	Обнаружение воздействия неизвестных угроз	Устранение обнаруженного воздействия угроз
	$ЗФ_1$	$ЗФ_2$	$ЗФ_3$	$ЗФ_4$	$ЗФ_5$	$ЗФ_6$
Идентификация и аутентификация $ЗМ_1$	+	+	-	+	-	-
Контроль и разграничение доступа к ИР $ЗМ_2$	+	+	+	+	-	+
Контроль и разграничение доступа к сетевым ресурсам $ЗМ_3$	+	-	-	+	-	+
Защита от ВП $ЗМ_4$	-	+	+	+	-	-
Защита внутренних КС $ЗМ_5$	-	+	+	-	+	+
Защита внешних КС $ЗМ_6$	+	+	+	-	+	+
Защита от удаленных атак $ЗМ_7$	-	+	+	-	+	+

Таблица 2.2 - Типовые средства реализации защитных мер технической политики ИБ в КТС

Меры (подсистемы) ЗИ / Средства защиты	Штатные средства ОС	Средства антивирусной защиты	Средства защиты от НСД	Средства шифрования	Средства аутентификации пользователей	МСЭ	СОВ (IDS / IPS)	VLAN	VPN
Идентификация и аутентификация	+	-	+	-	+	+	-	+	+
Контроль и разграничение доступа к ИР	+	-	+	-	+	-	+	-	-
Защита от ВП	-	+	-	-	-	-	+	-	-
Контроль и разграничение доступа к сетевым ресурсам	+	-	+	-	+	+	-	+	+
Защита внутренних КС	-	-	-	+	-	-	-	+	-
Защита от удалённых атак	-	+	+	-	-	+	+	-	+
Защита внешних КС	-	-	-	+	-	+	-	-	+

4. ТПИБ содержит требования к параметрам средств защиты. Например, в идентификации и аутентификации (мера) указано число неудачных попыток при входе в систему, количество и тип символов для пароля (параметры).

Конкретная реализация защитных мер в виде набора рекомендаций и правил, а также требований к параметрам, приведена в «Типовой (обобщенной) технической политике ИБ» (Приложение 1).

Взаимосвязь видов инцидентов с параметрами усложняется следующими обстоятельствами: одни и те же параметры могут быть показателями возникновения инцидентов разного типа; у однотипных параметров в сети могут быть различные источники.

Введем понятие *фактора (причины) нарушения* ТПИБ. Факторы представляют «отрицания» требований технической политики.

В таблице 2.3 приведен перечень таких факторов для типовой технической политики ИБ КТС.

Нетрудно видеть, что каждому фактору можно поставить в соответствие вполне конкретные параметры элементов КТС. Кроме того, подмножества факторов явно концентрируются вокруг мер защиты. В дальнейшее будем именовать параметр так же как фактор.

Таблица 2.3 - Перечень факторов нарушения технической политики ИБ

№	Наименование фактора
1	Антивирусная защита (АВЗ) не (установлена и активирована) на – шлюзе доступа (HTTP, FTP трафик)
2	АВЗ не (установлена и активирована) на почтовых системах (SMTP/POP3 трафик)
3	АВЗ не (установлена и активирована) на ФС
4	АВЗ не (установлена и активирована) на РС
5	АВЗ не обновляются централизованно и регулярно
6	Обнаружен неизвестный компонент КИТС
7	Имеется доступ к активному сетевому оборудованию (АСО) не только у СисАдм
8	Разрешен доступ к АСО по протоколу SNMP в режиме изменения
9	Не на всех используемых АСО установлен режим STP
10	Не все неиспользуемые порты АСО отключены
11	Не установлен контроль доступа на границе КИТС для входящих и исходящих данных на сетевом и транспортном уровне
12	Нет аудита контроля доступа по сетевому соединению
13	Имеется «множественный» доступ к журналам аудита
14	Разрешено использование VPN без шифрования данных
15	Не весь входящий и исходящий трафик анализируется на наличие ВП и сигнатур известных атак
16	На РС сетевые конфигурационные параметры не соответствуют шаблону
17	Учетные записи пользователей не актуальны
18	Учетная запись не соответствует роли ее владельца
19	Учетные записи уволенных сотрудников не блокируются и не удаляются
20	Использование некорректных паролей
21	Разрешена установка и/или изменение набора ПО на РС пользователям (не только системному администратору)
22	Не все используемое ПО идентифицировано в реестре разрешенного ПО
23	В РС и/или серверах имеется ПО, сведения о котором не внесены в реестр разрешенного ПО
24	Реестр ПО содержит сведения о ПО с «просроченной» лицензией
25	В папках пользователей присутствует информация «неслужебного» характера
26	Пользователям не запрещено самостоятельно организовывать файловые серверы
27	На РС пользователя открыт общий доступ к папкам
28	Обнаружено подключение портативных мобильных устройств, которые не учтены в реестре аппаратного обеспечения
29	Изменена аппаратная конфигурация РС
30	Изменена аппаратная конфигурация серверов

2.2 Разработка процедуры выявления существенных факторов нарушения технической политики информационной безопасности

Выявление существенных факторов нарушения ТПИБ основано на классификации, предложенной в п.2.1 и процедуре групповой экспертизы полного множества факторов способом ранжирования [7, 74] и удаления из данного множества «несущественных» факторов. Разработанную процедуру представим в виде алгоритма, поясняя формальные подходы соответствующими примерами. Заметим, что данный алгоритм описывает процедуру для любого вида инцидента.

Алгоритм выявления существенных факторов нарушения ТПИБ

Шаг 1. Задать множество факторов нарушения ТПИБ $\Phi=\{\Phi_k\}, k=1,\ldots,K$. Отобрать показатели (всего Ω), определяющие вид ИнИБ - нарушенные меры защиты (НМЗ), приводящие к возникновению инцидента. Соответствие «ИнИБ – НМЗ» показывает таблица 2.4. Знак «+» означает связность вида инцидента с соответствующим нарушением; знак «-» - отсутствие такой связи.

Анализ таблицы 2.4:

- для каждого из пяти выделенных видов инцидентов возможно определить «свои» множества показателей:

$\text{ИнИБ}_1 = \{\text{НМЗ}_1, \text{НМЗ}_2, \text{НМЗ}_3, \text{НМЗ}_6\}$,

$\text{ИнИБ}_2 = \{\text{НМЗ}_1, \text{НМЗ}_2, \text{НМЗ}_4, \text{НМЗ}_5, \text{НМЗ}_6, \text{НМЗ}_7\}$,

$\text{ИнИБ}_3 = \{\text{НМЗ}_2, \text{НМЗ}_4, \text{НМЗ}_5, \text{НМЗ}_6, \text{НМЗ}_7\}$,

$\text{ИнИБ}_4 = \{\text{НМЗ}_5, \text{НМЗ}_6, \text{НМЗ}_7\}$,

$\text{ИнИБ}_5 = \{\text{НМЗ}_2, \text{НМЗ}_3, \text{НМЗ}_5, \text{НМЗ}_6, \text{НМЗ}_7\}$;

- зная соответствие факторов нарушения ТПИБ мерам обеспечения ИБ возможно сопоставить определенные подмножества факторов «своему» виду инцидента.

Таблица 2.4 - НМЗ, приводящие к возникновению ИнИБ

Инцидент / Нарушенные меры (механизмы) ИБ	$ИнИБ_1$ («Не устранены условия возникновения угроз»)	$ИнИБ_2$ («Не обнаружена реализация угрозы»)	$ИнИБ_3$ («Нет защиты от реализованной угрозы»)	$ИнИБ_4$ («Реализация неизвестной угрозы»)	$ИнИБ_5$ («Не устраняется воздействие реализации угрозы»)
$НМЗ_1$ («Нарушены механизмы идентификации и аутентификации»)	+	+	-	-	-
$НМЗ_2$ («Нарушены механизмы контроля и разграничения доступа к защищаемым информационным ресурсам»)	+	+	+	-	+
$НМЗ_3$ («Нарушены механизмы контроля и разграничения доступа к сетевым ресурсам»)	+	-	-	-	+
$НМЗ_4$ («Нарушены механизмы защиты от вредоносных программ»)	-	+	+	-	-
$НМЗ_5$ («Нарушены механизмы защиты внутренних каналов связи»)	-	+	+	+	+
$НМЗ_6$ («Нарушены механизмы защиты внешних каналов связи»)	+	+	+	+	+
$НМЗ_7$ («Нарушены механизмы защиты от удаленных атак»)	-	+	+	+	+

Замечание. В дальнейшем будем считать выделенные показатели внутри «инцидентной» группы независимыми и равнозначными по важности.

Шаг 2. Для каждой «инцидентной» группы по каждому показателю получить множество факторов, сгруппированных в подмножества по важности (существенности) для обеспечения показателя, в соответствии с предпочтениями экспертов (всего экспертов N). Обозначим χ_{kn}^{ω} - ранги факторов, полученных по результатам экспертизы $(k=1,\dots,K; n=1,\dots,N; \omega=1,\dots,\Omega)$.

Пример 2.1. В приведенной ниже таблице 2.5 приведены ранги тридцати факторов, присвоенные им каждым из 13 экспертов в соответствии с представле-

нием экспертов о целесообразности включения фактора, как существенного для идентификации определенного инцидента по показателю $НМЗ_1$ («Нарушены механизмы идентификации и аутентификации»).

Замечание. Так как ранжировать факторы – качественные характеристики – достаточно сложно (а, может быть и невозможно) до уровня единиц рангов, то экспертам было предложено выделить «кластеры» факторов, обладающие по их (экспертов) мнению одинаковой «силой» в решении поставленной задачи. Поэтому в таблице 2.5 приведены «отрезки» одинаковых рангов.

Например, эксперт $Э_1$ посчитал факторы $Ф_{18}$,$Ф_{19}$ и $Ф_{20}$ одинаково существенными в решаемой задаче. Данные факторы должны были бы стоять на первом, втором и третьем местах и получить баллы 1, 2 и 3. Поскольку они равноценны, то получают в результате средний балл (1+2+3)/ 2 = 3.

Аналогичным образом построены соответствующие ячейки в таблице 2.5.

Анализируя результаты работы экспертов примера 2.1, приходится констатировать, что полного согласия между экспертами нет, а потому данные, приведенные в таблице, следует подвергнуть более тщательному математическому анализу. Конец примера 2.1.

Таблица 2.5 - Ранги факторов по результатам экспертизы (показатель НМЗ $_1$ «Нарушены механизмы идентификации и аутентификации»)

Э / Ф	$Э_1$	$Э_2$	$Э_3$	$Э_4$	$Э_5$	$Э_6$	$Э_7$	$Э_8$	$Э_9$	$Э_{10}$	$Э_{11}$	$Э_{12}$	$Э_{13}$
$Ф_1$	9-25	26-30	8-18	18-30	19-30	14-30	20-30	20-30	24-30	23-30	18-30	14-30	17-30
$Ф_2$	26-30	26-30	19-30	18-30	19-30	14-30	20-30	8-19	24-30	23-30	18-30	14-30	17-30
$Ф_3$	9-25	26-30	19-30	18-30	19-30	14-30	20-30	20-30	24-30	23-30	18-30	14-30	17-30
$Ф_4$	26-30	9-25	19-30	18-30	8-18	14-30	20-30	8-19	14-23	23-30	18-30	14-30	17-30
$Ф_5$	9-25	9-25	19-30	18-30	19-30	14-30	20-30	8-19	24-30	23-30	18-30	14-30	17-30
$Ф_6$	26-30	9-25	19-30	10-17	8-18	14-30	9-19	8-19	4-13	9-22	18-30	14-30	10-16
$Ф_7$	9-25	9-25	8-18	2-9	8-18	5-8	9-19	8-19	14-23	5-8	5-12	8-13	10-16
$Ф_8$	4-8	6-8	8-18	10-17	19-30	5-8	9-19	6-7	4-13	9-22	5-12	8-13	4-9
$Ф_9$	9-25	9-25	19-30	10-17	19-30	14-30	20-30	20-30	24-30	23-30	18-30	14-30	17-30
$Ф_{10}$	26-30	9-25	19-30	10-17	8-18	14-30	9-19	20-30	24-30	9-22	18-30	14-30	17-30
$Ф_{11}$	9-25	9-25	8-18	10-17	8-18	9-13	9-19	8-19	4-13	5-8	5-12	8-13	10-16
$Ф_{12}$	4-8	9-25	8-18	2-9	6-7	5-8	5-8	8-19	14-23	9-22	13-17	8-13	4-9
$Ф_{13}$	9-25	26-30	8-18	10-17	8-18	14-30	9-19	8-19	14-23	9-22	18-30	14-30	10-16
$Ф_{14}$	9-25	6-8	5-7	2-9	6-7	9-13	9-19	8-19	4-13	9-22	5-12	8-13	4-9
$Ф_{15}$	9-25	9-25	19-30	18-30	19-30	14-30	20-30	20-30	4-13	9-22	18-30	14-30	17-30
$Ф_{16}$	26-30	9-25	19-30	10-17	8-18	14-30	20-30	8-19	14-23	23-30	13-17	14-30	17-30
$Ф_{17}$	4-8	1-5	1-4	2-9	1-5	1-4	1-4	1-5	1-3	1-4	1-4	3-7	1-3
$Ф_{18}$	1-3	1-5	1-4	2-9	1-5	1-4	1-4	1-5	4-13	1-4	1-4	1-2	4-9
$Ф_{19}$	1-3	1-5	1-4	2-9	1-5	1-4	1-4	1-5	1-3	1-4	1-4	1-2	4-9
$Ф_{20}$	1-3	1-5	1-4	1	1-5	1-4	1-4	1-5	1-3	1-4	5-12	3-7	1-3
$Ф_{21}$	4-8	9-25	8-18	2-9	8-18	9-13	5-8	1-5	4-13	5-8	5-12	3-7	4-9
$Ф_{22}$	9-25	9-25	8-18	18-30	19-30	14-30	20-30	20-30	4-13	9-22	13-17	14-30	17-30
$Ф_{23}$	9-25	9-25	8-18	18-30	8-18	14-30	9-19	8-19	14-23	23-30	13-17	14-30	17-30
$Ф_{24}$	26-30	9-25	19-30	18-30	19-30	14-30	20-30	20-30	14-23	9-22	18-30	14-30	17-30
$Ф_{25}$	9-25	9-25	19-30	18-30	19-30	14-30	20-30	20-30	24-30	9-22	13-17	14-30	10-16
$Ф_{26}$	9-25	6-8	8-18	18-30	19-30	9-13	9-19	20-30	14-23	9-22	5-12	3-7	10-16
$Ф_{27}$	4-8	1-5	5-7	2-9	1-5	5-8	5-8	6-7	4-13	5-8	1-4	3-7	1-3
$Ф_{28}$	9-25	9-25	5-7	10-17	19-30	9-13	5-8	20-30	4-13	9-22	5-12	8-13	10-16
$Ф_{29}$	9-25	26-30	19-30	18-30	8-18	14-30	9-19	8-19	14-23	9-22	18-30	14-30	17-30
$Ф_{30}$	9-25	9-25	8-18	18-30	8-18	14-30	9-19	20-30	14-23	9-22	18-30	14-30	17-30

Шаг 3. Для получения группового мнения экспертов применить метод средних арифметических рангов [79]. Для этого подсчитаем средний арифметический ранг: $\tilde{\chi}_n^{\omega} = \frac{\sum_{k=1}^{K} \chi_{kn}^{\omega}}{K}$. По средним рангам строится итоговая

ранжировка (упорядочение), исходя из принципа - чем меньше средний ранг, чем существеннее фактор.

Пример 2.2. Столбец, обозначенный в таблице 2.6. как «$\tilde{\tilde{x}}_n^{\omega}$», содержит средние ранги факторов. Наименьший средний ранг, равный 3.0, у факторов Φ_{19}, Φ_{20} - следовательно, в итоговой ранжировке с точки зрения экспертов они равноценны (при рассматриваемом способе сведения вместе мнений экспертов), а потому они должны бы стоять на 1 и 2 местах и получают средний балл 1.5.

Ранжирование по суммам рангов (или, что то же самое, по средним арифметическим рангам) имеет вид:

$$\{\Phi_{19}, \Phi_{20}\} < \Phi_{17} < \Phi_{18} < \Phi_{27} < \Phi_{21} < \Phi_{14} < \{\Phi_{12}, \Phi_8\} < \Phi_7 < \Phi_{11} < \Phi_{28} < \Phi_{26} < \Phi_{13} < \Phi_6 < \Phi_{23} < \Phi_{30} < \Phi_{22} < \Phi_{29} < \Phi_{16} < \Phi_{10} < \Phi_{25} < \Phi_{15} < \Phi_4 < \Phi_5 < \Phi_9 < \Phi_{24} < \Phi_1 < \Phi_2 < < \Phi_3 \quad (2.1)$$

Здесь запись типа «$\Phi_а < \Phi_б$» означает, что фактор $\Phi_а$ предшествует фактору $\Phi_б$ (т.е. фактор $\Phi_а$ существеннее $\Phi_б$ для идентификации инцидентов по соответствующему показателю). Поскольку факторы Φ_{19} и Φ_{20}, а также факторы Φ_{12} и Φ_8, получили одинаковую сумму баллов, то по рассматриваемому методу они эквивалентны, а потому объединены в группу (в фигурных скобках). Конец примера 2.2

Таблица 2.6 - Обработка данных экспертизы (показатель НМЗ $_1$ «Нарушены механизмы идентификации и аутентификации»)

Э / Ф	$Э_1$	$Э_2$	$Э_3$	$Э_4$	$Э_5$	$Э_6$	$Э_7$	$Э_8$	$Э_9$	$Э_{10}$	$Э_{11}$	$Э_{12}$	$Э_{13}$	$\tilde{\chi}_n^{\omega}$	Ранг по $\tilde{\chi}_n^{\omega}$	$\hat{\chi}_n^{\omega}$	Ранг по $\hat{\chi}_n^{\omega}$
$Ф_1$	17	28	13	24	24.5	22	25	25	27	26.5	24	22	23.5	23.2	28	24	26
$Ф_2$	28	28	24.5	24	24.5	22	25	13.5	27	26.5	24	22	23.5	24.0	29	24.5	29.5
$Ф_3$	17	28	24.5	24	24.5	22	25	25	27	26.5	24	22	23.5	24.1	30	24.5	29.5
$Ф_4$	28	17	24.5	24	13	22	25	13.5	18.5	26.5	24	22	23.5	21.7	24	23.5	23.5
$Ф_5$	17	17	24.5	24	24.5	22	25	13.5	27	26.5	24	22	23.5	22.3	25	24	26
$Ф_6$	28	17	24.5	13.5	13	22	14	13.5	8.5	15.5	24	22	13	17.6	15	15.5	14.5
$Ф_7$	17	17	13	5.5	13	6.5	14	13.5	18.5	6.5	8.5	10.5	13	12.0	10	13	11
$Ф_8$	6	7	13	13.5	24.5	6.5	14	6.5	8.5	15.5	8.5	10.5	6.5	10.8	8.5	8.5	7.5
$Ф_9$	17	17	24.5	13.5	24.5	22	25	25	27	26.5	24	22	23.5	22.4	26	24	26
$Ф_{10}$	28	17	24.5	13.5	13	22	14	25	27	15.5	24	22	23.5	20.7	21	22	20
$Ф_{11}$	17	17	13	13.5	13	11	14	13.5	6.5	6.5	8.5	10.5	13	12.1	11	13	11
$Ф_{12}$	6	17	13	5.5	6.5	6.5	6.5	13.5	18.5	15.5	15	10.5	6.5	10.8	8.5	10.5	9
$Ф_{13}$	17	28	13	13.5	13	22	14	13.5	18.5	15.5	24	22	13	17.5	14	15.5	14.5
$Ф_{14}$	17	7	6	5.5	6.5	11	14	13.5	8.5	15.5	8.5	10.5	6.5	10.0	7	8.5	7.5
$Ф_{15}$	17	17	24.5	24	24.5	22	25	25	8.5	15.5	24	22	23.5	21.0	23	23.5	23.5
$Ф_{16}$	28	17	24.5	13.5	13	22	25	13.5	18.5	26.5	15	22	23.5	20.2	20	18.5	17.5
$Ф_{17}$	6	3	2.5	5.5	3	2.5	2.5	3	2	2.5	2.5	5	2	3.2	3	2.5	2.5
$Ф_{18}$	2	3	2.5	5.5	3	2.5	2.5	3	8.5	2.5	2.5	1.5	6.5	3.5	4	2.5	2.5
$Ф_{19}$	2	3	2.5	5.5	3	2.5	2.5	3	2	2.5	2.5	1.5	6.5	3.0	1.5	2.5	2.5
$Ф_{20}$	2	3	2.5	1	3	2.5	2.5	3	2	2.5	8.5	5	2	3.0	1.5	2.5	2.5
$Ф_{21}$	6	17	13	5.5	13	11	6.5	3	8.5	6.5	8.5	5	6.5	8.5	6	6.5	5
$Ф_{22}$	17	17	13	24	24.5	22	25	25	8.5	15.5	15	22	23.5	19.4	18	22	20
$Ф_{23}$	17	17	13	24	13	22	14	13.5	18.5	26.5	15	22	23.5	18.4	16	17	16
$Ф_{24}$	28	17	24.5	24	24.5	22	25	25	18.5	15.5	24	22	23.5	22.6	27	24	26
$Ф_{25}$	17	17	24.5	24	24.5	22	25	25	27	15.5	15	22	13	20.9	22	22	20
$Ф_{26}$	17	7	13	24	24.5	11	14	25	18.5	15.5	8.5	5	13	15.1	13	14	13
$Ф_{27}$	6	3	6	5.5	3	7	6.5	6.5	8.5	6.5	2.5	5	2	5.2	5	6	6
$Ф_{28}$	17	17	6	13.5	24.5	11	6.5	25	8.5	15.5	8.5	10.5	13	13.6	12	13	11
$Ф_{29}$	17	28	24.5	24	13	22	14	13.5	18.5	15.5	24	22	23.5	20.0	19	22	20
$Ф_{30}$	17	17	13	24	13	22	14	25	18.5	15.5	24	22	23.5	19.1	17	18.5	17.5

Замечание. Не совсем корректно усреднять ответы экспертов, полученные в порядковой шкале. Считается, что более эффективен здесь метод медиан рангов [79]. В дальнейшем экспертный анализ будем проводить только методом медиан.

Продолжение шага 3. Вычислить медианы ($\hat{\chi}_n^{\omega} = med\{\chi_{kn}^{\omega}\}$) совокупностей из 13 рангов, выставленных экспертами, соответствующих определенным факторам.

Пример 2.3. Медианы рангов приведены в таблице 2.3 в столбце, обозначенном «$\hat{\chi}_n^{\omega}$» . Итоговое упорядочение комиссии экспертов по методу медиан приведено в соответствующем столбце таблицы 2.6. Ранжирование (т.е. упорядочение - итоговое мнение комиссии экспертов) по медианам имеет вид:

$$\{\Phi_{17}, \Phi_{18}, \Phi_{19}, \Phi_{20}\} < \Phi_{21} < \Phi_{27} < \{\Phi_{14}, \Phi_8\} < \Phi_{12} < \{\Phi_7, \Phi_{11}, \Phi_{28}\} < \{\Phi_6, \Phi_{13}\} < \{\Phi_{16}, \Phi_{30}\} < \{\Phi_{10}, \Phi_{22}, \Phi_{25}, \Phi_{29}\} < \{\Phi_4, \Phi_{15}\} < \{\Phi_1, \Phi_5, \Phi_9, \Phi_{24}\} < \{\Phi_2, \Phi_3\}. \quad (2.2)$$

Сравнение ранжирований по методу средних арифметических (2.1) и методу медиан (2.2) показывает их близость (похожесть). Расхождение, касающееся упорядочения касается только малосущественных факторов. Рассмотренный пример демонстрирует сходство и различие ранжирований, полученных по методу средних арифметических рангов и по методу медиан, а также пользу от их совместного применения. Заметим, что различие в основном на малосущественных факторах со значением более 10. Конец примера 2.3.

Шаг 4. Проверить степень согласованности мнений экспертов. При ранжировании объектов используется мера согласованности мнений группы экспертов - дисперсионный коэффициент конкордации [98]. Рассмотрим матрицу результатов ранжирования факторов группой экспертов $\left\|\chi_{kn}^{\omega}\right\|$. Коэффициент конкордации оценок N экспертов по K объектам (факторам) для каждого из Ω показателей определяется по формуле:

$$W^{\omega} = \frac{12 \times Sum^{\omega}}{N^2(K^3 - K)}, \text{ где } Sum^{\omega} = \sum_{k=1}^{K}(\sum_{n=1}^{N} \chi_{kn}^{\omega} - \tilde{\chi}_k^{\omega})^2, \quad \tilde{\chi}_k^{\omega} = \frac{\sum_{n=1}^{N} \chi_{kn}^{\omega}}{N}$$

Замечание. Данная формула определяет коэффициент конкордации для случая отсутствия связных рангов. При $W^{\omega} = 0$ согласованность оценок различных экспертов отсутствует, а при $W^{\omega} = 1$ согласованность мнений экспертов полная. При крайних коэффициентах конкордации могут быть даны следующие рекомендации. Если $W^{\omega} \approx 0$, то для получения достоверных оценок следует уточнить исходные факторы и (либо) изменить состав группы экспертов. При $W^{\omega} \approx 1$ не всегда можно считать оценки объективными, поскольку может оказаться, что все члены экспертной группы условились придерживаться одинаковых взглядов. Необходимо, чтобы найденное значение W^{ω} было не менее заданного значения: $W^{\omega} \geq W_{зад}^{\omega}$. Обычно принимается $W_{зад}^{\omega} = 0.5$, т.е. при $W^{\omega} > 0.5$ выводы экспертов согласованы в большей мере (сходятся в оценке событий), чем не согласованы. При $W^{\omega} < 0.5$ оценки нельзя считать в достаточной степени согласованными.

Пример 2.4. Определим коэффициент конкордации экспертных оценок по НМЗ $_1$ «Нарушены механизмы идентификации и аутентификации» (таблица 2.7). Как видно из примера согласованность экспертов достаточно высокая. Конец примера 2.4.

Шаг 5. Выделить из ранжированного списка факторов три подмножества, в соответствии с предпочтениями экспертов, оценки которых примерно одинаковы для большинства экспертов:

- множество факторов, ранг которых у большинства экспертов максимальный (1 или 2), назовем данное подмножество множеством существенных факторов (СФ);

- множество факторов, не являющихся существенными (ранг которых у большинства экспертов не 1 или 2, но менее 10), назовем данное подмножество

множеством малосущественных факторов (МСФ);

Таблица 2.7 - Определение коэффициента конкордации (по показателю НМЗ $_1$ «Нарушены механизмы идентификации и аутентификации»)

	$\tilde{\chi}_k^{\omega}$	$\sum_{n=1}^{N} \chi_{kn}^{\omega}$	$\sum_{n=1}^{N} \chi_{kn}^{\omega} - \tilde{\chi}_k^{\omega}$	$(\sum_{n=1}^{N} \chi_{kn}^{\omega} - \tilde{\chi}_k^{\omega})^2$
Φ_1	189.7	301.7	112.0	12544.0
Φ_2	189.7	312.0	122.3	14957.3
Φ_3	189.7	337.1	147.4	21726.8
Φ_4	189.7	282.1	92.4	8537.8
Φ_5	189.7	289.9	100.2	10040.0
Φ_6	189.7	248.8	59.1	3492.8
Φ_7	189.7	169.0	-20.7	428.5
Φ_8	189.7	112,4	-77.3	5975.3
Φ_9	189.7	291.2	101.5	10302.3
Φ_{10}	189.7	269.1	79.4	6304.4
Φ_{11}	189.7	137.3	-52.4	20745.8
Φ_{12}	189.7	140.4	-49.30	2430.5
Φ_{13}	189.7	227.5	37.8	1428.8
Φ_{14}	189.7	130.0	-59.7	3564.1
Φ_{15}	189.7	273.0	83.3	6938.9
Φ_{16}	189.7	262.6	72.9	5314.4
Φ_{17}	189.7	41.6	- 148.1	21933.6
Φ_{18}	189.7	45.5	- 144.2	20793.6
Φ_{19}	189.7	39.0	- 150.7	22710.5
Φ_{20}	189.7	39.0	- 150.7	22710.5
Φ_{21}	189.7	110.0	-79.7	6352.1
Φ_{22}	189.7	252.2	62.5	3906.3
Φ_{23}	189.7	239.2	49.5	2450.3
Φ_{24}	189.7	293.8	104.1	10836.8
Φ_{25}	189.7	271.7	82.0	6724.0
Φ_{26}	189.7	196.3	6.6	43.56.0
Φ_{27}	189.7	67.0	-122.7	15055.3
Φ_{28}	189.7	176.8	-12.9	166.4
Φ_{29}	189.7	260.0	70.3	4942.1
Φ_{30}	189.7	248.3	58.6	3434.0
			Sum^{ω}	281103.0
			W^{ω}	0.7(4)

- множество остальных факторов, которые будем рассматривать как несущественные (НСФ). Заметим, что факторы несущественные в рамках данного показателя.

Пример 2.5. Для рассматриваемой обработка данных экспертизы по показателю НМЗ $_1$ «Нарушены механизмы идентификации и аутентификации» и приме-

нению медианного ранжирования СФ={ $Ф_{17}$, $Ф_{18}$, $Ф_{19}$, $Ф_{20}$ }. Такое выделение выглядит естественным, т.к. данные факторы необходимо в обязательном порядке учитывать при идентификации инцидента по данному показателю.

Для рассматриваемого примера МСФ={ $Ф_8$, $Ф_{12}$, $Ф_{14}$, $Ф_{21}$, $Ф_{27}$ }. Заметим, что согласованность экспертов во факторам «второго» плана достаточно высокая (по $Ф_8$ - 8 из 13, по $Ф_{12}$ – 7 из 13, по $Ф_{14}$ - 7 из 13, по $Ф_{21}$ -10 из 13, по $Ф_{27}$ – 13 из 13). Выявление малосущественных факторов может быть полезно при более точной идентификации вида инцидента. Конец примера 2.5.

В дальнейшем нас будут интересовать только множества СФ и МСФ.

Шаг 6. Обработать результаты экспертизы по всем показателям по аналогии с шагом 3. Получить множества СФ (МБ) и МСФ (МБ).

Пример 2.6. Обрабатывая результаты экспертизы по аналогии с примером 2.4, получим следующие подмножества:

- по показателю $НМЗ_2$ (Нарушены механизмы контроля и разграничения доступа к защищаемым ИР)

СФ($НМЗ_2$) = { $Ф_{20}$, $Ф_{21}$, $Ф_{22}$, $Ф_{23}$ },

МСФ($НМЗ_2$) = { $Ф_7$, $Ф_8$, $Ф_{13}$, $Ф_{17}$, $Ф_{25}$, $Ф_{26}$ };

- по показателю $НМЗ_3$ (Нарушены механизмы контроля и разграничения доступа к сетевым ресурсам)

СФ($НМЗ_3$) = { $Ф_7$, $Ф_8$, $Ф_{18}$, $Ф_{19}$, $Ф_{29}$ },

МСФ($НМЗ_3$) = ={ $Ф_6$, $Ф_{11}$, $Ф_{12}$, $Ф_{16}$, $Ф_{17}$, $Ф_{20}$, $Ф_{21}$, $Ф_{26}$, $Ф_{28}$, $Ф_{30}$ };

- по показателю $МБ_4$ (Нарушены механизмы защиты от ВП)

СФ($НМЗ_4$) = { $Ф_1$, $Ф_2$, $Ф_3$, $Ф_4$, $Ф_{17}$, $Ф_{23}$ },

МСФ($МБ_4$) = { $Ф_5$, $Ф_{22}$, $Ф_{25}$, $Ф_{26}$, $Ф_{27}$ };

- по показателю $НМЗ_5$ (Нарушены механизмы защиты внутренних КС)

СФ($НМЗ_5$) = { $Ф_{11}$ },

МСФ($НМЗ_5$) = { $Ф_4$, $Ф_7$, $Ф_8$, $Ф_9$, $Ф_{16}$, $Ф_{26}$, $Ф_{27}$, $Ф_{28}$, $Ф_{29}$, $Ф_{30}$ };

- по показателю $НМЗ_6$ (Нарушены механизмы защиты внешних КС)

СФ($МБ_6$)= { $Ф_{16}$ },

МСФ($МБ_6$)= { $Ф_1$, $Ф_8$, $Ф_{11}$, $Ф_{12}$, $Ф_{27}$, $Ф_{30}$ };

- по показателю $НМЗ_7$ (Нарушены механизмы защиты от удаленных атак)

$СФ(НМЗ_7) = \{ Ф_4, Ф_8, Ф_{12}, Ф_{17}, Ф_{29} \}$,

$МСФ(НМЗ_7) = \{ Ф_6, Ф_{11}, Ф_{12}, Ф_{16}, Ф_{17}, Ф_{20}, Ф_{21}, Ф_{26}, Ф_{28}, Ф_{30} \}$.

Для наглядности выявленные существенные (обозначены символом «**x**») и малосущественные (обозначены символом «**0**») факторы для нарушенных мер ТПИБ представлены таблицей 2.8.

Таблица 2.8 - Существенные и малосущественные факторы

Нарушенная мера защиты / Факторы	$НМЗ_1$	$НМЗ_2$	$НМЗ_3$	$НМЗ_4$	$НМЗ_5$	$НМЗ_6$	$НМЗ_7$
$Ф_1$				**x**		**0**	**0**
$Ф_2$				**x**			**0**
$Ф_3$				**x**			**0**
$Ф_4$				**x**	**0**		**x**
$Ф_5$				**0**			
$Ф_6$			**0**				
$Ф_7$		**0**	**x**		**0**		**0**
$Ф_8$		**0**	**x**		**0**	**0**	**x**
$Ф_9$					**0**		
$Ф_{10}$							
$Ф_{11}$			**0**		**x**	**0**	
$Ф_{12}$			**0**			**0**	**x**
$Ф_{13}$		**0**					
$Ф_{14}$							**0**
$Ф_{15}$							
$Ф_{16}$			**0**		**0**	**x**	
$Ф_{17}$		**0**	**0**	**x**			**x**
$Ф_{18}$			**x**				
$Ф_{19}$	**x**		**x**				**0**
$Ф_{20}$	**x**	**x**	**0**				
$Ф_{21}$	**x**	**x**	**0**				
$Ф_{22}$	**x**	**x**		**0**			
$Ф_{23}$		**x**		**x**			**x**
$Ф_{24}$							
$Ф_{25}$		**0**		**0**			
$Ф_{26}$		**0**	**0**	**0**	**0**		**0**
$Ф_{27}$	**0**			**0**	**0**	**0**	**0**
$Ф_{28}$			**0**		**0**		**0**
$Ф_{29}$			**x**		**0**		
$Ф_{30}$			**0**		**0**	**0**	

Сводная таблица 2.9 показывает соответствие «инциденты - существенные и малосущественные факторы».

Таблица 2.9 - Существенные и малосущественные факторы инцидентов ИБ

Инциденты / Факторы	$ИнИБ_1$	$ИнИБ_2$	$ИнИБ_3$	$ИнИБ_4$	$ИнИБ_5$
$Ф_1$		**x**	**x**	**0**	**0**
$Ф_2$		**x**	**x**	**0**	**0**
$Ф_3$		**x**	**x**	**0**	**0**
$Ф_4$		**x**	**x**	**x**	**x**
$Ф_5$		**0**	**0**		
$Ф_6$	**0**				**0**
$Ф_7$	**x**	**0**	**0**	**0**	**x**
$Ф_8$	**x**	**x**	**x**	**x**	**x**
$Ф_9$		**0**			**0**
$Ф_{10}$					
$Ф_{11}$	**0**	**x**	**x**	**x**	**x**
$Ф_{12}$	**0**	**x**	**x**	**x**	**x**
$Ф_{13}$	**0**	**0**	**0**		**0**
$Ф_{14}$		**0**	**0**	**0**	**0**
$Ф_{15}$					
$Ф_{16}$	**0**	**x**	**x**	**x**	**x**
$Ф_{17}$	**0**	**x**	**x**	**x**	**x**
$Ф_{18}$	**x**	**x**			**x**
$Ф_{19}$	**x**	**x**	**0**	**0**	**x**
$Ф_{20}$	**x**	**x**	**x**		**x**
$Ф_{21}$	**x**	**x**	**x**		**x**
$Ф_{22}$	**x**	**x**	**x**	**0**	**x**
$Ф_{23}$	**x**	**x**	**x**	**x**	**x**
$Ф_{24}$					
$Ф_{25}$	**0**	**0**	**0**		**0**
$Ф_{26}$	**0**	**0**	**0**	**0**	**0**
$Ф_{27}$	**0**	**0**	**0**	**0**	**0**
$Ф_{28}$	**0**	**0**	**0**	**0**	**0**
$Ф_{29}$	**x**	**0**	**0**	**0**	**0**
$Ф_{30}$	**0**	**0**	**0**	**0**	**0**

Анализ данных таблицы 2.9:

- строки $Ф_{10}$, $Ф_{15}$, $Ф_{24}$ не помечены знаками СФ и МСФ ни для одного

ИнИБ. Это означает, что, по коллективному мнению экспертов, данные факторы ($Ф_{10}$ – «Не все неиспользуемые порты АСО отключены», $Ф_{15}$ – «Не весь входящий и исходящий трафик анализируется на наличие ВП и сигнатур известных атак», $Ф_{24}$ – «Реестр ПО содержит сведения о ПО с «просроченной» лицензией») напрямую не приводят к серьезному нарушению ТПИБ. Следовательно, из дальнейшего рассмотрения данные факторы следует исключить;

- в практической работе для повышения производительности контроля инцидентов возникает возможность ограничиться только анализом существенных факторов.

Конец примера 2.6.

Шаг 6. Получить множество существенных факторов объединением множеств СФ для каждого инцидента: $Ф_{СФ} = \bigcup_{\omega} Ф_{СФ}^{\omega}, \omega = 1,..., \Omega$. Конец алгоритма.

Пример 2.7. Полное множество СФ для всех видов инцидентов получаем объединением множеств СФ для каждого инцидента (таблица 2.10):

СФ($ИнИБ_1$) = { $Ф_7$, $Ф_8$, $Ф_{18}$, $Ф_{19}$, $Ф_{20}$, $Ф_{23}$, $Ф_{29}$ };

СФ($ИнИБ_2$) = { $Ф_1$, $Ф_2$, $Ф_3$, $Ф_4$, $Ф_8$, $Ф_{11}$, $Ф_{12}$, $Ф_{16}$, $Ф_{17}$, $Ф_{18}$, $Ф_{19}$, $Ф_{20}$, $Ф_{23}$ };

СФ($ИнИБ_3$) = { $Ф_1$, $Ф_2$, $Ф_3$, $Ф_4$, $Ф_8$, $Ф_{11}$, $Ф_{12}$, $Ф_{16}$, $Ф_{17}$, $Ф_{20}$, $Ф_{21}$, $Ф_{22}$, $Ф_{23}$ };

СФ($ИнИБ_4$) = { $Ф_4$, $Ф_8$, $Ф_{11}$, $Ф_{12}$, $Ф_{16}$, $Ф_{17}$, $Ф_{23}$ }.

СФ($ИнИБ_5$) = { $Ф_4$, $Ф_7$, $Ф_8$, $Ф_{11}$, $Ф_{12}$, $Ф_{16}$, $Ф_{17}$, $Ф_{18}$, $Ф_{19}$, $Ф_{20}$, $Ф_{21}$, $Ф_{22}$, $Ф_{23}$ }.

Конец примера 2.6.

Таким образом, удалось уменьшить количество факторов, влияющих на возникновение инцидентов ИБ и выявить их совокупности, позволяющие идентифицировать вид инцидента (с 30 до 17, т.е. почти в два раза). На рис.2.1 представлена блок – схема описанного алгоритма.

Таблица 2. 10 - Существенные факторы возникновения инцидентов

Инциденты / Факторы	Ин1	Ин2	Ин3	Ин4	Ин5
$Ф_1$		**x**	**x**		
$Ф_2$		**x**	**x**		
$Ф_3$		**x**	**x**		
$Ф_4$		**x**	**x**	**x**	**x**
$Ф_7$	**x**				**x**
$Ф_8$	**x**	**x**	**x**	**x**	**x**
$Ф_{11}$		**x**	**x**	**x**	**x**
$Ф_{12}$		**x**	**x**	**x**	**x**
$Ф_{16}$		**x**	**x**	**x**	**x**
$Ф_{17}$		**x**	**x**	**x**	**x**
$Ф_{18}$	**x**	**x**			**x**
$Ф_{19}$	**x**	**x**			**x**
$Ф_{20}$	**x**	**x**	**x**		**x**
$Ф_{21}$	**x**	**x**	**x**		**x**
$Ф_{22}$	**x**	**x**	**x**		**x**
$Ф_{23}$	**x**	**x**	**x**	**x**	**x**
$Ф_{29}$	**x**				

Выводы к главе 2

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

Разработана методика формирования множества существенных факторов возникновения инцидентов информационной безопасности, которые определяют параметры контроля. В основе методики использован способ «усечения» полного множества факторов нарушения ТПИБ по разработанным правилам. На первом этапе методики выявляется взаимосвязь инцидентов разного типа с факторами нарушения конкретной технической политики. На втором этапе выполняется групповой экспертный анализ факторов, в основе которого использован способ группового ранжирования при обеспечении согласованности экспертов.

Практическое применение методики позволяет уменьшить количество факторов в среднем в 1.5 – 2 раза. Данный «выигрыш» зависит от особенностей конкретной КИТС и действующей технической политики.

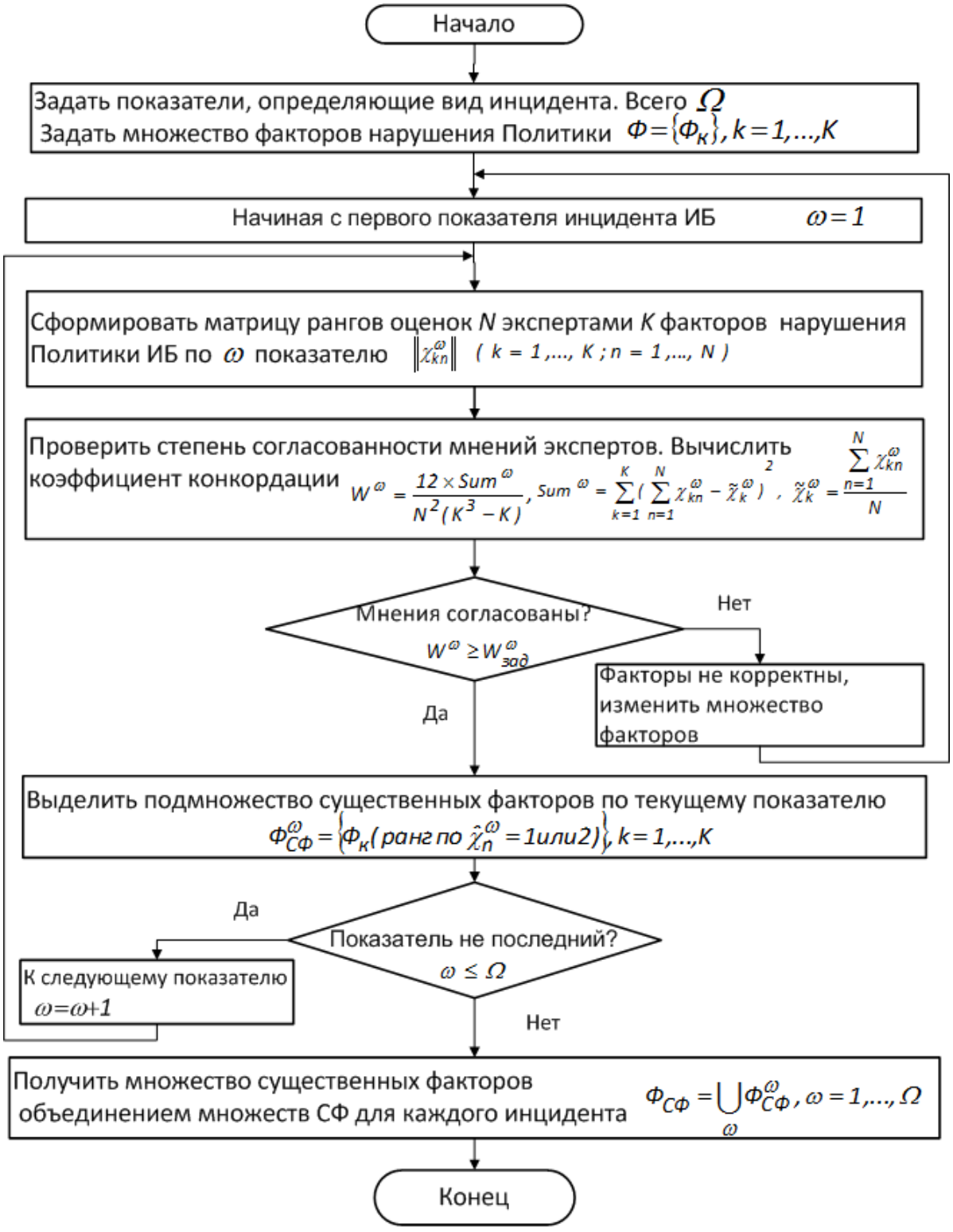


Рисунок 2.1 - Блок-схема алгоритма определения существенных факторов нарушения Политики ИБ.

3 РАЗРАБОТКА МАТЕМАТИЧЕСКИХ МОДЕЛЕЙ И АЛГОРИТМОВ ОПТИМИЗАЦИИ КОНТРОЛЯ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Оптимизация контроля инцидентов ИБ заключается в формировании оптимального пакета контроля. Оптимальным в предлагаемом подходе считается такой пакет, который содержит минимальное количество контролируемых параметров, которые в совокупности обеспечивают обнаружение инцидента определенного вида с вероятностью не хуже заданной. Контролируемые параметры пакета должны быть «распределены» по узлам КТС. Кроме того, для повышения оперативности обнаружения инцидента время, отводимое на контроль каждого параметра, должно быть минимально возможным. Для обнаружения инцидента по совокупности событий нарушения ТПИБ необходимы решающие правила, на основе которых автоматизированной системой контроля буде принято решение о наличие инцидента ИБ.

В главе разрабатываются математические и алгоритмические модели формирования пакета контроля инцидентов ИБ в КТС и распределения контролируемых параметров по узлам сети.

3.1 Разработка алгоритма формирования пакета контролируемых параметров

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 $\|p_{kt}\|, \|q_{kt}\|, k=1,...,K; K=I\times J;\ t=1,...,T.$ Требуется

- определить минимальный пакет контроля инцидента $M_{k\min}$, распределить кон-

тролируемые параметры по узлам.

Алгоритм формирования пакета контроля инцидентов

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

Пример 3.1. Пусть матрицы $\|p_{kt}\|$ и $\|q_{kt}\|$, полученные экспериментально, представлены таблицами 3.1 и 3.2 соответственно.

Таблица 3.1 - Исходная матрица $\|p_{kt}\|$

i, j	K	t				
		1	2	3	4	5
1,1	1	0.30	0.60	0.85	0.96	0.99
1,2		-	-	-	-	-
1,3	2	0.30	0.70	0.95	0.99	0.99
2,1		-	-	-	-	-
2,2	3	0.10	0.10	0.65	0.9	0.99
2,3		-	-	-	-	-
3,1	4	0.30	0.60	0.85	0.96	0.99
3,2	5	0.10	0.10	0.65	0.9	0.99
3,3		-	-	-	-	-

Таблица 3.2 - Исходная матрица $\|q_{kt}\|$

i, j	K	t				
		1	2	3	4	5
1,1	1	0.15	0.10	0.01	0.01	0.01
1,2		-	-	-	-	-
1,3	2	0.15	0.10	0.01	0.01	0.01
2,1		-	-	-	-	-
2,2	3	0.20	0.10	0.05	0.05	0.01
2,3		-	-	-	-	-
3,1	4	0.15	0.10	0.10	0.10	0.01
3,2	5	0.10	0.10	0.05	0.05	0.01
3,3		-	-	-	-	-

Здесь $I = 3$, $J = 3$, $m_1 = K = 9, T = max(t_{ij}^{max}) = 5$. Знаком «-» показан факт отсутствия параметра в контролируемом узле. В дальнейшем соответствующие строки удалим ($m_1 = 5$).

Шаг 2. Сформировать массивы $\|P_{lt}\|$ и $\|Q_{lt}\|$, $l = 0,\ldots,(2^{M_k} - 1)$, $t = \overline{1,T}$, 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 $\zeta_{lt} = P_{lt} / Q_{lt}$.

Пример 3.2. Таблица 3.3 содержит значения вероятности корректного и «ложного» обнаружения инцидента, полученные на всех возможных наборах событий ($2^{m_1} - 1$) в фиксированные моменты времени в соответствии с примером 3.1. Сверху в ячейках значения $P_{ИНlt}$, снизу - $Q_{ЛТlt}$. Таблица 3.4 содержит значения $\|\zeta_{lt}\|$. Конец примера 3.2.

Таблица 3.3 - Значения вероятности корректного и «ложного» обнаружения инцидента по комбинации событий

l	Комбинация событий	t				
		1	2	3	4	5
0	$\overline{X}_1\overline{X}_2\overline{X}_3\overline{X}_4\overline{X}_5$	0.2800	0.0400	0.0001	0	0
		0.4400	0.0040	0.8000	0.8000	0
1	$\overline{X}_1\overline{X}_2\overline{X}_3\overline{X}_4 X_5$	0.0300	0.0040	0.0002	0	0
		0.0500	0.0700	0.0400	0.0400	0.0100
2	$\overline{X}_1\overline{X}_2\overline{X}_3 X_4\overline{X}_5$	0.1200	0.0600	0.0008	0	0
		0.0800	0.0700	0.0900	0.0900	0.0100
3	$\overline{X}_1\overline{X}_2\overline{X}_3 X_4 X_5$	0.0100	0.0060	0.0010	0	0
		0.009	0.0070	0.0050	0.0050	0.0001
4	$\overline{X}_1\overline{X}_2 X_3\overline{X}_4\overline{X}_5$	0.1100	0.0040	0.0003	0	0
		0.1100	0.0700	0.0420	0.0420	0.0100
5	$\overline{X}_1\overline{X}_2 X_3\overline{X}_4 X_5$	0.0030	0.0005	0.0005	0	0
		0.0100	0.007	0.0020	0.0020	0.0001
6	$\overline{X}_1\overline{X}_2 X_3 X_4\overline{X}_5$	0.0100	0.006	0.0010	0	0.0100
		0.0200	0.007	0.0050	0.0050	0.0001
7	$\overline{X}_1\overline{X}_2 X_3 X_4 X_5$	0.0010	0.0007	0.0030	0.0003	0.0001
		0.0020	0.0008	0.0002	0.0002	0
8	$\overline{X}_1 X_2\overline{X}_3\overline{X}_4\overline{X}_5$	0.1200	0.0900	0.0030	0	0
		0.0800	0.0700	0.0080	0.0080	0.0100
9	$\overline{X}_1 X_2\overline{X}_3\overline{X}_4 X_5$	0.0100	0.0100	0.0050	0.0001	0
		0.0090	0.0070	0.0004	0.0004	0.0001

Продолжение таблицы 3.3

l	Комбинация событий	t				
		1	2	3	4	5
10	$\overline{X}_1 X_2 \overline{X}_3 X_4 \overline{X}_5$	0.0500	0.1400	0.0150	0.0004	0
		0.0140	0.0070	0.0009	0.0009	0.0001
11	$\overline{X}_1 X_2 \overline{X}_3 X_4 X_5$	0.0060	0.0200	0.0280	0.0030	0.0001
		0.0020	0.0008	0.0001	0.0001	0
12	$\overline{X}_1 X_2 X_3 \overline{X}_4 \overline{X}_5$	0.0100	0.0100	0.0050	0.0001	0
		0.0200	0.0070	0.0004	0.0004	0.0001
13	$\overline{X}_1 X_2 X_3 \overline{X}_4 X_5$	0.0010	0.0010	0.0090	0.0010	0.0001
		0.0020	0.0008	0	0	0
14	$\overline{X}_1 X_2 X_3 X_4 \overline{X}_5$	0.0060	0.0200	0.0300	0.0030	0.0001
		0.0020	0.0008	0	0	0
15	$\overline{X}_1 X_2 X_3 X_4 X_5$	0.0006	0.0020	0.0500	0.0300	0.0100
		0.0004	0.0001	0	0	0
16	$X_1 \overline{X}_2 \overline{X}_3 \overline{X}_4 \overline{X}_5$	0.1200	0.0600	0.0008	0	0
		0.0800	0.0700	0.0080	0.0080	0.0100
17	$X_1 \overline{X}_2 \overline{X}_3 \overline{X}_4 X_5$	0.0100	0.0060	0.0010	0	0
		0.0090	0.0070	0.0004	0.0004	0.0001
18	$X_1 \overline{X}_2 \overline{X}_3 X_4 \overline{X}_5$	0.0500	0.0900	0.0040	0.0001	0
		0.0100	0.0070	0.0009	0.0009	0.0001
19	$X_1 \overline{X}_2 \overline{X}_3 X_4 X_5$	0.0060	0.0100	0.0080	0.0008	0.0001
		0.0020	0.0008	0.0001	0.0001	0
20	$X_1 \overline{X}_2 X_3 \overline{X}_4 \overline{X}_5$	0.0100	0.0060	0.0010	0	0
		0.0200	0.0070	0.0004	0.0004	0.0001
21	$X_1 \overline{X}_2 X_3 \overline{X}_4 X_5$	0.0010	0.0007	0.0030	0.0003	0.0001
		0.0020	0.0008	0	0	0
22	$X_1 \overline{X}_2 X_3 X_4 \overline{X}_5$	0.0060	0.0100	0.0080	0.0008	0.0001
		0.0020	0.0008	0	0	0
23	$X_1 \overline{X}_2 X_3 X_4 X_5$	0.0006	0.0010	0.0200	0.0070	0.0100
		0.0004	0	0	0	0
24	$X_1 X_2 \overline{X}_3 \overline{X}_4 \overline{X}_5$	0.0500	0.1400	0.0150	0.0004	0
		0.0140	0.0070	0	0	0.0001
25	$X_1 X_2 \overline{X}_3 \overline{X}_4 X_5$	0.0060	0.0150	0.0280	0.0030	0.0001
		0.0020	0.0008	0	0	0
26	$X_1 X_2 \overline{X}_3 X_4 \overline{X}_5$	0.0200	0.2000	0.1840	0.0090	0.0001
		0.0020	0.0008	0	0	0
27	$X_1 X_2 \overline{X}_3 X_4 X_5$	0.0020	0.0200	0.1560	0.0800	0.0100
		0.0003	0	0	0	0

Окончание таблицы 3.3

l	Комбинация событий	t				
		1	2	3	4	5
28	$X_1 X_2 X_3 \overline{X}_4 \overline{X}_5$	0.0060	0.0150	0.0280	0.0030	0.0001
		0.0020	0.0008	0	0	0
29	$X_1 X_2 X_3 \overline{X}_4 X_5$	0.0006	0.0150	0.0500	0.0300	0.0100
		0.0004	0	0	0	0
30	$X_1 X_2 X_3 X_4 \overline{X}_5$	0.0020	0.0230	0.0500	0.0300	0.0100
		0.0006	0.0001	0	0	0
31	$X_1 X_2 X_3 X_4 X_5$	0.0003	0.003	0.29	0.7400	0.9500
		0	0	0	0	0

Таблица 3.4 - Значения $\|\zeta_{lt}\|$

l	Комбинация событий	t				
		1	2	3	4	5
0	$\overline{X}_1 \overline{X}_2 \overline{X}_3 \overline{X}_4 \overline{X}_5$	0.6	10	0	0	0
1	$\overline{X}_1 \overline{X}_2 \overline{X}_3 \overline{X}_4 X_5$	0.6	0.1	0	0	0
2	$\overline{X}_1 \overline{X}_2 \overline{X}_3 X_4 \overline{X}_5$	1.5	0.8	0	0	0
3	$\overline{X}_1 \overline{X}_2 \overline{X}_3 X_4 X_5$	1.1	0.8	0.2	0	0
4	$\overline{X}_1 \overline{X}_2 X_3 \overline{X}_4 \overline{X}_5$	1	0.6	0	0	0
5	$\overline{X}_1 \overline{X}_2 X_3 \overline{X}_4 X_5$	0.3	0.1	0.3	0	0
6	$\overline{X}_1 \overline{X}_2 X_3 X_4 \overline{X}_5$	0.5	0.8	0.2	0	100
7	$\overline{X}_1 \overline{X}_2 X_3 X_4 X_5$	0.5	0.8	15	1.5	100
8	$\overline{X}_1 X_2 \overline{X}_3 \overline{X}_4 \overline{X}_5$	1.5	1.3	0.4	0	0
9	$\overline{X}_1 X_2 \overline{X}_3 \overline{X}_4 X_5$	1.1	1.4	12	0.3	0
10	$\overline{X}_1 X_2 \overline{X}_3 X_4 \overline{X}_5$	3	20	16.7	0.5	0
11	$\overline{X}_1 X_2 \overline{X}_3 X_4 X_5$	3	25	560	60	100
12	$\overline{X}_1 X_2 X_3 \overline{X}_4 \overline{X}_5$	0.5	1.3	12.5	0.25	0
13	$\overline{X}_1 X_2 X_3 \overline{X}_4 X_5$	0.5	1.3	450	50	100
14	$\overline{X}_1 X_2 X_3 X_4 \overline{X}_5$	3	25	600	80	100
15	$\overline{X}_1 X_2 X_3 X_4 X_5$	1.5	22.2	25	15	1000000
16	$X_1 \overline{X}_2 \overline{X}_3 \overline{X}_4 \overline{X}_5$	1.5	0.8	0.1	0	0

Продолжение таблицы 3.4

l	Комбинация событий	t				
		1	2	3	4	5
17	$X_1\overline{X}_2\overline{X}_3\overline{X}_4X_5$	0.12	0.8	2.5	0.1	0
18	$X_1\overline{X}_2\overline{X}_3X_4\overline{X}_5$	5	14	4	0.1	0
19	$X_1\overline{X}_2\overline{X}_3X_4X_5$	3	12.5	160	16	100
20	$X_1\overline{X}_2X_3\overline{X}_4\overline{X}_5$	0.5	0.8	2.5	0.1	0
21	$X_1\overline{X}_2X_3\overline{X}_4X_5$	0.5	0.8	150	16	100
22	$X_1\overline{X}_2X_3X_4\overline{X}_5$	3	12.5	160	16	100
23	$X_1\overline{X}_2X_3X_4X_5$	1.5	11.1	10000	3500	1000000
24	$X_1X_2\overline{X}_3\overline{X}_4\overline{X}_5$	3.5	20	187.5	5	0
25	$X_1X_2\overline{X}_3\overline{X}_4X_5$	3	18.75	7000	750	100
26	$X_1X_2\overline{X}_3X_4\overline{X}_5$	10	250	8400	900	100
27	$X_1X_2\overline{X}_3X_4X_5$	15	222	312000	160000	1000000
28	$X_1X_2X_3\overline{X}_4\overline{X}_5$	3	18.8	7000	750	100
29	$X_1X_2X_3\overline{X}_4X_5$	1.5	167	250000	150000	1000000
30	$X_1X_2X_3X_4\overline{X}_5$	3.3	256	100000	60000	1000000
31	$X_1X_2X_3X_4X_5$	4.5	300	9700000	24700000	9500000000

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

Пример 3.3. В рассматриваемых примерах $\zeta_{доп} = \dfrac{0.85}{0.01} = 85.$

$$\Psi = \{\Psi_6^5, \Psi_7^5, \Psi_{11}^5, \Psi_{13}^5, \Psi_{14}^5, \Psi_{15}^5, \Psi_{19}^5, \Psi_{21}^5, \Psi_{22}^5, \Psi_{23}^5, \Psi_{24}^5,$$
$$\Psi_{25}^5, \Psi_{26}^5, \Psi_{27}^5, \Psi_{28}^5, \Psi_{29}^5, \Psi_{30}^5, \Psi_{31}^5\}.$$

Клетки таблицы, соответствующие данным наборам на минимально возможном значении времени контроля выделены серой «заливкой». Отсортированный массив элементов Ψ по убыванию их $P_{ИНlt_{min}}$ представлен в таблице 3.5.

Таблица 3.5 - Отсортированный массив элементов Ψ

l	Комбинация событий	$P_{ИНlt_{min}}$
31	$x_1 x_2 x_3 x_4 x_5$	0.2900
26	$x_1 x_2 \bar{x}_3 x_4 \bar{x}_5$	0.200
27	$x_1 x_2 \bar{x}_3 x_4 x_5$	0.1600
25	$x_1 x_2 \bar{x}_3 \bar{x}_4 x_5$	0.0300
28	$x_1 x_2 x_3 \bar{x}_4 \bar{x}_5$	0.0300
11	$\bar{x}_1 x_2 \bar{x}_3 x_4 x_5$	0.0300
14	$\bar{x}_1 x_2 x_3 x_4 \bar{x}_5$	0.0300
23	$x_1 \bar{x}_2 x_3 x_4 x_5$	0.0200
24	$x_1 x_2 \bar{x}_3 \bar{x}_4 \bar{x}_5$	0.0200
29	$x_1 x_2 x_3 \bar{x}_4 x_5$	0.0200
30	$x_1 x_2 x_3 x_4 \bar{x}_5$	0.0200
6	$\bar{x}_1 \bar{x}_2 x_3 x_4 \bar{x}_5$	0.0100
13	$\bar{x}_1 x_2 x_3 \bar{x}_4 x_5$	0.0100
15	$\bar{x}_1 x_2 x_3 x_4 x_5$	0.0100
19	$x_1 \bar{x}_2 \bar{x}_3 x_4 x_5$	0.0100
22	$x_1 \bar{x}_2 x_3 x_4 \bar{x}_5$	0.0100
21	$x_1 \bar{x}_2 x_3 \bar{x}_4 x_5$	0.0030
7	$\bar{x}_1 \bar{x}_2 x_3 x_4 x_5$	0.0001

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 $P_{lt_{min}}$).

Пример 3.4. Анализируем таблицу 5. $|\Psi| = 18$. Значение $P_{ИН} = \sum_{l=1}^{|\Psi|} P_{ИНlt_{min}} = 0.9031 \geq P^* = 0.85$. Удаляем последовательно наборы 7, 21, 22, 19, 15, 13, 6. Соответствующие строки таблицы 5 выделены серой «заливкой». Новое значение $|\Psi| = 11 . P_{ИН} = 0.85 = P^*$. Конец примера 3.4.

Шаг 6. Выполнить минимизацию логической функции, образованной дизъ-

юнкцией термов в Ψ. Число оставшихся логических переменных определяет значение $M_{k\,min}$. Данная функция представляет собой совершенную дизъюнктивную нормальную форму (СДНФ), так как содержит логические термы максимального ранга. Формально минимизация есть процесс получения минимальной ДНФ (МДНФ) исходной логической функции, которая содержит минимальное количество логических переменных и логических операций над ними. Конец алгоритма.

Пример 3.5. Выполним минимизацию функции, составленной при использовании результатов таблицы 5, применив метод Квайна – Мак Класки. Получим минимальную дизъюнктивную нормальную форму

МДНФ= $x_1 x_2 \vee x_1 x_3 x_4 x_5 \vee x_2 \overline{x}_3 x_4 x_5 \vee x_2 x_3 x_4 \overline{x}_5$.

Конец примера 3.5.

3.2 Разработка алгоритма назначения контролируемым параметрам минимально допустимого времени на контроль и их распределение по узлам сети

Данный алгоритм естественным образом продолжает предыдущий.

Алгоритм назначения контролируемым параметрам минимально допустимого времени на контроль

Шаг 1. Полный перебор: для всех возможных наборов $t = 1,\ldots,T$ $(T = max(t_{ij}^{max}))$ вычислить $T_z = \sum_{k=1}^{K} t_z(X_k)$ и $P_{ИНz}$, здесь $z = 1,\ldots,T^T$ - номер набора, $t_z(X_k)$ - значение времени для X_k на данном наборе.

Шаг 2. Отобрать множество $\hat{Z}$ наборов значений $t_z(X_k)$ по правилу: $z \in \hat{Z}$, если $P_{ИНz} \geq P^*$. Каждому набору из Ψ поставить в соответствие значение $P_{ИНlt_{min}}$. Оптимальный набор имеет номер минимального числа из $\hat{Z}$:

$z_{опт} = min\{\hat{z}\}$. Конец алгоритма.

Пример 3.6. Выполним процедуру определения минимального времени на контроль по каждому параметру в соответствии с шагами 1 и 2 приведенного алгоритма и используя данные предыдущих примеров. Для $T = max(t_{ij}^{max}) = 5$ всего наборов $5^5 = 3125$, поэтому приведем лишь фрагмент анализа, содержащий оптимальные наборы. Таблица 3.6 содержит наборы $t_z(X_k)$ по событиям (параметрам), а также вычисляемые значения $T_z = \sum_{k=1}^{K} t_z(X_k)$ и $P_{ИНz} = \sum_{l=1}^{|\Psi|} P_{ИНzl}$.

Таблица 3.6 - Значения T_z и $P_{ИНz}$ на наборах $t_z(X_k)$

	Набор t по событиям (параметрам)						$P_{ИНz}$				
z	x_1	x_2	x_3	x_4	x_5	$T_z = \sum_{k=1}^{K} t_z(X_k)$	f_1	f_2	f_3	f_4	$P_{ИНz} = \sum_{l=1}^{\|\Psi\|} P_{ИНzl}$
1687	2	3	2	2	2	11	0.57	0.004	0.04	0.05	0.664
1688	2	3	2	2	3	12	0.57	0.02	0.21	0.02	0.82
1689	2	3	2	3	2	12	0.57	0.01	0.03	0.07	0.68
1690	2	3	2	3	3	13	0.57	0.03	0.27	0.03	0.9
1691	2	3	3	2	2	12	0.57	0.02	0.03	0.33	0.95
1692	2	3	3	2	3	13	0.57	0.12	0.03	0.13	0.85
1693	2	3	3	3	2	13	0.57	0.04	0.03	0.3	0.94
1694	2	3	3	3	3	14	0.57	0.11	0.12	0.18	0.98
2187	3	2	2	2	2	11	0.6	0.04	0.004	0.04	0.684
2188	3	2	2	2	3	12	0.6	0.21	0.02	0.01	0.84
2189	3	2	2	3	2	12	0.6	0.04	0.05	0.05	0.74
2190	3	2	2	3	3	13	0.6	0.27	0.04	0.02	0.93
2191	3	2	3	2	2	12	0.6	0.03	0.02	0.25	0.9
2192	3	2	3	2	3	13	0.6	0.18	0.12	0.07	0.97
2193	3	2	3	3	2	13	0.6	0.05	0.03	0.30	0.98
2194	3	2	3	3	3	14	0.6	0.21	0.14	0.02	0.97

В таблице введено обозначение минтермов: $f_1 = X_1 X_2$, $f_2 = X_1 X_3 X_4 X_5$, $f_3 = X_2 \bar{X}_3 X_4 X_5$, $f_4 = X_2 X_3 X_4 \bar{X}_5$. Из таблицы видно, что

условию $\sum_{l=1}^{|\Psi|} P_{ИНl t_{min}} \geq P^*$ соответствуют наборы с номерами 1690, 1691, 1692, 1693, 1694, 2190, 2191, 2192, 2193.

Минимальное суммарное время на контроль (12 единиц) имеют наборы с номерами 1691 и 2191. Из них выбираем набор номер 1691, так как он обеспечивает большую вероятность обнаружения (0.95) по сравнению с набором 12 (0.9). Таким образом, чтобы обеспечить требуемую вероятность обнаружения инцидента за минимальное время, необходимо параметр 1 в первом узле измерять 2 ед.времени, параметр 2 в первом узле – 3 ед.времени, параметр 2 в узле 2 – 3 ед.времени, первый и второй параметры в 3 узле по 2 ед.времени. Из практических соображений иногда может быть желательно, чтобы длительности оценки параметров в одном узле была не только минимальной, но и одинаковой. Для нашего примера следует ввести коррекцию – 1 и 2 параметры измерять по 3 ед.времени. Это сделать можно, так как вероятность обнаружения по каждому контролируемому параметру с увеличением времени растер, а вероятность ложной тревоги – уменьшается. Конец примера 3.6.

На рис. 3.1 представлена блок-схема обобщенного алгоритма нахождения минимального набора контролируемых параметров, распределения их по узлам, и нахождения минимально допустимого времени на контроль каждого параметра.

Выводы к главе 3

Разработан алгоритм формирования оптимального 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. Отличительной особенностью по сравнению с логико-статистическим подходом является включение в методику этапа логической минимизации наборов комбинаций событий, в результате которой достигается минимальное число событий, и как следствие, контролируемых параметров.

Дополнительные возможности предложенного подхода связаны с разработкой процедуры расстановки параметров оптимального пакета контроля по узлам КТС и решением задачи выбора минимального времени, достаточного для контроля инцидентов с заданными показателями эффективности обнаружения, что позволяет повысить производительность системы контроля инцидентов за счет снижения суммарного времени на контроль.

Предложен алгоритм обнаружения инцидента ИБ в КТС, основанный на переборе всех возможных комбинаций событий ИБ, имеющих вид бинарных сигналов и полученных при измерении параметров оптимального пакета контроля. Преимуществом предлагаемого подхода является использование минимального количества анализируемых комбинаций событий, обеспечивающих обнаружение инцидента с вероятностью не хуже заданной.

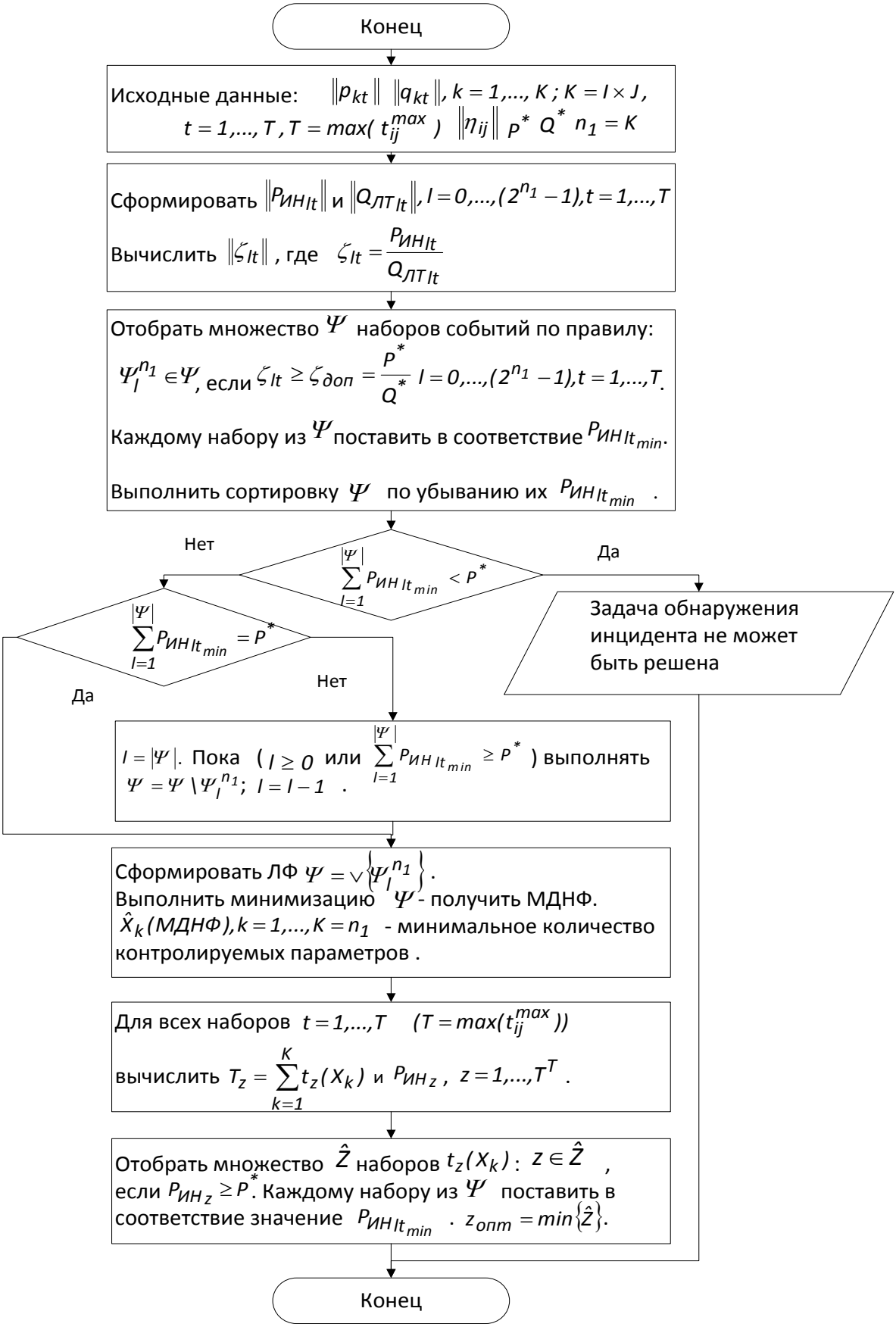


Рисунок 3.1 - Блок-схема алгоритма нахождения минимального набора контролируемых параметров

4 РАЗРАБОТКА И АНАЛИЗ ЭФФЕКТИВНОСТИ СИСТЕМНЫХ СРЕДСТВ КОНТРОЛЯ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОРПОРАТИВНОЙ ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ

Практическая реализация моделей и алгоритмов, предложенных в предыдущих главах, требует системного подхода, то есть рассмотрения предложенных средств в их взаимосвязи, что предопределяет построение системы с выделением подсистем (блоков) с четко ограниченными функциональными свойствами, а также алгоритмизацию системных функций.

В главе предлагается структурная модель системы контроля инцидентов ИБ в КТС (СКИн), описывается алгоритм ее функционирования. Приводятся результаты экспериментов по определению статистических характеристик обнаружения событий ИБ разработанными средствами. Рассматриваются примеры практической реализации функциональных блоков системы контроля.

4.1 Структурная схема системы контроля инцидентов. Порядок функционирования

Структурная схема СКИн представлена на рисунке 4.1. На схеме выделены следующие функциональные блоки:

1. Блок управления измерителями (БУИ). Измеритель – это программный модуль, позволяющий «измерить» значение контролируемого параметра, который, как правило, представляет собой текстовый файл настройки соответствующего средства защиты в узле КТС. Источником параметров в большинстве являются системные средства ОС и программ-приложений. БУИ осуществляет настройку дистрибутивов измерителей в соответствии с определенными параметрами, такими как тип устройства, адрес и т.д., формирует пакет измерителей для конкретного узла с номером, задаваемым из БУ, выставляет сигнал для БУ, что пакет измерителей для узла сформирован. При настройке измерителя под конкретный узел ис-

пользует данные об архитектуре узлов КИТС (из БХПА).

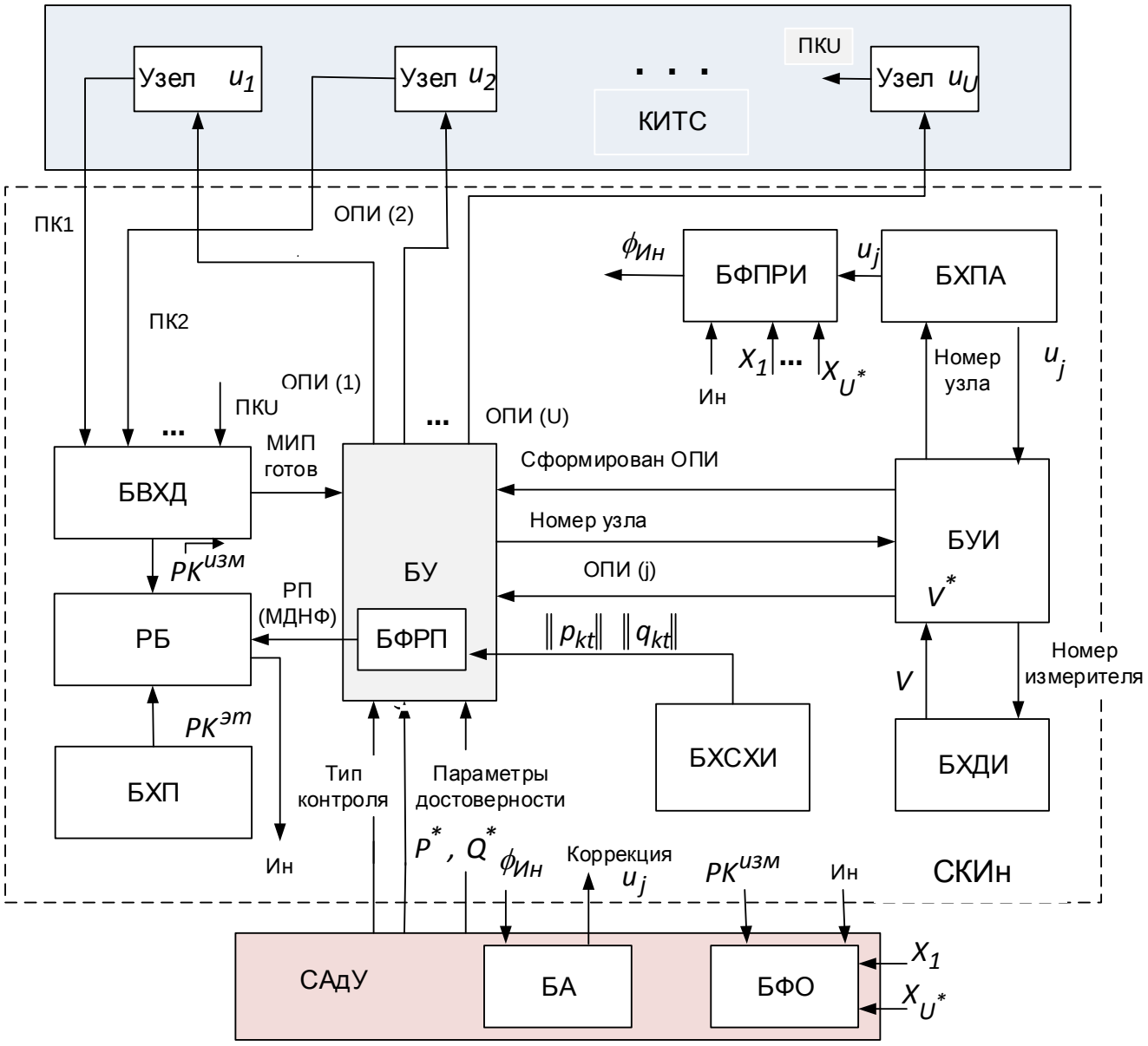


Рисунок 4.1 – Структурная схема системы контроля инцидентов

2. Блок хранения статистических характеристик обнаружения событий ИБ (БХСХИ) – для каждого параметра и каждого узла хранятся массивы вероятностей корректного и «ложного» обнаружения СоИБ.

3. Блок хранения дистрибутивов измерителей (БХДИ) – содержит исходные коды программных модулей, для формирования объектных модулей программ необходима соответствующая компиляция и настройка под операционную среду узла.

4. Блок управления (БУ) – осуществляет координацию работы всех компонентов системы, инициирует запросы на формирование и настройку измерителей, распределяет пакеты с измерителями по сетевым узлам, управляет получением значений контролируемых параметров. В состав БУ включен блок формирования решающего правила (БФРП), который в соответствии с множеством параметров для контроля и статистическими характеристиками обнаружения СоИБ «вычисляет» решающее правило обнаружения инцидента. В состав такого правила в соответствии с алгоритмами главы 3 включен оптимальный набор контролируемых параметров, их расстановка по узлам КТС, задание времени на контроль каждого параметра.

5. Решающий блок (РБ) – формирует массив событий ИБ на основе сравнений значений контролируемых параметров с их эталонными значениями из БХП, вычисляет значение логической функции обнаружения , выставляет сигнал «Инцидент».

6. Блок временного хранения данных (БВХД) - служит хранилищем, которое используется для записи результатов работы измерителей.

7. Блок хранения параметров архитектуры (БХПА) КТС содержит сведения об особенностях операционной среды каждого узла, что позволяет настраивать измерители под конкретные условия применения.

8. Блок формирования программы «решения» инцидента (БФПРИ) служит для автоматизации формирования задания на устранение инцидента и/или его последствий. Под программой «решения» инцидента ИБ понимается автоматизированная процедура формирования объема работ по восстановлению структурно - функциональных компонент «инцидентных» узлов КТС. Выполнение программы позволяет восстановить требования действующей технической политики. Данный блок формирует программу $\phi_{ИН}$ по типу инцидента, событиям ИБ, его составляющих, характеристикам «инцидентных» узлов.

9. Блок администраторов (БА). Задачей БА является исполнение предписаний программы «решения» инцидента. В блоке происходит распределение работ по администраторам (исполнителям) и выполнение этих работ.

10. Блок формирования отчетов (БФО). Задачей БФО является представление в виде документированного отчета сведений о текущем, прошедшем и прогнозируемом состоянии КТС по запросу. При получении запроса (извне) о формировании отчета, БФО отправляет запрос на получение требуемых сведений БАПР. После получения запрошенных данных от БАПР, БФО обрабатывает их и формирует отчет в одной из требуемых форм. Входными данными БФО являются сведения о текущих значениях (последний раз измеренных) параметров инцидентов, событиях ИБ, исполненных и сформированных программах «решения». Выходными данными являются запрошенные сведения о функционировании СКИн в виде документированного отчета.

На схеме обозначены:

$U = \{u_1, ..., u_U\}$ - узлы КТС;

PK - множество контролируемых ПИн;

V - множество дистрибутивов измерителей,

V^* - множество «настроенных» измерителей;

$PK^{изм}$ - множество результатов;

$PK^{эт}$ - «профиль» ТПИБ.

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 $M_{k\min}$ в виде $\left\| t_{ij} \right\|, i = \overline{1, M_{k\min}}; j = \overline{1, U^*}; U^* \le U$ (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 - $\varphi_{ИН}$. (Пример процесса синтеза программы «решения» инцидента приведен в приложении 4). Исполнить программу: передать программу в БА, ждать завершения. Сохранить исполненную программу. Конец алгоритма.

4.2 Особенности практической реализации системы контроля инцидентов

А. Измерители параметров инцидентов (ИПИ) – основные элементы системы контроля. Это программные модули, позволяющие определить значение параметра. ИПИ запускаются на удаленных устройствах (РС, сервер, АСО) и передают на выход результаты работы. Ошибки первого и второго рода при обнаружении событий ИБ обусловлены рядом особенностей, как работы самой программы, так и узла, на котором происходит выполнение программного кода. Из наиболее

значимых, можно выделить следующие:

1. ограничение максимально допустимого времени работы программы;

2. последовательное считывание данных, составляющих значение параметра;

3. ошибки при чтении конфигурационных файлов вследствие изменения прав доступа – отклонений по сути нет, хотя данные параметра изменены;

4. отключение узлов во время работы программы ИПИ;

5. изменение конфигурационных файлов узлов (плановые изменения в ОС) и др.

Исходные коды ИПИ представлены в Приложении 2. Далее приводятся результаты экспериментальной оценки статистических характеристик обнаружения СоИБ по данным, полученным ИПИ.

Основными статистическими характеристиками являются функции вероятности корректного и «ложного» обнаружения события, заданные массивами $\|p_{kt}\|, \|q_{kt}\| \; k = 1,...,K; K = I \times J; t = 1,...,T, T = max(t_{ij}^{max})$. В дальнейшем двойные индексы будем опускать, полагая идентичность РС, серверов и АСО (в рассматриваемой задаче это вполне приемлемо).

Для «снятия» характеристик обнаружения была создана экспериментальная установка (рисунок 4.2). Она состояла из 4 элементов:

1. конечная станция (Компьютер А), работающая в режиме настройки и пересылки ИПИ, а также получения результатов значений параметров;

2. фрагмент телекоммуникационной сети с управляемыми настройками сетевого оборудования (маршрутизатор);

3. конечная станция (Компьютер В), которая работает в режиме получателя ИПИ, выполнения программы измерения параметра и отправки результатов компьютеру А;

4. конечная станция (Компьютер С), которая «нагружает» маршрутизатор, имитируя среднюю загрузку в КТС, а именно: опрашивает маршрутизатор, отправляя эхо-запросы на него.

При работе экспериментальной установки приняты следующие соглашения:

- в процессе измерения используется «чистая» КТС (на систему в это время не проводилось атакующих воздействий, ПО и аппаратные средства элементов функционируют без сбоев и т.п.);

- внешние условия (по отношению к наблюдаемому элементу) не изменяются (например, 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.).

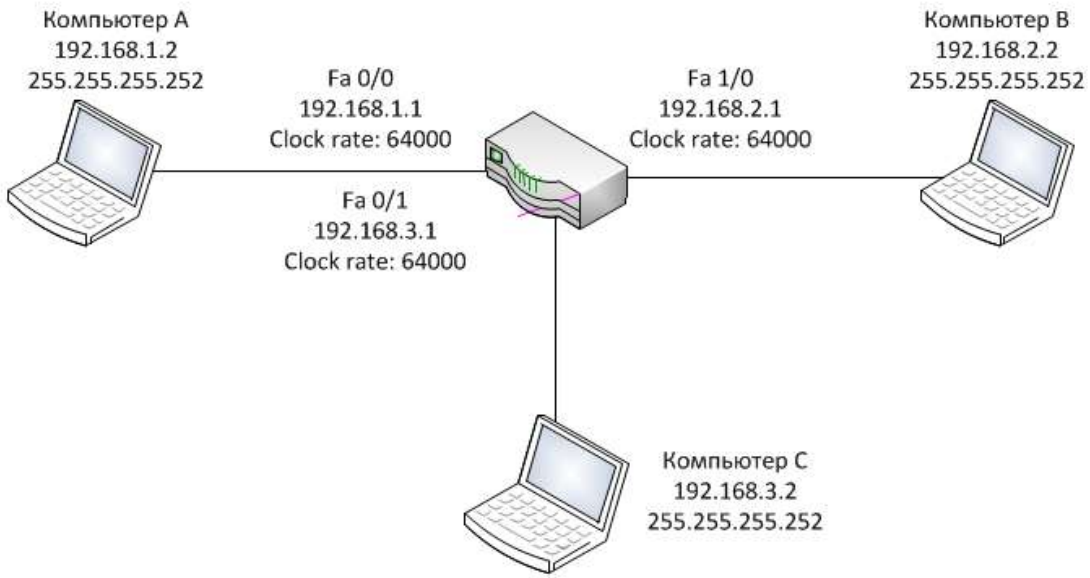


Рисунок 4.2 – Схема экспериментальной установки

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. В таблице 4.1 приведена реализация компонентов экспериментальной установки. Настройки интерфейсов маршрутизатора, компьютеров A, B и C приведены в таблице 4.2.

Таблица 4.1 – Реализация элементов экспериментальной установки

Элемент экспериментальной установки	Функция	Техническая реализация	Программное обеспечение
Компьютер A	Генерация трафика с ИПИ, получение результатов измерения, вычисление событий	Персональный компьютер с сетевым интерфейсом Fast Ethernet	D-ITG (ITGSend.exe), анализатор трафика Wireshark
Маршрутизатор	Передача трафика	Модульный маршрутизатор Cisco	Операционная система IOS
Компьютер B	Прием ИПИ, инициирование его работы, формирование пакета с результатами	Персональный компьютер с сетевым интерфейсом Fast Ethernet	D-ITG (ITGRecv.exe, ITGDec.exe), анализатор трафика Wireshark
Компьютер C	Опрос маршрутизатора путем отправка эхо-запросов	Персональный компьютер с сетевым интерфейсом Fast Ethernet	Утилита Ping

Таблица 4.2 - Настройки интерфейсов маршрутизатора и компьютеров

Устройство	Интерфейс	Параметр	Значение
Маршрутизатор	Fa0/0	IP-адрес	192.168.1.1
Маршрутизатор	Fa0/0	Маска подсети	255.255.255.252
Маршрутизатор	Fa0/0	Частота синхронизации	64000
Маршрутизатор	Fa1/0	IP-адрес	192.168.2.1
Маршрутизатор	Fa1/0	Маска подсети	255.255.255.252
Маршрутизатор	Fa1/0	Частота синхронизации	64000
Маршрутизатор	Fa0/1	IP-адрес	192.168.3.1
Маршрутизатор	Fa0/1	Маска подсети	255.255.255.252
Маршрутизатор	Fa0/1	Частота синхронизации	64000
Компьютер A	Fast Ethernet	IP-адрес	192.168.1.2
Компьютер A	Fast Ethernet	Маска подсети	255.255.255.252
Компьютер A	Fast Ethernet	Шлюз по умолчанию	192.168.1.1
Компьютер B	Fast Ethernet	IP-адрес	192.168.2.2
Компьютер B	Fast Ethernet	Маска подсети	255.255.255.252
Компьютер B	Fast Ethernet	Шлюз по умолчанию	192.168.2.1
Компьютер C	Fast Ethernet	IP-адрес	192.168.3.2
Компьютер C	Fast Ethernet	Маска подсети	255.255.255.252
Компьютер C	Fast Ethernet	Шлюз по умолчанию	192.168.3.1

Эксперимент по формированию массива значений вероятности корректного обнаружения СоИБ за время не более заданного заключался в следующем:

1. В узле А создавался модуль программы – измерителя параметра, кроме того, А хранил эталонное значение параметра;

2. В узле В в настройках источника контролируемого параметра (текстовый файл, используемый либо системными средствами ОС, либо программами-приложениями) случайным образом изменялся один символ. В результате измененный символ находился в разных местах файла. Кроме того, в узле запускались программы-приложения, имитирующие обычную работу рабочей станции;

3. Задавалось время на контроль (в ИПИ). Сначала определялись границы времени обнаружения, далее временные отрезки распределялись равномерно (до 100 интервалов в зависимости от параметра). Из А измеритель отправлялся в В, ожидался ответ. Если за заданное время тайм-аута в А приходил пакет с результатом работы измерителя, то сравнивались измеренное значение с эталонным. В случае несовпадения фиксировалось СоИБ. Если за время тайм-аута ответа не было, результат работы ИПИ считался не корректным.

4. Узел С равномерно «подгружал» маршрутизатор.

5. На каждое значение задаваемого времени контроля процедура обнаружения события осуществлялась 100 раз. Относительная частота обнаружения СоИЮ дает одну точку графика.

Эксперимент по формированию массива значений вероятности «ложного» обнаружения СоИБ за время не более заданного заключался в следующем:

1. В узле А создавался загрузочный модуль программы – измерителя параметра, кроме того, А хранил эталонное значение параметра;

2. В узле В фиксировалась эталонная настройка источника контролируемого параметра, в узле запускались программы-приложения, имитирующие обычную работу рабочей станции;

3. Задавалось время на контроль (в ИПИ). Сначала определялись границы времени обнаружения, далее временные отрезки распределялись равномерно (до

100 интервалов в зависимости от параметра). Из А измеритель отправлялся в В, ожидался ответ. Если за заданное время тайм-аута в А приходил пакет с результатом работы измерителя, то сравнивались измеренное значение с эталонным. В случае несовпадения фиксировалось СоИБ. Если за время тайм-аута ответа не было, результат работы ИПИ считался не корректным.

4. Узел С равномерно «подгружал» маршрутизатор.

5. На каждое значение задаваемого времени контроля процедура обнаружения события осуществлялась 100 раз. Относительная частота обнаружения СоИБ дает одну точку графика.

Экспериментально полученные значения статистических характеристик обнаружения:

- Измерителя №1 параметров «АВЗ не установлена и активирована на шлюзе доступа (HTTP, FTP трафик)», «АВЗ не установлена и активирована на почтовых системах (SMTP/POP3 трафик)», «АВЗ не установлена и активирована на ФС», «АВЗ не установлена и активирована на РС» представлены на рис. 4.3, а. Длительность контроля: $t_{\text{мин}} = 421$ мс, $t_{\text{макс}} = 590$ мс, $t_{\text{ср}} = 505$ мс;

- Измерителя №2 параметра «Имеется доступ к активному сетевому оборудованию не только у системного администратора» представлены на рис. 4.3, б. Длительность контроля: $t_{\text{мин}} = 545$ мс, $t_{\text{макс}} = 1084$ мс, $t_{\text{ср}} = 766$ мс;

- Измерителя №3 параметра «Разрешен доступ к АСО по протоколу SNMP в режиме изменения» (рис. 4.3, в). Длительность контроля: $t_{\text{мин}} = 497$ мс , $t_{\text{макс}} = 814$ мс, $t_{\text{ср}} = 604$ мс);

- Измерителя №4 параметров «Не установлен контроль доступа на границе КИТС для входящих и исходящих данных на сетевом и транспортном уровне» и «Нет аудита контроля доступа по сетевому соединению» (рис. 4.3,г). Длительность контроля:$t_{\text{мин}} = 501$ мс, $t_{\text{макс}} = 755$ мс, $t_{\text{ср}} = 607$мс;

- Измерителя №5 параметра «На РС сетевые конфигурационные параметры не соответствуют шаблону (Политике)» (рис 4.3, д). Длительность контроля: $t_{\text{мин}} = 896$ мс, $t_{\text{макс}} = 1551$ мс, $t_{\text{ср}} = 1256$ мс;

- Измерителя №6 параметра «Учетные записи пользователей не актуальны» (рис. 4.3, е). Длительность контроля: $t_{\text{мин}} = 983$ мс, $t_{\text{макс}} = 2841$ мс, $t_{\text{ср}} = 1831$ мс;

- Измерителя № 7 параметра «Учетная запись не соответствует роли ее владельца» (рис. 4.3, ж). Длительность контроля: $t_{\text{мин}} = 714$ мс, $t_{\text{макс}} = 1401$ мс, $t_{\text{ср}} = 1016$ мс;

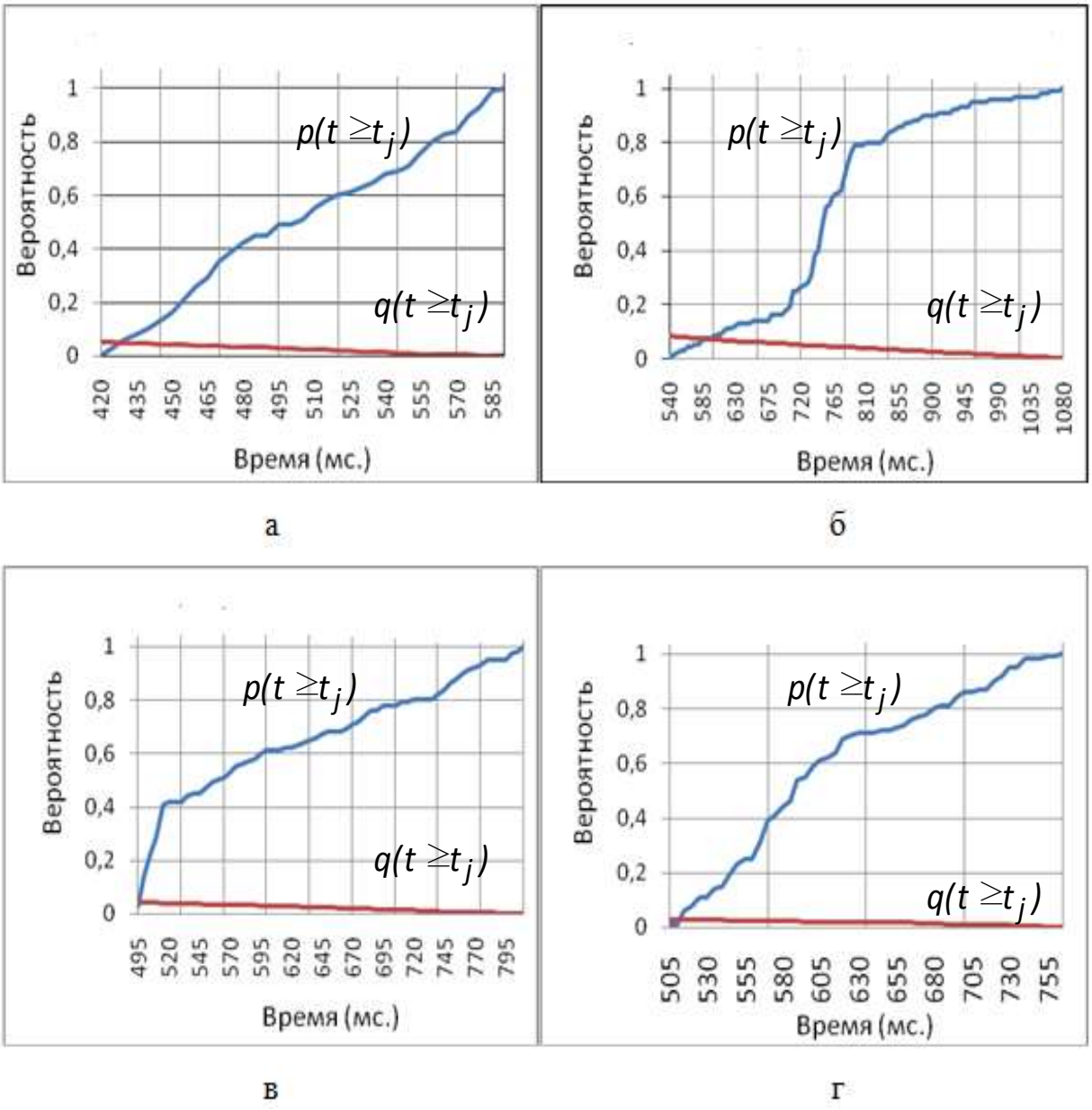
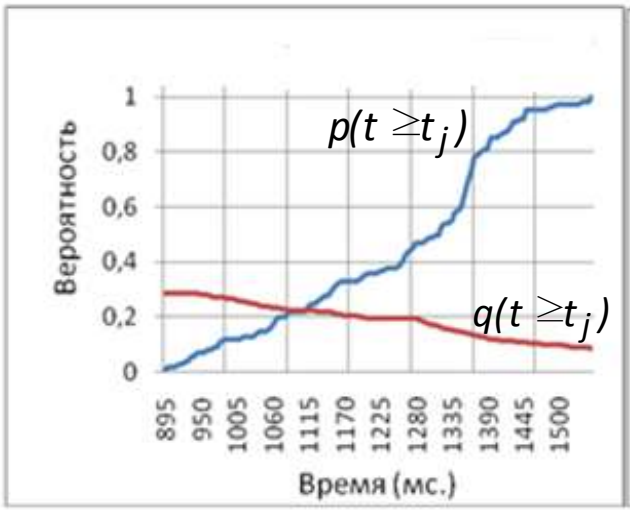
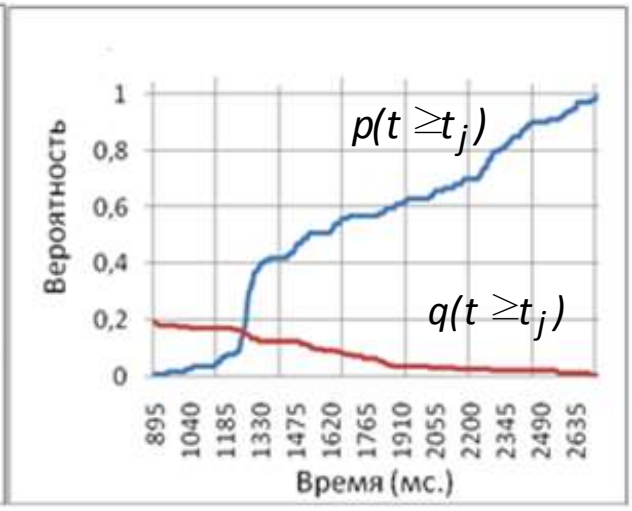


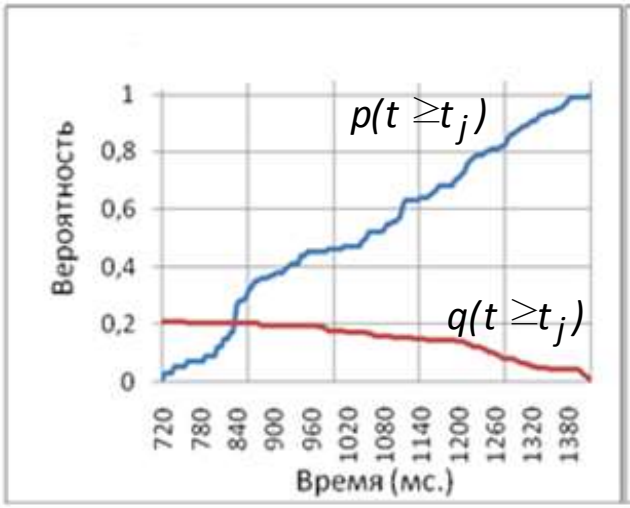
Рисунок 4.3 - Статистические характеристики обнаружения



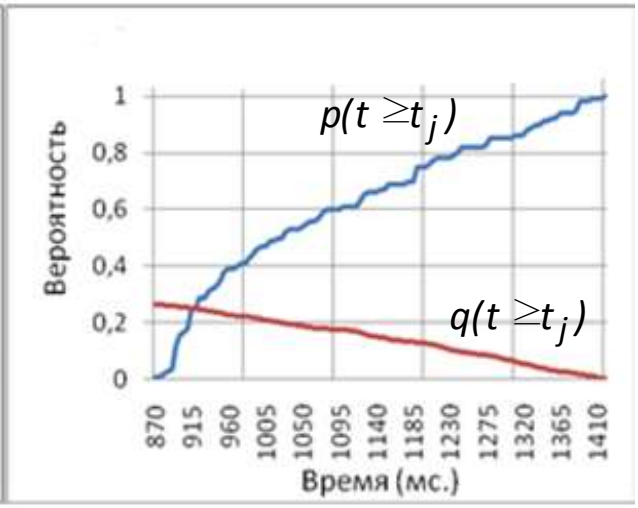
д



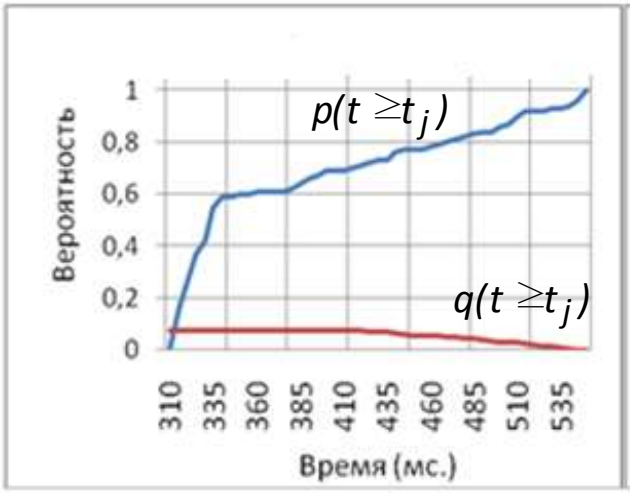
е



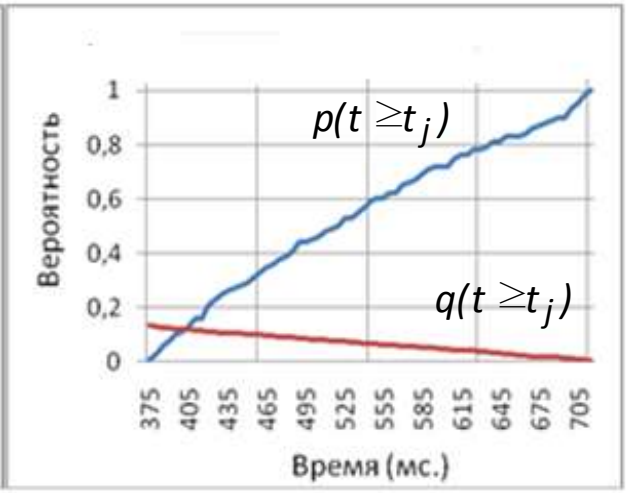
ж



з

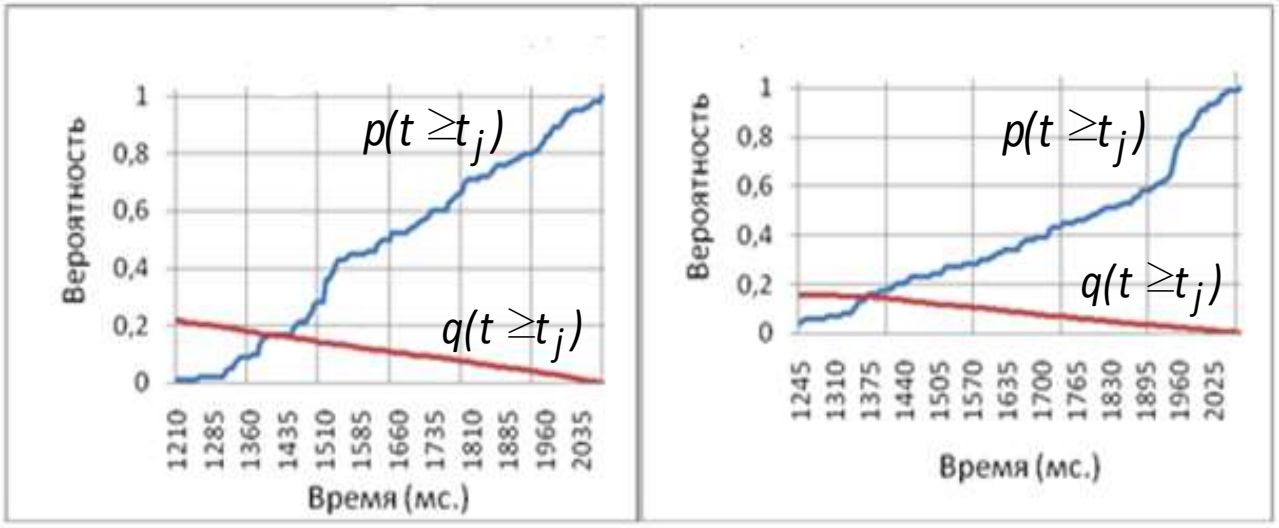


и



к

Рисунок 4.3 (продолжение)



л м

Рисунок 4.3(окончание)

- Измерителя №8 параметра «Учетные записи уволенных сотрудников не блокируются и не удаляются» (рис. 4.3, з). Длительность контроля: $t_{\text{мин}} = 714$ мс, $t_{\text{макс}} = 1401$ мс, $t_{\text{ср}} = 1016$ мс;

- Измерителя №9 параметра «Использование некорректных паролей» (рис. 4.3, и). Длительность контроля: $t_{\text{мин}} = 312$ мс, $t_{\text{макс}} = 744$ мс, $t_{\text{ср}} = 516$ мс;

- Измерителя №10 параметра «Разрешена установка и/или изменение набора ПО на РС пользователям (не только системному администратору)» (рис. 4.3, к). Длительность контроля: $t_{\text{мин}} = 378$ мс, $t_{\text{макс}} = 718$ мс, $t_{\text{ср}} = 533$ мс;

- Измерителя №11 параметров «Не все используемое ПО идентифицировано в реестре разрешенного ПО» и «В РС и/или серверах имеется ПО, сведения о котором не внесены в реестр разрешенного ПО» (рис. 4.3, л). Длительность контроля: $t_{\text{мин}} = 1211$ мс, $t_{\text{макс}} = 2135$ мс, $t_{\text{ср}} = 1719$ мс;

- Измерителя №12 параметра «Изменена аппаратная конфигурация РС» (рис. 4.3, м). Длительность контроля: $t_{\text{мин}} = 1256$ мс, $t_{\text{макс}} = 2126$ мс, $t_{\text{ср}} = 1790$ мс.

Таблица 4.3 содержит сведения об источниках измеряемых параметров, характеристиках обнаружения и особенностях измерения.

Таблица 4.3 – Сводная таблица характеристик измерителей параметров

№ измерителя	Существенные факторы /Параметры	Источник параметра	Характеристики измерителя					Особенности измерителя
			$t_{мин}$	$t_{макс}$	$t_{ср}$	$P(t_{ср})$	$Q(t_{ср})$	
1	Антивирусная защита (АВЗ) не (установлена и активирована) на – шлюзе доступа (HTTP, FTP трафик)	Реестр PC или сервера по путям: [HKEY_LOCAL_MACHINE\ SYSTEM\ CurrentControlSet\ Services; HKEY_LOCAL_MACHINE\System\ CurrentControlSet\Control \GroupOrderList. (команда «gwmi Win32_SystemDriver»).	210	695	496	0,19	0,07	- антивирусной программой и системой должен быть разрешен доступ к конфигурации в реестре; - конфигурация антивируса проверяется только в реестре; - конфигурация реестра может не соответствовать реальной.
	АВЗ не (установлена и активирована) на почтовых системах (SMTP/POP3 трафик)							
	АВЗ не (установлена и активирована) на ФС							
	АВЗ не (установлена и активирована) на PC							
2	Имеется доступ к активному сетевому оборудованию не только у системного администратора	Оперативная память АСО	545	1084	766	0,47	0,046	- конфигурация АСО считывается последовательно (построчно); - обмен данных происходит по telnet протоколу; перед обработкой данные разбиваются на логические единицы.

Продолжение таблицы 4.3

№ измерителя	Существенные факторы /Параметры	Источник параметра	$t_{мин}$	$t_{макс}$	$t_{ср}$	$P(t_{ср})$	$Q(t_{ср})$	Особенности измерителя
			497	814	604	0,61	0,027	- конфигурация АСО считывается последовательно (построчно); - обмен данных происходит по telnetпротоколу; перед обработкой данные разбиваются на логические единицы.
4	Не установлен контроль доступа на границе КИТС для входящих и исходящих данных на сетевом и транспортном уровне Нет аудита контроля доступа по сетевому соединению	Буфер АСО	501	755	607	0,69	0,018	- буфер может быть очищен в любой момент времени и данные будут не достоверны; - обмен данных происходит по telnet протоколу.
5	На РС сетевые конфигурационные параметры не соответствуют шаблону (Политике)	HKEY_LOCAL_MACHINE\ SYSTEM\CurrentControlSet\ Control\Network\	896	1551	1256	0,39	0,19	- решение принимается на основании данных только из реестра; - системой должен быть разрешен доступ к реестру; - данные считываются построчно.

Продолжение таблицы 4.3

№ измерителя	Существенные факторы /Параметры	Источник параметра	$t_{мин}$	$t_{макс}$	$t_{ср}$	$P(t_{ср})$	$Q(t_{ср})$	Особенности измерителя
6	Учетные записи пользователей не актуальны	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList	983	2841	1831	0,6	0,05	- решение принимается на основании данных только из реестра; - системой должен быть разрешен доступ к реестру; - данные считываются построчно; - на принятие решения влияет последовательность считывания пользователей.
7	Учетная запись не соответствует роли ее владельца	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList	714	1410	1016	0,46	0,21	- решение принимается на основании данных только из реестра; - системой должен быть разрешен доступ к реестру; - данные считываются построчно.
8	Учетные записи уволенных сотрудников не блокируются и не удаляются	HKLM\SAM\SAM\Domains\Account\users	714	1401	1016	0,53	0,195	-решение принимается на основании данных только из реестра; - системой должен быть разрешен доступ к реестру; - данные считываются построчно; - на принятие решения влияет последовательность считывания

Окончание таблицы 4.3

№ измерителя	Существенные факторы /Параметры	Источник параметра	$t_{мин}$	$t_{макс}$	$t_{ср}$	$P(t_{ср})$	$Q(t_{ср})$	Особенности измерителя
9	Использование некорректных паролей	C:\Windows\security\database	312	744	516	0,95	0,025	- проверка осуществляется только на основании установленной в системе парольной политики (сами пароли не проверяются)
10	Разрешена установка и/или изменение набора ПО на РС пользователям (не только СисАдм)	HKLM:\Software\Microsoft\Windows\CurrentVersion\ Uninstall	378	718	533	0,55	0,07	- возможна ложная тревога в случае временного изменения прав пользователя, для установки ПО; - данные считываются только из реестра; системой должен быть разрешен доступ к реестру.
11	Не все используемое ПО идентифицировано в реестре разрешенного ПО В РС и/или серверах имеется ПО, сведения о котором не внесены в реестр разрешенного ПО	HKEY_LOCAL_MACHINE\ SOFTWARE\Microsoft\ Windows\ CurrentVersion\ Uninstall	1211	2135	1719	0,65	0,06	- данные считываются построчно; - на принятие решения влияет последовательность считывания; - данные считываются только из реестра; - системой должен быть доступ к реестру.
12	Изменена аппаратная конфигурация РС	HKLM\HARDWARE	1256	2126	1790	0,5	0,049	- системой должен быть разрешен доступ к реестру; - решение принимается на основании данных только из реестра; - считывание данных осуществляется построчно; - на решение влияет последовательность считывания.

Б. Система документированного обеспечения администрирования корпоративной сети передачи данных (СДО КСПД) [49, 56, 59, 73], как средство автоматизации функций предусмотренных БХП, БХПА, БФО СКИн (рис. 4.1), представлена базой данных эталонов узлов КТС, комплектом технической документации и программными модулями, позволяющими автоматизировать процессы документирования ресурсов КТС. Основываясь на правилах [59], были созданы типовые документы, составляющие комплект технической документации на КТС. Комплект технической документации представлен информационно-технической, информационно-графической и организационно-правовой составляющими. Правила составления и типовые формы комплекта технической документации описаны в [49]. Процессы БХП СКИн предусматривают организацию упорядоченного хранения эталонов параметров КТС – базу данных. Автоматизация и визуализация процессов реализовано в программной среде ГИС MapInfo, что позволяет просматривать, добавлять и модифицировать объекты и связанную с ними информацию, выполнять специализированные, в том числе картоориентированные запросы к данным, решать аналитические и прогностические задачи [48, 51, 57]. База данных профиля КТС реализована в среде IBM Lotus Notes. Обработка массивов данных осуществляется в использовании специализированного приложения, реализованного в среде Lotus Domino Designer. Применение системы позволило снизить время выполнения функций администраторами предприятий до 20% за счет снижения времени на поиск информации об элементах КТС и принятие решений по управлению КТС, что подтверждено соответствующими актами (Приложение 3):

Программный комплекс мониторинга состояния элементов КТС CSNM v.1.0 [41, 45, 55] предназначен для автоматизации процессов блоков БХП, БХПА, БФО СКИн (рис. 4.1). База данных CSNM v.1.0 реализована в среде MS SQL Server 2000, бесплатной редакции MSDE-2000 SP-4. Каждый параметр элемента КТС выделяется в отдельный классификатор. С помощью хранимых процедур и триггеров производится анализ, преобразование, хранение и актуализация необходи-

мых данных. Рассматриваемый комплекс может быть масштабирован для применения в крупных распределенных КТС, за счет увеличения количества серверов сообщений (для каждого сегмента сети). В случае нелегитимных изменений программно-аппаратной конфигурации элементов сети, программа АРМ администратора сигнализирует об этом посредством цветовой индикации. Интерфейс программы АРМ администратора представлен на рисунке 4.4.

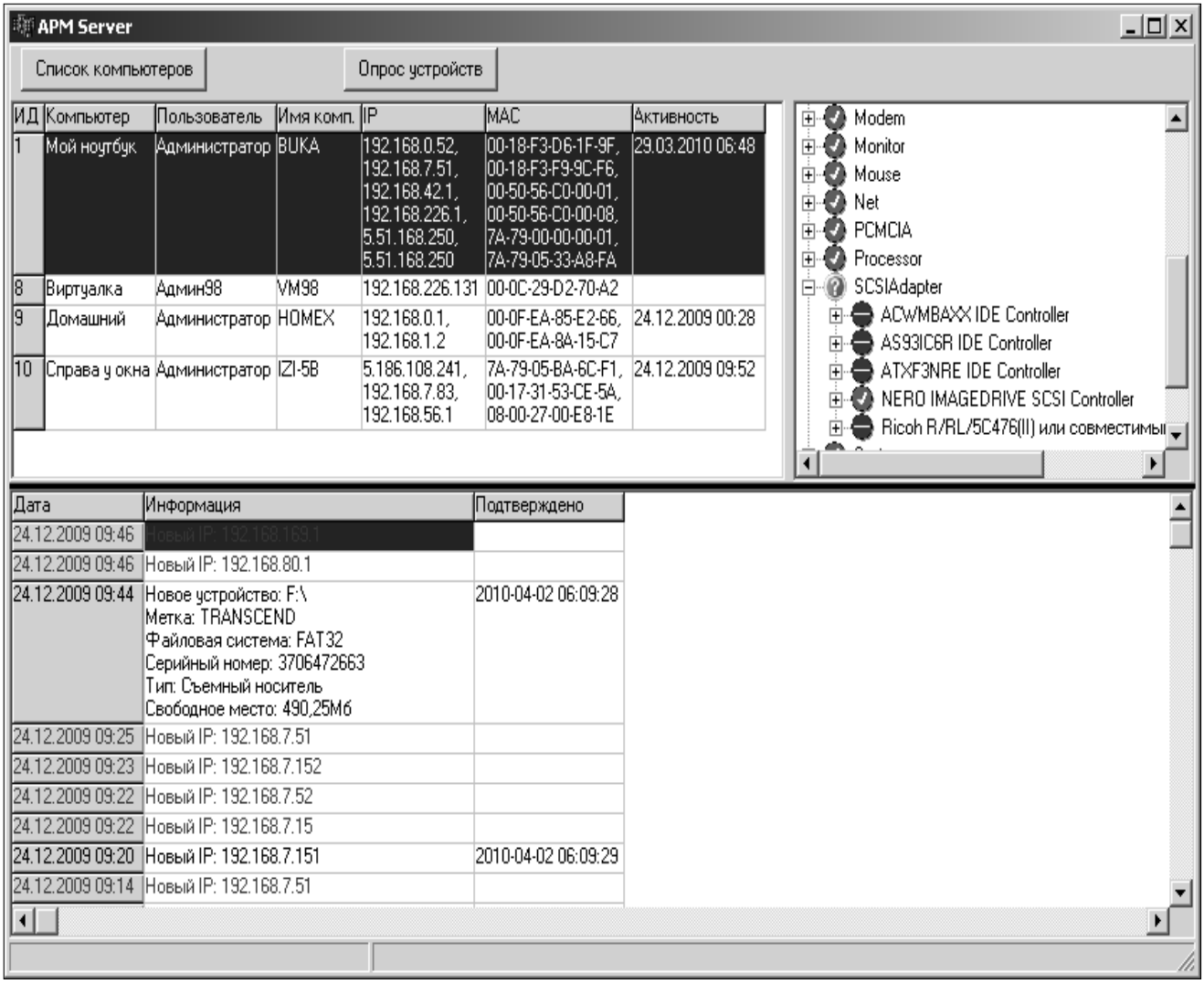


Рисунок 4.4 - Интерфейс АРМ администратора CSNM v.1.0.

С целью обеспечения совместимости при обмене структурированными данными между компонентами комплекса, разработаны протоколы на основе расширяемого языка разметки XML. Для защиты от атак класса Man in the middle

(MitM) служебный трафик шифруется, с применением криптографического алгоритма с открытым ключом RSA.

В. Программный комплекс администрирования корпоративной сети передачи данных DTNAM v1.0 (Data Transmission Network Administrator Manager [90] позволяет автоматизировать процессы, предусмотренные функциональными блоками БА и БАПР (СКИн). В основу DTNAMv.1.0 легли модели и алгоритмы, описанные в [33-35, 40-48, 53, 58, 62, 64-66, 71, 115]. Архитектура системы предполагает три основные группы пользователей: пользователи, администраторы, диспетчер. Обобщенная структура программного комплекса в виде диаграммы развертывания в нотации UML, алгоритмы функционирования каждой из групп пользователей, модель данных БД в виде диаграмм в нотации Баркера описаны в [62, 64, 66, 71]. DTNAM v.0.1 был развернут в сегменте КТС ОАО «Завод «Автоприбор». Период тестовой эксплуатации комплекса составлял 1 месяц, в процессе которого проводились замеры следующих показателей: время ожидания заявки пользователей, обнаруживших проявление инцидента ИБ, на обработку; время выполнения функции устранения инцидента; назначения исполнителя на решения инцидента. Рассматриваемые показатели фиксировались средствами DTNAMv.0.1.

Усредненные показатели периода тестовой эксплуатации комплекса и аналогичные показатели за период предшествующий внедрению представлены в таблице 4.4. Уточним, что исследуемые показатели периода предшествующего периоду тестовой эксплуатации системы были получены из базы данных функционирующей на предприятии системы поддержки пользователей Servise Desk. Минимальное время ожидания заявки пользователей, обнаруживших проявление инцидента ИБ, на обработку в среднем снизилось в 3 раза, максимальное время ожидания заявки - на 16,7%, среднее время - на 33%; минимальное время выполнения функции устранения инцидента не изменилось, максимальное время снизилось до 17%, среднее время снизилось на 25%; снизилось время назначения исполнителя на решения инцидента. Отметим что, период тестовой эксплуатации не достаточно продолжителен, однако наблюдаемое снижение среднего времени по всем по-

казателям позволяет говорить об эффективности применяемых методов.

Таблица 4.4– сравнение исследуемых показателей

Наименование показателя	Минимальное, максимальное и среднее время (мин.)	
	До внедрения	В период внедрения
Время ожидания заявки пользователей, обнаруживших проявление инцидента ИБ, на обработку	6; 12; 8;	2; 10; 6;
Время выполнения функции устранения инцидента	5; 90; 20;	5; 75; 15;
Время назначения исполнителя на решения инцидента	10; 30; 15;	4; 20; 9;

С. Дополнительные программные средства:

- комплекс для расчета значимости элементов корпоративной сети передачи данных [89] позволяющий автоматизировать процесс назначения исполнителей на выполнение работ по восстановлению КТС после обнаружения инцидента ИБ;

- автоматизированная система расчета статических характеристик инцидентов информационной безопасности КСПД АСУП [91], позволяющая автоматизировать процедуры выявления наиболее важных «инцидентных» сетевых узлов;

- программные модули системы поддержки принятия решения административного управления корпоративной АСУ для формирования оптимальной очереди задач администрирования [92], расчета показателей значимости ресурсов программно-технической инфраструктуры [93] и имитационного моделирования процессов администрирования [94], позволяющие администратору безопасности принять оптимальное решение по восстановлению производительности КТС после обнаружения инцидента;

- система анализа защищенности объекта информатизации SaNaS 1.0 [95] и ее база данных [88], позволяющие моделировать разнообразные ситуации с формированием технической политики ИБ (и, соответственно, построения СЗИ).

4.3 Оценка эффективности функционирования системы контроля инцидентов

Время цикла контроля будет рассматриваться как основной показатель эффективности процессов контроля инцидентов в КТС. Составляющие цикла:

1. T_1 – время измерения параметров инцидентов. Для пакета ПК(m_1) определим затраты времени на выполнение действий по измерению каждого параметра $p_i, i \in m_1$ и сопоставлению с эталоном следующим образом. Введем обозначения:

- $t_i^{св}$ - затраты времени на установление связи с источником p_i. Данное время необходимо на взаимное «узнавание» источника и приемника данных и может быть в среднем оценено половиной тайм-аута, отводимого на данную процедуру (заметим, что элемент КТС (например, РС), может в данный момент быть отключен, занят и т.п). Для типовой сети это постоянная величина, равная приблизительно 250 мс;

- $t_i^{зап}$ - затраты времени на установку (настройку) ПО ИПИ «по месту» и его запуск. Здесь, как минимум, необходимо проверить установку необходимых для работы ПО измерителя системных средств);

- $t_i^{изм}$ - затраты времени непосредственно на измерение (задается программой контроля и обеспечивается в обязательном порядке);

- $t_i^{дос}$ - затраты времени на доставку результатов измерения. Здесь включены процедуры установления связи «источник-приемник», ожидание и прием результата от измерителя, а также восстановление работы элемента КТС с контролируемым параметром (удаление ПО измерителя). Данное время в первом приближении может быть оценено половиной тайм-аута, отводимого на соответствующую процедуру (250 мс);

- $t_i^{рез}$ - затраты времени на «сопоставление» результатов измерения пара-

метра, полученного от измерителя, с его эталонным значением.

Суммарное время $t_i^к$, затрачиваемое на контроль одного параметра p_i определим в виде суммы: $t_i^к = t_i^{св} + t_i^{зап} + t_i^{дос} + t_i^{рез}$. Из практических соображений положим: $t_i^{св} = \tau = const$ для всех узлов, $t_i^{зап} << t_i^{изм}$, $t_i^{дос} \approx t_i^{св}$, $t_i^{рез} << t_i^{изм}$. Тогда $t_i^к \approx t_i^{изм} + 2\tau$. Затраты времени на выполнение действий по измерению параметров и сопоставлению с эталоном $T_1 = \sum_{i \in m_1} t_i^к \approx \sum_{i \in m_1} (t_i^{изм} + 2\tau)$.

2. T_2 - время обнаружения инцидента. Это время синтеза по данным измерений логической функции и ее вычисления. Длительностью данного этапа для практической оценки эффективности СКИн можно пренебречь.

3. T_3 - время идентификации инцидента. Данный этап цикла возникает, если проводится тотальный контроль, проверяются все параметры инцидентов на всех узлах. Идентификация проводится по сопоставлению единичных событий с типовым для каждого типа инцидента. Задача чисто вычислительная, не требующая существенных затрат времени (по сравнению с T_1).

4. T_4 - время формирования программы «решения» инцидента. Данное время состоит из «идентификации» параметров «инцидентных» узлов и решения задачи назначения работ по приведению характеристик «инцидентных» узлов профилю Политики. Данная вычислительная задача не трудоемка, и длительностью этапа можно пренебречь.

5. T_5 - время выполнения программы «решения» инцидента. Пусть определены события ИБ - $X_i, i \in m_1$. Все компоненты, параметры которых не соответствуют Политике ($X_i \neq 0$), должны быть «восстановлены». Прогнозируемое время $\tilde{t}_{ia}, i \in m_1, a \in A$ выполнения функции восстановления значения i – го параметра a - м исполнителем (системным администратором), в общем случае, зависит от типа «инцидентного» узла $\tilde{u}_j$, вида работы pk_i, «назначения» γ_{ia} исполнителя

на работу и профессиональных качеств (компетентности k_{ia}) исполнителя: $\tilde{t}_{ia} = f(\tilde{u}_j, k_{ia}, \gamma_{ia}, pk_i)$, f - функционал.

Компетенция – интегральный показатель, отражающий уровень знаний, умений и опыта исполнителя работ [67]. В простейшем случае за значение k_{ia} примем вероятность выполнения функции за время, не превышающее нормативное время $t_i^н$: $k_{ia} = p(t_{ia} \le t_i^н)$. Значения k_{ia} используются для решения оптимизационных задач назначения исполнителей на работы [48, 61, 71]. Суммарное время выполнения программы «решения» инцидента T_5 зависит от общего количества исполнителей (если число исполнителей меньше количества работ, то создаются «очереди» работ). Если имеется достаточное количество исполнителей, и допускается параллельное (одновременное) исполнение, то T_5 определяется самой трудоемкой работой: $T_5 = max(\tilde{t}_{ia})$. Если исполнитель один, то $T_5 = \sum_{i \in m_1} \tilde{t}_{ia}$.

6. T_6 - время завершения инцидента. Завершается инцидент формированием отчета и запоминанием успешно реализованной программы решения инцидента. Отчет формируется из готовых форм. Длительность данного этапа (по крайней мере, в реализованных системах [41, 45, 55]) незначительна по сравнению с T_1 и T_5. Таким образом, $T_ц \approx T_1 + T_5$.

Замечание. В диссертации рассматриваются в основном средства определения T_1. Поэтому снижение времени цикла контроля будет достигаться, в основном, уменьшением суммарного времени измерения параметров инцидентов.

Рассмотрим пример оценки среднего времени контроля инцидентов для фрагмента КТС Предприятия. Исследуемый фрагмент состоит из шести подсетей, содержащих от 3 до 25 узлов – PC и серверов. Для объединения узлов в рамках подсетей используются 8 коммутаторов. Подсети объединены посредством трех маршрутизаторов, доступ в Интернет обеспечивает пограничный маршрутизатор.

Характеристики сетевых узлов:

- PC (49 единиц) - ОС Windows 7 (64-bit), процессор IntelPentiumG645 (2.9 ГГц), оперативная память DDR 3 (4 Гб, частота 1333 MHz), HDDSATA 500Гб;

- серверы (7 единиц: 1 север-шлюз доступа, 1 почтовый сервер, 5 файловых сервера (они же серверы корпоративных приложений) – все HewlettPackard (HP) 385841-421 DL320G3 P3.0-2MB 1GBA80 VPN (P4-3.0Ghz 2Mb/ 1x1024mb /SATARAID 80GbHDD / CD / 2x10/100/1000NIC/ISA);

- коммутаторы (8 единиц) - Cisco Catalyst 2960 Series Intelligent Ethernet Switch (24 порта, 10/100 Fast Ethernet и 10/100/1000 Gigabit Ethernet);

- маршрутизаторы (4 единицы) - Cisco 2911/K9, Ethernet 10Base-T/100Base-TX/1000Base-T.

Характеристики измерителей в данной сети (режим обнаружения события с вероятностью равной 1) сведены в таблицу 4.5.

Вычислим время контроля:

- для маршрутизаторов. Пограничный маршрутизатор (контролируемые параметры 7 и 8). Общее время контроля параметров пограничного маршрутизатора $755 + 500 = 1255мс$ (оба параметра измеряются одним измерителем). Остальные маршрутизаторы (3 единицы, параметры 5 и 6). Общее время контроля $(1084 + 814 + 500) \times 3 = 7194мс \approx 0.1мин$.

Общее время контроля $686 + 23.3 + 19.2 + 7.2 = 735.7с \approx 12.3мин.$

Нетрудно видеть, что основной вклад в общее время контроля вносит измерение параметров рабочих станций. Например, в сети, в которой на каждые 15 компьютеров выделен 1 коммутатор, на три коммутатора выделен 1 маршрутизатор (маршрутизатор имеет один резервный порт), время контроля при 100 рабочих станциях ≈ 24.1 мин, для 200 PC ≈47.9 мин, для 500 PC ≈ 1.9 час, для 1000 ≈ 4 час.

Таблица 4.5 - Характеристики измерителей анализируемой сети

№ параметра	Параметр	Компонент сети контроля	Время обнаружения события (мс)
1	Антивирусная защита (АВЗ) не установлена и активирована на – шлюзе доступа (HTTP, FTP трафик)	Сервер доступа	695
2	АВЗ не установлена и активирована на почтовых системах (SMTP/POP3 трафик)	Почтовый сервер	695
3	АВЗ не установлена и активирована на ФС	Все файловые серверы	695
4	АВЗ не установлена и активирована на РС	Все РС	695
5	Имеется доступ к активному сетевому оборудованию не только у системного администратора	Все маршрутизаторы (без пограничного) и коммутаторы	1084
6	Разрешен доступ к АСО по протоколу SNMP в режиме изменения	Все маршрутизаторы (без пограничного) и коммутаторы	814
7	Не установлен контроль доступа на границе КИТС для входящих и исходящих данных на сетевом и транспортном уровне	Пограничный маршрутизатор	755
8	Нет аудита контроля доступа по сетевому соединению	Пограничный маршрутизатор	755
9	На РС сетевые конфигурационные параметры не соответствуют шаблону (Политике)	Все РС	1551
10	Учетные записи пользователей не актуальны	Все РС	2841
11	Учетная запись не соответствует роли ее владельца	Все РС	1410
12	Учетные записи уволенных сотрудников не блокируются и не удаляются	Все РС	1401
13	Использование некорректных паролей	Все РС	744
14	Разрешена установка и/ли изменение набора ПО на РС пользователям (не только СисАдм)	Все РС	718
15	Не все используемое ПО идентифицировано в реестре разрешенного ПО	Все РС	2135
16	В РС или серверах имеется ПО, сведения о котором не внесены в реестр разрешенного ПО	Все РС и все серверы	2135
17	Изменена аппаратная конфигурация РС	Все РС	2126

Конечно, 4 часа на контроль инцидентов – значительное время, за такой промежуток КИТС может прекратить выполнять свою основную функцию. Необ-

ходимы средства повышающие производительность СКИн (в части снижения длительности цикла).

4.4 Повышение производительности системы контроля инцидентов

Повышения производительности СКИн можно достичь двумя путями:

- уменьшением количества контролируемых рабочих станций;
- реализацией способа многопоточности в цикле контроля.

1. Уменьшение количества контролируемых РС.

Инцидент ИБ, как правило, приводит к снижению системной производительности КТС. В [46] рассматривается возможность идентификации сетевого сегмента с «нарушением» системной производительности. «Узнавание» сегмента с инцидентом происходит по сопоставлению маршрутных таблиц маршрутизаторов. Алгоритм обнаружения подсетей с возникшим инцидентом информационной безопасности приведен в приложении 3. В результате контроль ограничивается одним сегментом сети. Как правило, сетевой сегмент содержит 3-4 коммутатора и 12-20 компьютеров, подключенных к каждому коммутатору. Рис. 4.6 иллюстрирует относительное снижение времени контроля при данном подходе.

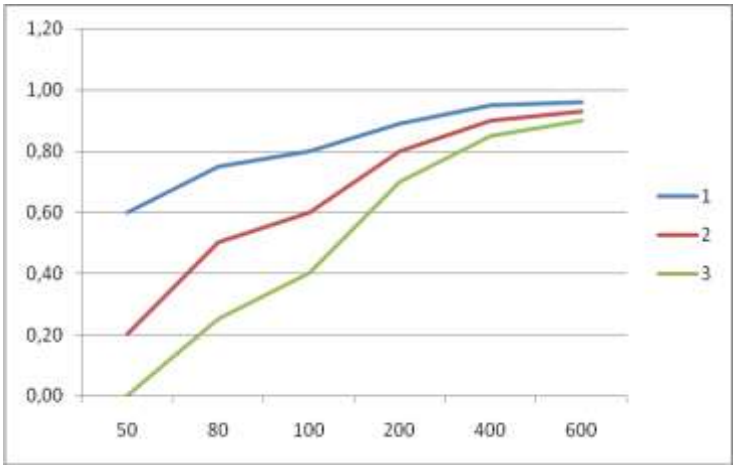


Рисунок 4.6 – Относительное снижение времени контроля (цифрами обозначены «1» -20 РС в сегменте (верхний, синий), «2» – 40 РС (средний, красный), «3» - 60 РС (нижний, зеленый)).

Из графиков видно, что существенное (более 50%) снижение времени контроля наблюдается уже в КТС, имеющей порядка 150-200 РС.

Недостаток данного похода состоит в том, что считается, что инцидент ИБ произошел в одной подсети. При множественных инцидентах выигрыш может быть не столь очевиден.

2. Реализация способа многопоточности в цикле контроля.

Модернизируем «списковый» алгоритм контроля, при котором перед посылкой очередного ОПИ ожидается МИП с предыдущего узла. Изменение алгоритма происходит следующим образом: в очередь посылаются все ОПИ для всех узлов, далее принимаются МИПы от узлов с подготовленными данными, неважно, в каком порядке. Естественно предположить, что к моменту отсылки последнего ОПИ некоторые данные будут уже готовы. Оценить снижение времени контроля при данном подходе достаточно сложно, оно зависит от текущего состояния КТС. Если сеть в данный момент работает с номинальной производительностью, и инцидентов сильно на это влияющих нет, то время контроля будет складываться из длительности передачи всех ОПИ и длительности приема всех МИПов, то есть, по сути, длительностями тайм-аутов.

Здесь есть ограничение. Данные первого узла должны быть готовы сразу после отправки последнего ОПИ.Для примера в предыдущем разделе (49 РС, 7 серверов, 8 коммутаторов и 4 маршрутизатора) длительность отправки всех ОПИ равна $250 \times 49 = 12250мс \approx 12.3с$, а время готовности данных первого узла составляет $250 + 13621 = 13871мс \approx 14с.$ Это означает, что система контроля должна ждать 1.7 с. Общее время контроля ≈40 с, что значительно меньше. Выигрыш больше, если не надо «ждать» результатов. Для нашего примера это достигается, если число РС увеличится минимум до 56.

Дальнейшее снижение времени контроля может быть достигнуто при использовании широковещательного ОПИ, но данный подход применим только при тотальном контроле.

Выводы к главе 4

Предложена структурная модель системы контроля инцидентов ИБ, отличающаяся введением в состав структуры блоков, позволяющих сформировать оптимальные пакеты контроля, учесть архитектуру КТС, варьировать решающие правила обнаружения инцидента, хранить значения параметров, определяемых технической политикой ИБ предприятия.

Разработан алгоритм функционирования системы контроля, обеспечивающий возможности контроля инцидентов а автоматическом режиме, что позволяет сформировать требования к практической реализации систем данного вида.

Предложены подходы к повышению производительности системы контроля, основанные на выделении «инцидентных» подсетей, применении многопоточности в цикле контроля, что в отдельных случаях позволяет значительно снизить время цикла контроля, что особенно ощутимо при полном (тотальном) контроле инцидентов.

Разработано информационное и программное обеспечение системы контроля инцидентов ИБ, включающее программные комплексы документированного обеспечения, мониторинга состояния элементов, 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.

ЗАКЛЮЧЕНИЕ

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.

СПИСОК ПРИНЯТЫХ СОКРАЩЕНИЙ

АБ – администратор безопасности

АВЗ – антивирусная защита

АРМ – автоматизированное рабочее место

АСО - активное сетевое оборудование

БА – блок администраторов

БВХД - блок временного хранения данных системы контроля инцидентов

БУ – блок управления системы контроля инцидентов

БУИ - блок управления измерителями системы контроля инцидентов

БФО - блок формирования отчетов системы контроля инцидентов

БФПРИ - блок формирования программы «решения» инцидента системы контроля инцидентов

БХДИ - блок хранения дистрибутивов измерителей системы контроля инцидентов

БХП - блок хранения профиля системы контроля инцидентов

БХПА - блок хранения параметров архитектуры системы контроля инцидентов

БХСХИ - блок хранения статистических характеристик измерителей системы контроля инцидентов

ВП – вредоносная программа

ЗИ – защита информации

ЗМ – защитная мера

ЗФ – защитная функция

ИБ – информационная безопасность

ИПИ - измеритель параметра инцидентов

ИР – информационные ресурсы

ИС – информационная система

КТС - корпоративная телекоммуникационная сеть

КС - канал связи

КСПД – корпоративная сеть передачи данных

ИнИБ – инцидент ИБ

ПИБ - Политика обеспечения информационной безопасности

ПИн - параметры инцидентов ИБ

ПК – пакет контроля

ПО – программное обеспечение

САдУ – система административного управления

РБ – решающий блок системы контроля инцидентов

РС – рабочая станция

СВТ – средства вычислительной техники

СЗИ – система защиты информации

СКИн - система контроля инцидентов

СоИБ – событие информационной безопасности

ТПИБ – техническая политика обеспечения информационной безопасности

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Александр Бондаренко Политика информационной безопасности. [Электронный ресурс]. – Режим доступа: http://www.leta.ru/press-center/publications/article_295.html (дата обращения:19.02.2015).

2. Артемов, Д.В. Влияние компьютерных вторжений на функционирование вычислительных сетей / Д.В. Артемов. - М: Приор, 2001. - 123 с.

3. Барабаш, О.В. Построение функционально устойчивых распределенных информационных систем / О.В. Барабаш; – Киев: НАОУ, 2004. – 226 с.

4. Баранов, И.Ю. Исследование гибкого инструментального комплекса для интеллектуальной системы административного управления в корпоративных АСУП: дис. … канд. технич. наук: 05.13.06 : защищена 2006 г. / Баранов Игорь Юрьевич. – Орел, 2006.

5. Безруков, Н.Н. Компьютерная вирусология: энциклопедия / Н.Н. Безруков; - Киев: Укр. сов.энцик., 1991. - 416 с.

6. Бекасов, В.Ю. Аспекты анализа структуры корпоративных мультисервисных сетей / В.Ю. Бекасов. - СПб: Питер, 2004. - 208с.

7. Блюмин, С.Л. Модели и методы принятия решений в условиях неопределенности / С.Л. Блюмин, И.А. Шуйкова. - Липецк: ЛЭГИ, 2001. - 138 с.

8. Бойченко, М.К. Мониторинг ресурсов узлов корпоративной сети / М.К. Бойченко, И.П. Иванов. - Приборостроение, №2. – 2010. - С. 114 - 120.

9. Бондаренко, А.Д. Методы и средства разработки интеллектуальных систем управления корпоративными компьютерными сетями: дис. … канд. технич. наук: 05.13.13 : защищена 2007 г. / Бондаренко Алексей Дмитриевич. – Москва, 2007.

10. Бондаренко, А.Д., Проектирование интеллектуальных систем управления компьютерными сетями / А.Д. Бондаренко Ю.Л. Леохин. - Лесной вестник, №2. - 2007. - С. 180 - 186.

11. Бройдо, В.Л. Вычислительные системы, сети и телекоммуникации / В.Л. Бройдо. - СПб.: Питер, 2006. - 703 с.

12. Брэгг, Р., Безопасность сетей: полное руководство / Р. Брэгг, М. Родс-

Оусли, К. Страссберг. - М: Эком, 2006. - 912 с.

13. Воробиенко, П.П. Обобщенная информационная модель взаимодействия систем инфокоммуникаций / П. П. Воробиенко, М. И. Струкало. - Электросвязь. – 2004. – №11.

14. Гатчин, Ю. А. Теория информационной безопасности и методология защиты информации / Ю. А. Гатчин, В. В. Сухостат. - СПб: СПбГУ ИТМО, 2010. - 98 с.

15. Герасименко, В.А. Защита информации в автоматизированных системах обработки данных: В 2-х кн.: Кн. 1. – М.: Энергоатомиздат, 1994. – 400 с.; Кн. 2. – М.: Энергоатомиздат, 1994. - 176 с.

16. Герасименко, В.А., Малюк А.А. Основы защиты информации / В.А. Герасименко, А.А. Малюк. – М.: МОПО, МИФИ, 1997. - 537 с.

17. Голдовский, И.М. Банковские микропроцессорные карты / И.М. Голдовский. — М.: «Альпина Паблишер». - 2010. - 694 с.

18. ГОСТ Р ИСО/МЭК 18044:2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. – М.: Стандартинформ,2009. – 50 с.

19. ГОСТ Р ИСО/МЭК ТО 13335-5-2006. Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети. – М.: Стандартинформ,2006. – 22 с.

20. Гошко, С.В. Энциклопедия по защите от вирусов / С.В. Гошко. - М.: СОЛОН-Р, 2005. - 352 с.

21. Грибунин В.Г. Разработка и реализация политики безопасности предприятия [Электронный ресурс]. – Режим доступа: http://bre.ru/security/22754.html (дата обращения:19.02.2015).

22. Груздева, Л.М. Модели повышения производительности корпоративных телекоммуникационных сетей в условиях воздействия угроз информационной безопасности: дис. … канд. технич. наук: 05.12.13 : защищена 2011 г. / Груздева Людмила Михайловна. – Владимир, 2011.

23. Ден Томашевский Microsoft Windows 8. Руководство пользователя = Microsoft Windows 8. - Вильямс, 2013. - С. 352.

24. Джей Б. Snort 2.1. Обнаружение вторжений. - М.: Бином-пресс, 2006. - 656 с.

25. Домарев, В.В. Безопасность информационных технологий. Методология создания систем защиты / В.В. Домарев. - К.:ООО «ТИД «ДС», 2001. - 688 с.

26. Дэвис, Д. Вычислительные сети и сетевые протоколы / Д. Дэвис, Д. Барбер, У. Прайс. - Москва: Мир, 1982. - 214 с.

27. Запечников, С. В. Информационная безопасность открытых систем. Средства защиты в сетях: Том 2 / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. - М: Горячая линия - Телеком, 2008. - 560 с.

28. Защита информации в телекоммуникационных системах: Учебник / В.Г. Кулаков, А.Б. Андреев, А.В. Заряев и др. – Воронеж: Воронежский институт МВД России, 2002. – 300с.

29. Козлов, Д.А. Энциклопедия компьютерных вирусов: энциклопедия / Д.А. Козлов, А.А. Парандовский, А.К. Парандовский; - М.: Солон-Р, 2001. - 464 с.

30. Компьютерные сети. Принципы, технологии, протоколы / В.Г. Олифер, Н.А. Олифер–СПб. Питер, 2010. – 944 с.

31. КриптоПро CSP с поддержкой Windows 8. [Электронный ресурс]. – Режим доступа: http://www.cryptopro.ru/news/2012/08/kriptopro-csp-s-podderzhkoi-windows-8 (дата обращения:25.01.2016).

32. Кульгин, М.В. Технологии корпоративных сетей: энциклопедия / М.В. Кульгин; - СПб.: Питер, 1999. - 704с.

33. Лучинкин, С.Д. К вопросу о создании автоматизированной системы администрирования инцидентами безопасности телекоммуникационных сетей / С.Д. Лучинкин, М.М.Монахова. - Проблемы эффективности и безопасности функционирования сложных технических и информационных систем: Материалы XXXIII Всероссийской НТК. – Серпухов: Филиал ВА РВСН, 2014. – С. 186 - 189.

34. Лучинкин, С.Д. О функциях администратора безопасности АИС предприятия / М.Ю. Монахов, Д.В. Мишин, М.М. Монахова. - Проблемы эффективности и безопасности функционирования сложных технических и информационных систем: Материалы XXXIII Всероссийской НТК. – Серпухов:

Филиал ВА РВСН, 2014. – с. 201-204.

35. Лучинкин, С.Д. Решение задачи эффективной загрузки персонала технической поддержки при обслуживании телекоммуникационных систем / И.И. Семенова, Д.В. Мишин, М.М. Монахова. - Материалы VI Международной НТК «Инженерные системы» . – М: РУДН, 2014. – С. 274-280.

36. Лысков, О.Э. Автоматизация поддержки процесса обеспечения работоспособности вычислительной сети предприятия: дис. … канд. технич. наук: 05.13.06 : защищена 2008 г. / Лысков Олег Эдуардович. – Орел, 2008.

37. Марат Давлетханов. Обзор Security Studio Endpoint Protection (ч. 1 и ч.2). [Электронный ресурс]. – Режим доступа: http://www.anti-malware.ru/reviews/security_studio_endpoint_rotection_part1 и http://www.anti-malware.ru/reviews/security_code_endpoint_protection_part2 (дата обращения:25.01.2016)

38. Милославская, Н.Г. Управление рисками информационной безопасности: Уч. пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. - «Горячая линия – Телеком», 2014. – 130 с.

39. Михайлов, А.В. Модели и алгоритмы повышения живучести распределенных информационно-вычислительных систем АСУП: дис. … канд. технич. наук: 05.13.06 : защищена 2007 г. / Михайлов Андрей Витальевич. – Владимир, 2007.

40. Мишин, Д.В. О дополнениях к методике расчета значимости элементов корпоративной сети передачи данных / Д.В. Мишин, И.Ю. Богомазова, А.В. Андреев, М.М. Монахова. - Современные научные исследования. Выпуск 1. - Концепт. - 2013. - URL: http://e-koncept.ru/article/689/ (дата обращения:25.01.2016).

41. 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.

42. Монахова, М.М. Исследование алгоритмов повышения функциональной живучести АСУП в среде имитационного моделирования AnyLogic / Мишин

Д.В., М.М. Монахова // Труды XXX Всероссийской НТК «Проблемы эффективности и безопасности функционирования сложных технических и информационных систем». Часть IV. - Серпуховской ВИ РВ. - 2011. - С. 175-177.

43. Монахова, М.М. Математическая модель приоритетов функциональных элементов корпоративных сетей передачи данных / Д.В. Мишин, М.М. Монахова // Тезиси доповідей XIX міжнародноі науково-практичноі конференціі «Інформаційні технологіі: наука, техніка, технологія, освіта, здоров'я». 2011, НТУ ХПІ. - С.56-57.

44. Монахова, М.М. Модели и алгоритмы администрирования корпоративных сетей передачи данных / Д.В. Мишин, М.М. Монахова //Труды XXIX Всероссийской НТК «Проблемы эффективности и безопасности функционирования сложных технических и информационных систем». - Серпуховской ВИ РВ. - 2010. - С. 165-170.

45. 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.

46. 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

47. Мишин, Д.В. Модель администратора корпоративной сети передачи данных / Д.В. Мишин, М.М. Монахова. – Сборник трудов XII Санкт-Петербургской Международной конференция «Региональная информатика (РИ-2010)». 2010, - СПб. - С.55 - 56.

48. Мишин, Д.В. Проблемы оптимизации распределения работ администраторов как основных исполнительных субъектов в рамках решения целевой задачи администрирования КСПД / Д.В. Мишин, М.М. Монахова. – Материалы III Международной научно-практической конференции «Современные информационные технологии в образовательном процессе и научных исследованиях». 2010. -

Изд-во ГОУ ВПО «ШГПУ». - С. 91 - 95.

49. 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.

50. Мишин, Д.В. Современные подходы к автоматизации администрирования корпоративных сетей передачи данных / / Д.В. Мишин, М.М. Монахова. – Материалы III Международной научно-практической конференции «Современные информационные технологии в образовательном процессе и научных исследованиях». 2010. - Изд-во ГОУ ВПО «ШГПУ». - С. 88-91.

51. Монахова, М.М. Имитационное исследование алгоритмов оптимизации административных ресурсов КСПД / Д.В. Мишин, М.М. Монахова // Тезиси XI міжнародноі науково-технічноі конференціі «Проблеми інформатики і моделювання». - Харків-Ялта. - НТУ ХПІ, 2011. - С. 56.

52. Монахова, М.М. Математическая модель автоматизированной системы обеспечения живучести АСУП / Д.В. Мишин, М.М. Монахова. - Труды научно-практической конференции «Математика и математическое моделирование». 2011. - Мордовский государственный педагогический институт имени М.Е. Евсевьева. – Саранск, 2011.

53. 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.

54. Монахова, М.М. О проблеме оптимизации администрирования корпоративных сетей передачи данных / Д.В. Мишин, М.М. Монахова // Сборник материалов II Международной молодежной научно-практической школы «Информационный менеджмент социально-экономических и технических систем». 2011. – Владимир : Транзит-ИКС, 2011. – С.209-212.

55. Монахова, М.М. Имитационное исследование алгоритмов оптимизации административных ресурсов КСПД / Д.В. Мишин, М.М. Монахова // Тезиси XI міжнародноі науково-технічноі конференціі «Проблеми інформатики і моделю-

вання». - Харків-Ялта. - НТУ ХПІ, 2011. - С. 84.

56. 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.

57. Монахова, М.М. Решение задачи эффективной загрузки персонала технической поддержки при обслуживании телекоммуникационных систем / Д.В. Мишин, М.М. Монахова, И.И. Семенова, С.Д. Лучинкин Труды VI Международной научно-практической конференции «Инженерные системы - 2013». - М.: Изд-во РУДН, 2013. - С.274-280.

58. Мишин, Д.В. Модели и алгоритмы административного управления корпоративной распределенной информационно-вычислительной средой АСУ: диссертация кандидата технических наук: 05.13.06 / Д.В. Мишин [Место защиты: Владимир. гос. ун-т] Владимир, 2013. - 218 с.

59. Мишин, Д.В. Новый подход к системе инвентаризации программно-аппаратных ресурсов распределенной информационной системы / Д.В. Мишин; Материалы межвуз. науч.-практ. конф. «Современные проблемы экономического и социального развития России глазами молодежи». - Филиал ВЗФЭИ в г. Владимире. – Владимир, 2009. - С.204-206.

60. Монахова, М.М. Экспериментальное исследование по обнаружению инцидентов информационной безопасности в корпоративных вычислительных сетях на основе исследования характеристик протокола маршрутизации OSPFv2 / М.М. Монахова, Г.В. Путинцев сборник статей по материалам IV международной научно-практической конференции «Современные технологии и технический прогресс: г. Воронеж), 2015.

61. Монахова, М.М. Алгоритм выбора администраторов корпоративной сети передачи данных / Д.В. Мишин, М.М. Монахова // Материалы XVII международной НТК «Информационные системы и технологии». - Н. Новгород. - С. 147-148.

62. Монахова, М.М. Математическая модель приоритетов функциональных элементов корпоративных сетей передачи данных / Д.В. Мишин, М.М. Монахова // Тезиси доповідей XIX міжнародноі науково-практичноі конференціі «Ін-

формаційні технології: наука, техніка, технологія, освіта, здоров'я». 2011, НТУ ХПІ. - С.56-57.

63. Монахова, М.М. Модель администратора корпоративной сети передачи данных / Д.В. Мишин, М.М. Монахова // Труды XII Международной конференции «Региональная информатика». - 2010. - СПб. - СПОИСУ. - С. 55-56.

64. 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.

65. Монахова, М.М. Объектно-ориентированная модель информационной системы администрирования корпоративной сети передачи данных / Д.В. Мишин, М.М. Монахова // Труды XXIII Международной НТК «Математические методы в технике и технологиях». - Смоленск. - 2010. - С. 8-10.

66. Монахова, М.М. Алгоритм ранжирования ресурсов информационной инфраструктуры АСУП при планировании восстановительных работ / М.Ю. Монахов, Д.В. Мишин, М.М. Монахова //Труды X российской НТК «Новые информационные технологии в системах связи и управления». Калуга, «Ноосфера», 2011. - С.585-588.

67. Монахов, М.Ю. Безопасное управление ресурсами в распределенных информационных и телекоммуникационных системах: монография / М.Ю. Монахов Ю.А. Илларионов . - Владимирский гос. ун-т. - Владимир, 2004. - 212 с.

68. Монахов, Ю.М. Модели обнаружения аномального функционирования информационно-вычислительной среды интегрированных АСУ: дис. … канд. технич. наук: 05.13.06: защищена 2009 г. / Монахов Юрий Михайлович. – Владимир, 2009.

69. Монахов, Ю.М. Уязвимости протокола транспортного уровня TCP / Ю.М. Монахов; Алгоритмы, методы и системы обработки данных. Сборник научных статей. - М.: Горячая линия-Телеком, 2006. - с. 203-210.

70. Монахов, Ю.М. Вредоносные программы в компьютерных сетях: учеб. пособие / Ю.М. Монахов, Л.М. Груздева М.Ю. Монахов. - Владим. гос.ун-т. –

Владимир: Изд-во Владим. гос. ун-та, 2010. – 76 с.

71. Монахова, М.М. Модель администратора корпоративной сети передачи данных / М.М. Монахова. - Материалы XV Всероссийской НТК студентов, молодых ученых и специалистов «Новые информационные технологии в научных исследованиях и образовании». - Рязанский государственный радиотехнический университет. 2010. - С. 356 - 357.

72. Мур, М. Телекоммуникации / Мур М., Притск Т., Риггс К., Сауфвик П. - СПб.: БХВ - Петербург, 2005. - 624 с.

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

74. Орлов, А.И. Организационно-экономическое моделирование: учебник в 3ч. / А.И. Орлов. – М.: Изд-во МГТУ им. Н.Э. Баумана. – 2009. Ч. 2 : Экспертные оценки. – 2011. – 486 с.

75. Официальная документация по Ubuntu 12.04 LTS. [Электронный ресурс]. – Режим доступа: http://help.ubuntu.ru/doc/12.04/ (дата обращения: 25.01.2016).

76. Официальный сайт DallasLock. [Электронный ресурс]. – Режим доступа: http://www.dallaslock.ru/ (дата обращения: 25.01.2016).

77. Официальный сайт антивируса AvastPro. [Электронный ресурс]. – Режим доступа: https://www.avast.com/pro-antivirus (дата обращения: 25.01.2016).

78. Официальный сайт антивируса NOD32. [Электронный ресурс]. – Режим доступа: https://www.esetnod32.ru/ (дата обращения: 25.01.2016).

79. Пескова, С.А. Сети и телекоммуникации / Пескова С.А., Кузин А.В., Волков А.Н.. М.: Академия, 2008. - 576 с.

80. Пол Мак-Федрис Microsoft Windows 7. Полное руководство = Microsoft Windows 7 Unleashed. — М.: Вильямс, 2012. — 800 с.

81. Политика информационной безопасности АО «Фонд развития предпринимательства «Даму». [Электронный ресурс]. – Режим доступа:

www.damu.kz/content/files/PolitikaInformatsionnoyBezopasnosti.pdf (дата обращения: 25.01.2016).

82. Политика информационной безопасности АО НК „КазМунайГаз“ [Электронный ресурс]. – Режим доступа: www.kmg.kz/upload/company/Politika_informacionnoi_bezopasnosti.pdf (дата обращения: 25.01.2016).

83. Политика информационной безопасности ЗАО «СМАРТБАНК». [Электронный ресурс]. – Режим доступа: http://smartbank.ru/sites/default/files/documents/politika_informacionnoj_bezopasnosti.pdf (дата обращения: 25.01.2016).

84. Политика информационной безопасности ОАО «Газпромбанк» [Электронный ресурс]. – Режим доступа: www.gazprombank.ru/upload/iblock/ee7/infibez.pdf (дата обращения: 25.01.2016).

85. Политика информационной безопасности ОАО «Радиотехнический институт имени академика А. Л. Минца». [Электронный ресурс]. – Режим доступа: www.rti-mints.ru/uploads/files/static/8/ politika_informacionnoy_ bezopasnosti_rti.pdf (дата обращения: 25.01.2016).

86. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных: Учеб. пособие для вузов / П.Ю. Белкин, О.О. Михальский, А.С. Першаков и др. – М.: Радио и связь, 1999. – 168 с.

87. Руководящие документы по информационной безопасности: [Электронный ресурс]. – Режим доступа: http://securitypolicy.ru/index.php/ (дата обращения: 25.01.2016).

88. Свидетельство о государственной регистрации базы данных №2014620496 от 27 марта 2014г. «База данных автоматизированной системы анализа защищенности объекта информатизации SaNaS 1.0».

89. Свидетельство о государственной регистрации программы для ЭВМ №2012612368 от 5 марта 2012г. «Программный комплекс для расчета значимости элементов корпоративной сети передачи данных» .

90. Свидетельство о государственной регистрации программы для ЭВМ №2012660376 от 9 октября 2012г. «Программный комплекс администрирования корпоративной сети передачи данных DTNAM v1.0».

91. Свидетельство о государственной регистрации программы для ЭВМ №2012660377 от 9 октября 2012г. «Автоматизированная система расчета статических характеристик инцидентов информационной безопасности КСПД АСУП».

92. Свидетельство о государственной регистрации программы для ЭВМ №2013613705 от 15 апреля 2013г. «Программный модуль СППР административного управления корпоративной АСУ для формирования оптимальной очереди задач администрирования».

93. Свидетельство о государственной регистрации программы для ЭВМ №2013613706 от 15 апреля 2013г. «Программный модуль СППР административного управления корпоративной АСУ расчета показателей значимости ресурсов программно-технической инфраструктуры».

94. Свидетельство о государственной регистрации программы для ЭВМ №2016313761 от 6 апреля 2013г. «Программный модуль имитационного моделирования процессов администрирования СППР административного управления корпоративной АСУ».

95. Свидетельство о государственной регистрации программы для ЭВМ №2014610966 от 21 января 2014г. «Автоматизированная система анализа защищенности объекта информатизации SaNaS 1.0».

96. Сергей Петренко, Владимир Курбатов Разработка политики информационной безопасности предприятия. [Электронный ресурс]. – Режим доступа: http://www.nestor.minsk.by/sr/2005/08/sr50803.html (дата обращения: 25.01.2016).

97. Сетевые сканеры, шпионы, снифферы (ИНТЕРНЕТ для Windows): [Электронный ресурс]. – Режим доступа: http://freesoft.ru/?sec=iscan1 (дата обращения: 25.01.2016).

98. Система сетевого управления RADview: [Электронный ресурс]. – Режим доступа:http://www.rad.ru/3-11827/RADview/.

99. Средства анализа и управления сетями / [Электронный ресурс]. URL: http://kafvt.narod.ru/Osia/Glava7.htm (дата обращения: 25.01.2016).

100. Средства шифрования Symantec. [Электронный ресурс]. – Режим доступа: http://www.symantec.com/ru/ru/encryption/ (дата обращения: 25.01.2016).

101. Таненбаум, Э. Компьютерные сети / Э. Таненбаум. - СПб: "Питер". -

2008. - 992 с.

102. Теория и практика обеспечения информационной безопасности / Под ред. П. Д. Зегжды. - М.: «Яхтсмен». -- 1996. - 192 с.

103. Хоффман, Л.Дж. Современные методы защиты информации / Пер. с англ.; Под ред. В.А. Герасименко. - М.: Советское радио, 1980. - 363 с.

104. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер. - М.: Триумф, 2002. - 816 с.

105. Электронные ключи для аутентификации RSA SecurID. [Электронный ресурс]. – Режим доступа: http://www.infobezpeka.com/products/keyforauntification/?view=409 (дата обращения: 25.01.2016).

106. Berk, V. H., Gray, R.S., Bakos, G. Using sensor networks and data fusion for early detection of active worms / V.H. Berk and others; SPIE-The International Society for Optical Engineering, 2003. - Volume 5071. - p. 92-104.

107. Blazek, R.B., Novel, A Approach to Detection of «Denial-of-Service» Attacks via Adaptive Sequential and Batch-Sequential Change-Point Detection Methods / R.B. Blazek and others; - IEEE CS Press, 2001, p. 220–226.

108. Carl, G., Kesidis, G., Brooks, R. R., Rai, S. [Text] / G. Carl and others; Denial-of-Service Attack-Detection Techniques. IEEE Internet Computing, 2006. - vol. 10, № 1. - p. 82-89.

109. Cisco ASA 5505 Adaptive Security Appliance. [Электронный ресурс]. – Режим доступа: http://www.cisco.com/c/en/us/support/security/asa-5505-adaptive-security-appliance/model.html (дата обращения: 25.01.2016).

110. Cisco ASA 5510 Adaptive Security Appliance. [Электронный ресурс]. – Режим доступа: http://www.cisco.com/c/en/us/support/security/asa-5510-adaptive-security-appliance/model.html (дата обращения: 25.01.2016).

111. Cisco Systems, Inc. Программа сетевой академии Cisco CCNA 3 и 4. Вспомогательное руководство = Cisco Networking Academy Program CCNA 3 and 4 Companion Guide. - М.: «Вильямс», 2006. - С. 944.

112. Cisco's Product Documentation Website for Catalyst Switches. [Электронный ресурс]. – Режим доступа: http://www.cisco.com/c/en/us/tech/lan-switching/multi-layer-switching-mls/index.html (дата обращения: 25.01.2016).

113. CMU/SEI-2004-TR-015 Defining incident management processes for CISRT.

114. Cyber Safe Enterprise. [Электронный ресурс]. – Режим доступа: http://cybersafesoft.com/rus/products/enterprise/ (дата обращения: 25.01.2016).

115. D.V. Mishin, M.M. Monakhova About the optimization of the administration corporate area networks of the data transmission under scarce administrative resources // Herald of the National Technical University "KhPI". Subject issue: Information Science and Modelling. - Kharkov: NTU "KhPI". - 2011. - №17. - P. 101 - 108.

116. Enisa Annual Incident Report. - [Электронный ресурс]. – Режим доступа: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2013 (дата обращения: 25.01.2016).

117. Everest Ultimate Edition / [Электронный ресурс]. URL: http://www.securitylab.ru/software/267497.php (дата обращения: 25.01.2016)

118. Everest Ultimate Edition: [Электронный ресурс]. – Режим доступа:http://www.lavalys.com/ (дата обращения: 25.01.2016).

119. Feinstein, L. Statistical Approaches to DDoS Attack Detection and Response / L. Feinstein; - IEEE CS Press, 2003. - vol. 1. - p. 303–314.

120. ISO/IEC 27001:2005. Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования. – 2005. – 54 с.

121. ISO/IEC 27035:2011. Информационные технологии. Метод обеспечения безопасности. Управление случайностями в системе информационной безопасности. – 2011. – 78 с.

122. ISO/IEC TR 18044 Information security incident management.

123. IT-Baseline Protection Manual : [Электронныйресурс]. – Режим доступа: http://www.iss.net (дата обращения: 25.01.2016).

124. Kaspersky Anti-Virus. [Электронный ресурс]. – Режим доступа: http://www.kaspersky.ru/antivirus (дата обращения: 25.01.2016).

125. Krings, A.W., Dror, M. Real-time dispatching: scheduling stability and precedence [Text] / A.W. Krings, M. Dror. - International Journal of Foundations of Computer Science. World Scientific Publishing Co, 1999. - P. 313-327.

126. Lian, F.L., Moyne, J.R., Tilbury, D.M. Performance evaluation of control networks: Ethernet, ControlNet, and DeviceNet / F. L. Lian, J .R. Moyne, D. M. Tilbury. - IEEE Contr.Syst. Mag. vol. 22, no. 1,2001. - p. 66-83.

127. Luchinkin, S.D., Mishin, D.V., Monakhova, M.M. The adapted algorithm of Kun-Mankers in administrative tasks ECM-computing environment [текст] / S.D. Luchinkin and others. -The Strategies of Modern Science Development: Proceedings of the International scientific–practical conference. -Yelm, WA, USA: Science Book Publishing House, 2013. - P. 21-28.

128. M. M. Monakhova, D. V. Mishin, A. V. Andreev The use of the priority model in optimization of corporate data network administrating // 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.

129. M. M. Monakhova, D. V. Mishin, S. D. Luchinkin The adapted algorithm of kun-mankers in adminastrative tasks ecm-computing environment // 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. 21-28.

130. 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.

131. NIST SP 800-61 Computer security incident handling guide.

132. OpenVPN. [Электронный ресурс]. – Режим доступа: https://openvpn.net/(дата обращения: 25.01.2016).

133. Sanchez, Andrew. Technical Support Essentials: Advice to Succeed in Technical Support. — Apress, 2010. - 260 p.

134. SecretNet. [Электронный ресурс]. – Режим доступа: http://www.securitycode.ru/products/secret_net/ (дата обращения: 25.01.2016).

135. Shade You VPN. [Электронный ресурс]. – Режим доступа: https://shadeyouvpn.com/ru/ (дата обращения: 25.01.2016).

136. Spagnoletti, P.; Resca, A. Information Systems Audit and Control Association / Paolo Resca. - CISA. - p. 85. - ISBN 1-933284-15-3.

137. USB-ключи eToken. Электронный ресурс]. – Режим доступа: http://www.aladdin-rd.ru/catalog/etoken/models (дата обращения: 25.01.2016).

138. Zitello, T., Weber, P., Williams, D. HP Open View System [Text]: Administration Handbook / Tammy Zitello, Paul Weber, Deborah Williams. - New Jersy: Pearson Education, Inc., Upper Saddle River, 2004.- 688 p.

Приложение 1. Типовая техническая политика информационной безопасности КТС

Антивирусная защита

1. Антивирусная защита (АВЗ) должна строиться на трех уровнях: уровне защиты сети Интернет – шлюза доступа (HTTP, FTP трафика), уровне защиты почтовых систем (SMTP/POP3 трафика) и уровне защиты файловых серверов и PC.

2. Антивирусное ПО должно быть установлено, настроено и активировано на всех программно-технических средствах.

3. Все возможные каналы поступления ВП в КСПД должны быть защищены средствами АВЗ.

4. Контролю на предмет обнаружения ВП должна подвергаться вся создаваемая и обрабатываемая информация.

5. Должно выполняться централизованное, регулярное обновление всех средств АВЗ.

Сетевое администрирование

6. Все сетевые компоненты КСПД должны быть идентифицированы и учтены в базе данных сетевого администрирования.

7. Доступ и удаленное управление активным сетевым оборудованием (АСО) КСПД разрешено только системному администратору после прохождения аутентификации и авторизации.

8. Не разрешается устанавливать доступ к АСО по протоколу SNMP в режиме изменения.

9. На всех портах АСО КСПД должен быть установлен режим управления доступом к среде.

10. На всех используемых портах АСО должен быть режим STP. Все неиспользуемые порты АСО должны быть отключены.

11. На границе КСПД должен быть установлен контроль доступа в КСПД для входящих и исходящих данных.

12. Сетевое взаимодействие между КСПД и сторонней организацией допускается только через межсетевой экран.

13. На границе межсетевого взаимодействия должен быть установлен контроль доступа на входящие и исходящие данные на сетевом и транспортном уровне.

14. Для контроля доступа по сетевому соединению должен быть установлен аудит. Доступ к журналам аудита имеет системный администратор.

15. Создание виртуальных частных сетей с использованием сети Интернет разрешается только по шифрованному каналу.

16. Весь входящий и исходящий трафик анализируется на наличие ВП и сигнатур известных атак.

17. Взаимодействие по сетевому соединению между узлом связи организации и персоналом, работающим в местах, удаленных от организации допускается только через межсетевой экран. Для данного сервиса выполняются все требования к сетевому соединению «Соединение с однородными областями общего пользования»

18. Пользователь РС не должен иметь возможность изменять сетевые конфигурационные параметры.

Управление доменом

Требования к учетным записям пользователей

19. Учетные записи должны отражать актуальную информацию о пользователе

20. Учетная запись обладает полномочиями, определенными ролью ее владельца

21. В случае увольнения или перевода сотрудника, учетная запись пользователя блокируется и удаляется.

Требования к паролям

22. Запрещается использовать в качестве пароля даты рождения, фразы, которые могут быть легко подобраны методом перебора.

23. Требования к паролю: минимум 6 символов, должен состоять из букв верхнего или нижнего регистра русского или латинского алфавита и цифр, может быть задана частота смены пароля.

Интернет

24. Пользователям запрещается преднамеренное распространение компьютерных вирусов, сетевых червей или другого злонамеренного кода.

25. Запрещается использовать корпоративный доступ к сети Интернет для любой деятельности, не связанной со служебными функциональными обязанностями.

26. Запрещается распространять информацию, отнесенную к коммерческой тайне или содержащую персональные данные сотрудников, на общественных серверах в сети Интернет и в локальной сети института.

Управление ПО

27. Набор и конфигурация ПО РС, установка ПО должно осуществляться сотрудниками отдела автоматизации (информационных технологий), и определяется в соответствии с действующей политикой безопасности.

28. Изменение набора ПО, соответствующего пользователя (или его роли), должно осуществляться администраторами.

29. Все ПО идентифицируется в реестре разрешенного ПО.

30. К использованию в КСПД допускается только ПО, внесенное в реестр разрешенного ПО.

31. Реестр ПО содержит лицензионное ПО и свободно распространяемое ПО, прошедшее проверку на отсутствие вредоносного кода.

Файловый обмен

32. Пользователям запрещается хранение информации «неслужебного» характера в своей папке пользователя.

33. Полный доступ к документам пользователя имеет только сам пользователь.

34. Доступ к документам пользователя в режиме чтения имеет администратор файлового сервера и специалисты службы ИБ.

35. Пользователям запрещается самостоятельно организовывать файловые серверы вне зависимости от способа их реализации.

36. Пользователям запрещается самостоятельно открывать общий доступ к папкам на своем компьютере.

37. Для передачи файлов между собой внутри КСПД пользователи должны использовать только свою папку пользователя, электронную почту.

38. Запрещается применять любые виды шифрования при передаче файлов, как внутри КСПД, так и за ее пределы, кроме лиц, имеющих на это право.

Эксплуатация портативных мобильных устройств

39. Все портативные мобильные устройства должны быть учтены в реестре аппаратного обеспечения. Неконтролируемое подключение портативных мобильных устройств к элементам КСПД запрещено.

40. Портативный ПК приравнивается к РС, и все требования безопасности применяются в полной мере.

Для пользователя

41. Пользователю разрешается выполнять только те действия в КСПД, которые явно разрешены.

42. Всем пользователям запрещается создавать или использовать ПО, модули для ПО, включенного в перечень разрешенного ПО, в том числе составные части ОС, реализующие следующие функции:

- Нарушение работы серверов, РС, САО
- Перехватывание/подмена сетевого трафика
- Получение НСД к серверам, РС, используя уязвимости или недокументированные функции

43. Запрещается преодолевать любые системы защиты

44. Несанкционированное изменение аппаратной конфигурации РС запре-

щено.

Архивирование, резервное копирование и восстановление данных

45. Режим работы файлового архива круглосуточный, время восстановления 4 часа.

46. Полное ежедневное копирование базы данных и хранение в течение 30 дней. 2 раза в год полное копирование и хранение в течение 5 лет.

Приложение 2. Листинги программных модулей измерителей параметров инцидентов

1. Функция получения конфигурации сетевого оборудования

```
public Config GetConfig()
        {
            string data_run = "";
            string data_line = "";
            string logging = "";
            TcpClient client = new TcpClient(ip, port);
            NetworkStream stream = client.GetStream();
            Thread.Sleep(1);
            SendMessage(stream, "test");
            Thread.Sleep(1);
            SendMessage(stream, "en");
            Thread.Sleep(1);
            SendMessage(stream, "test");
            Thread.Sleep(1);
            SendMessage(stream, "terminal length 0");
            Thread.Sleep(1);
            SendMessage(stream, "sh run");
            Thread.Sleep(200);
            data_run = SendMessage(stream, "sh run");
            Thread.Sleep(1);
            SendMessage(stream, "sh log");
            Thread.Sleep(200);
            logging = SendMessage(stream, "sh log");
            Thread.Sleep(1);
            SendMessage(stream, "sh line");
            Thread.Sleep(200);
            data_line = SendMessage(stream, "sh line");
            stream.Close();
            client.Close();
            return (new Config(data_run, data_line, logging));
    }
```

2. Измеритель параметров «АВЗ не установлена, не активизирована на шлюзе HTTP FTP», «АВЗ не установлена, не активизирована на почтовых системах SMTP/POP3», «АВЗ не установлена не активизирована на файловых серверах», «АВЗ не установлена не активизирована на РС»

```
$max_time = 0
$service = get-service
echo "0"
foreach ($i in $service)
{
     if ($i.Name -eq "avast! Antivirus")
     {
```

```
                $status = 1
                echo "1"
                sleep(2)
                if ($i.Status -eq 'Running')
                {
                     $status = 2
                     $device = gwmi Win32_SystemDriver
                     echo "2"
                     foreach ($j in $device)
                     {
                            if ($j.DisplayName -eq "aswStm" -and
$j.State -eq "Running")
                        {
                             $status = 3
                             echo "3"
                             break
                        }}break}}}
```

3. Измеритель параметра «Имеется доступ к активному сетевому оборудованию не только у системного администратора»

```
     public int AsoConfiguration(List<string> really_tokens)
             {
                 if (really_tokens != null && tokensList != null)
                 {
                     double token_number;
                     bool flag;
                     double count = 0;
                     if (really_tokens.Count > tokensList.Count)
                         token_number = really_tokens.Count;
                     else
                         token_number = tokensList.Count;
                     for (int i = 0; i < really_tokens.Count; i++)
                     {
                         flag = false;
                         for (int j = 0; j < tokensList.Count; j++)
                         {
                             if
(really_tokens[i].Equals(tokensList[j]))
                             {
                                 flag = true;
                                 break;
                             }
                         }
                         if (flag)
                             count++;
                     }
                     if((100 / token_number * count).Equals(100))
                     {
                         return 0;
                     }
```

```
                else
                {return 1;}
            }
            else
            {return 0;}
        }
```

4. Измеритель параметра «Не запрещен доступ к АСО по протоколу SNMP в режиме изменения»

```
$max_time = 0
public int SnmpServer()
        {
            if(tokensList != null)
            {
                foreach(string line in tokensList)
                {
                  if(line.IndexOf("snmp-server community")>= 0)
                    {
                        if (line.IndexOf("RW") >= 0)
                            return 1;
                        else
                            return 0;
                    }
                }
            }
            return 0;
        }
```

5. Измеритель параметров «Не установлен контроль доступа на границе КИТС для входящих и исходящих данных на сетевом и транспортном уровне», «Нет аудита контроля доступа по сетевому соединению»

```
public int AccessConfig()
      {
          if (tokensList != null)
          {
              foreach (string line in tokensList)
              {
                  if (line.IndexOf("interface ") >= 0)
                  {
                    if (!(line.LastIndexOf("switchport") >= 0))
                      {
                          return 1;
                      }
                  }}}
return 0;}
```

6. Измеритель параметра «На PC сетевые конфигурационные параметры не соответствуют шаблону»

```
 $max_time = 0
$adapter = gwmi -class Win32_NetworkAdapterConfiguration
foreach ($i in $adapter)
{
     if ($i.IPAddress -ne $null)
     {
          $dgw = "DefaultIPGateway: "+$i.DefaultIPGateway
          $intname = "Description "+$i.Description
          $ip_add = "IP "+$i.IPAddress[0]
          $ip_sub = "Subnet "+$i.IPSubnet[0]
          $mac_add = "MAC "+$i.MacAddress
          $end = "END_INTERFACE"
          $str = $intname+" "+$ip_add+" "+$ip_sub+" "+$mac_add
          echo $str
     }
}
```

7. Измеритель параметра «Учетные записи пользователей не актуальны»

```
$max_time = 0
echo 0
$all_users_info = gwmi Win32_UserAccount
$name_user = @()
foreach($i in $all_users_info){$name_user += $i.SID}
function rise_char_name($text, $len)
{
     $temp = $text
     for($i=0; $i -lt $len; $i += 1)
     {
          $text += $text[$i]
     }
     return $text
}
function getHash($name)
{
     $length = 0
     if ($name[0].Length -gt $name[1].Length)
     {
          $length = $name[0].Length
          $temp = $length - $name[1].Length
          $name[1] = rise_char_name $name[1] $temp
     }
     else
     {
          $length = $name[1].Length
          $temp = $length - $name[0].Length
          $name[0] = rise_char_name $name[0] $temp
     }
```

```
          $temp_hash = @()
          for($i = 0; $i -lt $length; $i += 1)
          {
               $temp_hash += [int] $name[0][$i] -bxor [int]
$name[1][$i]
          }
          return $temp_hash
     }
     $temp_hash = $name_user[0].Replace('-','')
     $temp_hash = $temp_hash.Replace('-','')
     for ($i = 1; $i -lt $name_user.Length; $i += 1)
     {
          $temp = $name_user[$i].Replace('-','')
          $temp = $temp.Replace('S','')

          $temp_hash = getHash($temp_hash,$temp)
          $temp_hash = ([string] $temp_hash).Replace(' ','')
          echo $hash
     }
```

8. Измеритель параметра «Учетная запись не соответствует роли ее владельца»

```
     $user_list = @{"bydos"="";"Администратор"="Администраторы"}
     $mas = ''
     $adsi = [ADSI]"WinNT://$env:COMPUTERNAME"
     $mas = $adsi.Children | where {$_.SchemaClassName -eq 'user'} |
Foreach-Object {
          $groups = $_.Groups() | Foreach-Object
{$_.GetType().InvokeMember("Name", 'GetProperty', $null, $_, $null)}
          $_ | Select-Object
@{n='UserName';e={$_.Name}},@{n='Groups';e={$groups -join ';'}}
     }
     foreach($obj in $mas){
         foreach($user in $user_list){
             if($user.Keys -match $obj.UserName){
                 if($user.Values -match $obj.Groups){
     echo 1
                 }
                 else{
                     echo 0
                 }
             }
         }
     }
```

9. Измеритель параметра «Используются некорректные пароли»

```
     secedit /export /cfg c:\secpol.cfg > null
     echo 1
```

```
secedit /export /cfg c:\old_secpol.cfg > null
echo 1
$file = Get-Content c:\secpol.cfg
$old_file = Get-Content C:\old_secpol.cfg
$c = Compare-Object $file $old_file
foreach($i in $c){
    echo 0
}
```

10. Измеритель я параметра «Разрешена установка или изменение набора ПО на ПК пользователям (не только системному администратору)»

```
$event = Get-SoftRight
foreach($i in $event){
   if($i.EntryType -match 'Change'){
echo 0
    }
    else{echo 1 }
}
```

11. Измеритель параметра «Не все используемое ПО идентифицировано в реестре разрешенного ПО»

```
echo 0
$soft_list = " "
$state = 0
$list = Get-ChildItem
HKLM:\Software\Microsoft\Windows\CurrentVersion\Uninstall |
% {Get-ItemProperty $_.PsPath} |
where {$_.Displayname -and ($_.Displayname -match ".*")} |
sort PSChildName | select PSChildName
foreach($obj in $list){
    if($soft_list -match $obj.DisplayName){
}
    else{
        $state = 1
    }
}
echo $state
```

12. Измеритель параметра «Изменена аппаратная конфигурация PC»

```
$list = “”

$class = 'Win32_Processor', 'Win32_MotherboardDevice',
'Win32_PhysicalMemory', 'Win32_NetworkAdapter'
$nameP = 'Name', 'Caption', 'Manufacturer', 'Level',
'MaxClockSpeed', 'L3CacheSize', 'NumberOfCores',
```

```
'NumberOfLogicalProcessors', 'Name',
'PrimaryBusType','SecondaryBusType', 'SystemName' , 'Name',
'FormFactor', 'PartNumber', 'SerialNumber', 'Speed', 'TotalWidth',
'TypeDetail' , 'DeviceID', 'ServiceName', 'Name' , 'DeviceID',
'ServiceName', 'Name'
    $countN = 8, 4, 7, 3, 3
    $m_hinfo = foreach($i in $class){
        $k = Get-WmiObject -class $i -namespace "root\CIMV2"
        echo $k
    }
    $c = Compare-Object $h_info $m_hinfo
    foreach($j in $c){
        echo 0
    }
```

13. Измеритель параметра «Изменена аппаратная конфигурация серверов»

```
    $list = “”
    $class = 'Win32_Processor', 'Win32_MotherboardDevice',
'Win32_PhysicalMemory', 'Win32_NetworkAdapter'
    $nameP = 'Name', 'Caption', 'Manufacturer', 'Level',
'MaxClockSpeed', 'L3CacheSize', 'NumberOfCores',
'NumberOfLogicalProcessors', 'Name',
'PrimaryBusType','SecondaryBusType', 'SystemName' , 'Name',
'FormFactor', 'PartNumber', 'SerialNumber', 'Speed', 'TotalWidth',
'TypeDetail' , 'DeviceID', 'ServiceName', 'Name' , 'DeviceID',
'ServiceName', 'Name'
    $countN = 8, 4, 7, 3, 3
    $m_hinfo = foreach($i in $class){
        $k = Get-WmiObject -class $i -namespace "root\CIMV2"
        echo $k
    }
    $c = Compare-Object $h_info $m_hinfo
    foreach($j in $c){
        echo 0
    }
```

Приложение 3. Алгоритм обнаружения подсетей с возникшим инцидентом информационной безопасности

Шаг 1. Дана корпоративная телекоммуникационная сеть (рисунок П3.1). Граф сетевого уровня изображен на рисунке П3.2. Заметим, что на графе отсутствуют устройства, не функционирующие на сетевом уровне, такие, как коммутаторы второго уровня (SW1 – SW4). Множество U на графе представляет собой совокупность таких множеств, как R, PK и S (маршрутизаторов, рабочих станций и серверов). Для наглядности все вычислительные сети на графе выделены цветом.

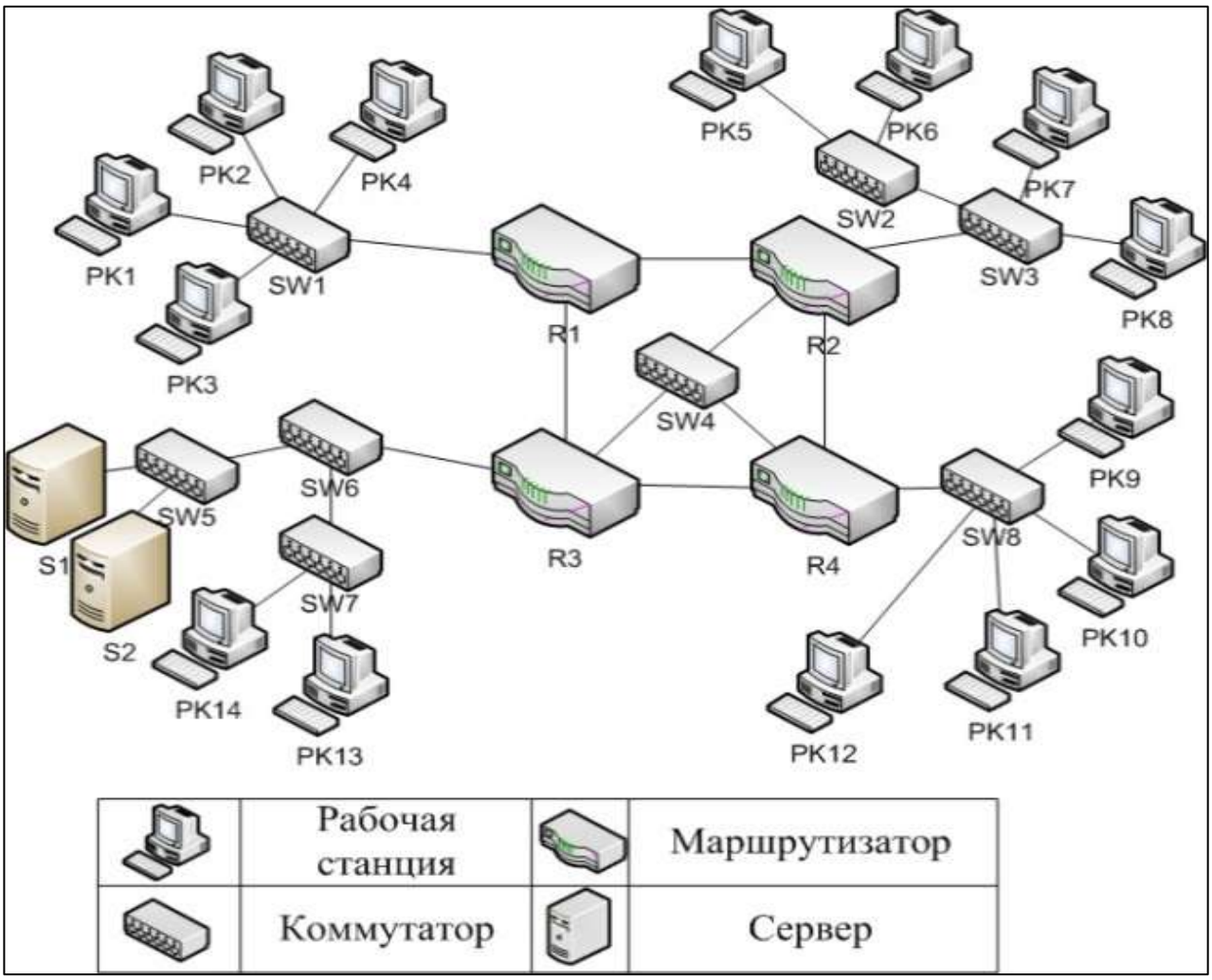


Рисунок П3.1 - Схема КТС

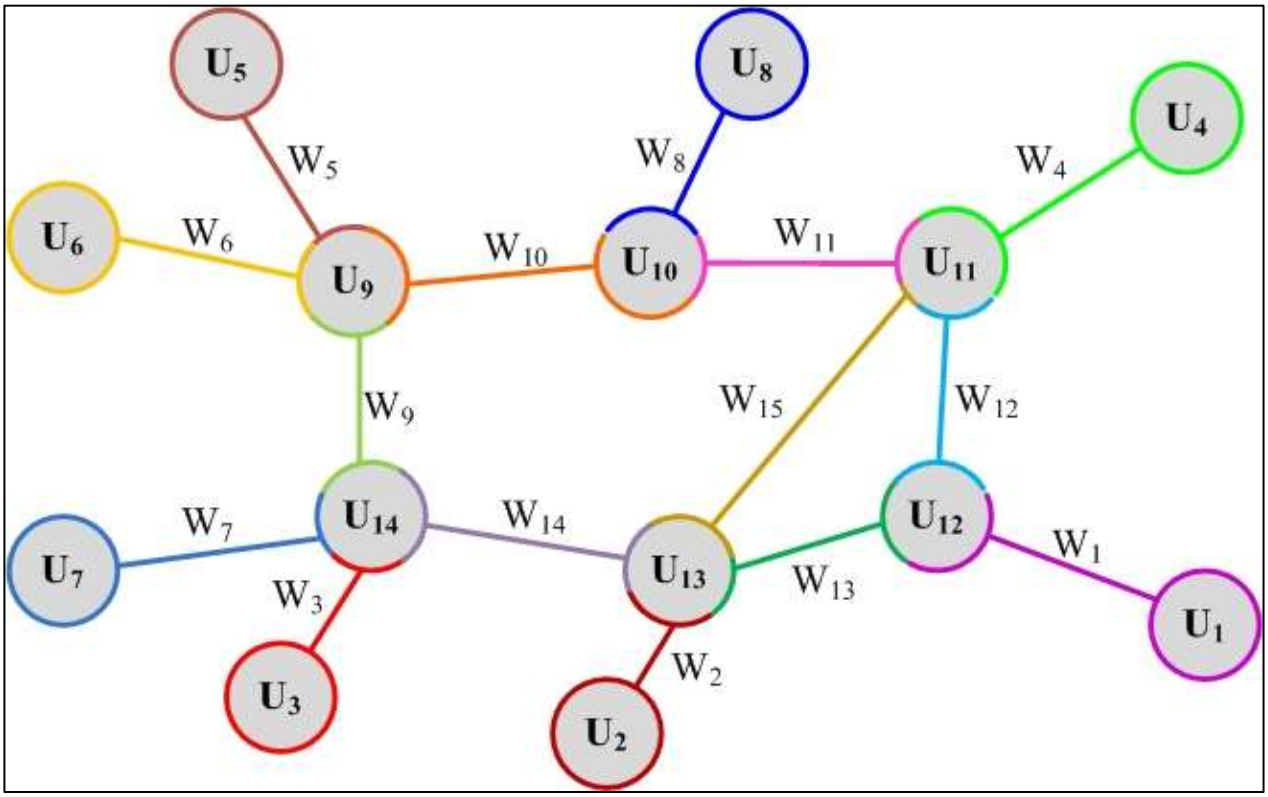


Рисунок П1.2 - Граф сетевого уровня рассматриваемой КТС с выделенными R, РК и S

Строится граф F = (W, H) (рисунок П3.3), где узлами графа W будут являться R, РК и S, а ребрами H – логические соединения между сетями (вне зависимости от маршрута).

Отметим, что граф будет характеризоваться следующими особенностями:

- в большинстве случаев данный граф будет полносвязным, т.к. внутри одной КТС имеется связь всех узлов между собой (если иное не предусмотрено политикой безопасности, такими факторами, как установленный ACL, межсетевой экран и т.д.). В связи с этим было принято построить полносвязный граф, а в случае отсутствия связи между узлами вес ребра принять равным нулю;

- в случае использования различных протоколов маршрутизации, либо разделения внутри протоколов КТС на различные автономные системы, строятся разные матрицы, соответственно и разные графы для каждого протокола/системы;

- на данном шаге примем все веса ребер равными нулю.

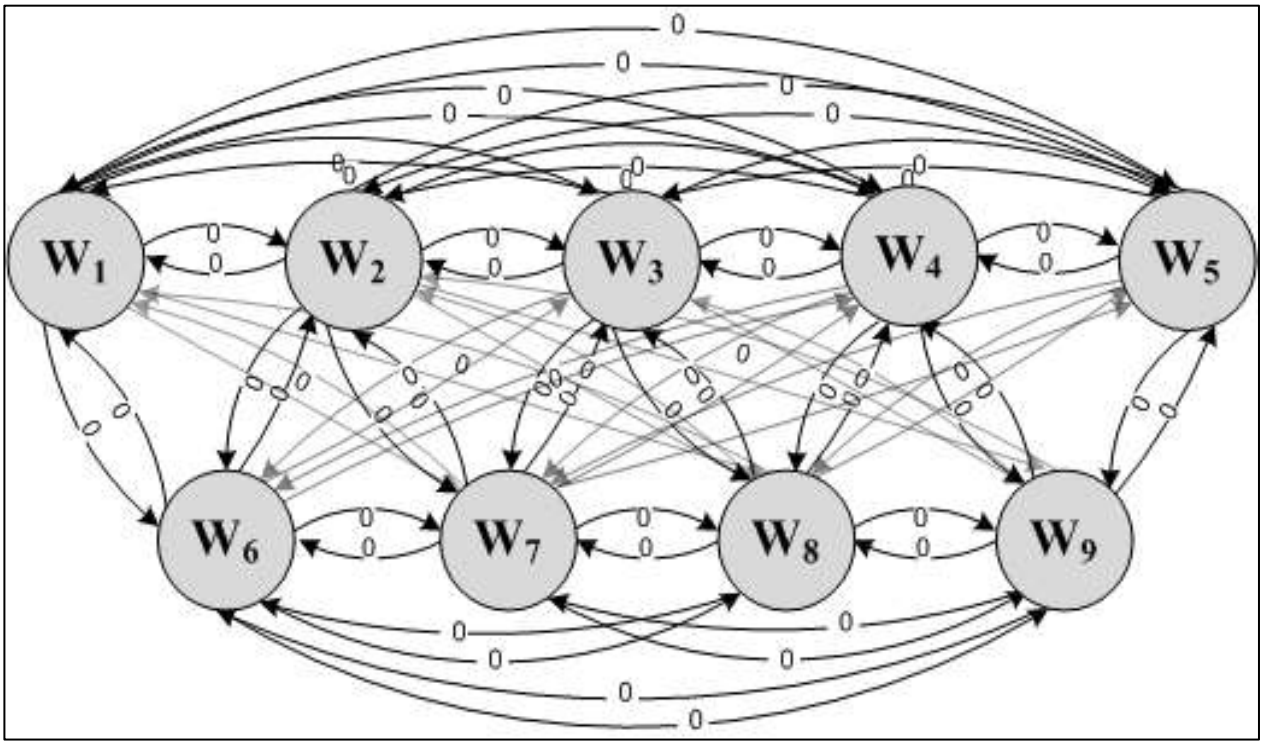


Рисунок П3.3 - Граф межсетевого взаимодействия рассматриваемой КТС

Шаг 2. «Взвесим» ребра ранее построенного графа F, для удобства перейдя от графового представления к матричному. Построим квадратную матрицу M=m*m, где m=|W| (таблица П3.1). По умолчанию все значения в матрице примем равные нулю.

Таблица 1 - Начальный этап построения матрицы M

	W_1	…	W_m
W_1	0	0	0
…	0	0	0
W_m	0	0	0

Шаг 3. Заполним нулевые ячейки. Для расчета метрик воспользуемся формулой расчета метрики того протокола, который функционирует в данной сети. Для самых распространенных протоколов они приведены в таблице П3.2.

Таблица П3.2 - Расчет метрики в протоколах маршрутизации

Протокол	Диапазон	Формула	Примечания
RIPv2	1..15	Число шагов («хопов») до сети назначения	В матрицу метрик заносится минимальное число «хопов», т.е. число шагов по кратчайшему пути до сети назначения
OSPF	1..65535	Сумма стоимостей путей до сети назначения; стоимость равна отношению эталонной пропускной способности к пропускной способности интерфейса	Эталонная пропускная способность может быть изменена, по умолчанию равна 100 Мбит/с
EIGRP	Не ограничен	$[(K_1 \times \text{ПС}) + \frac{K_2 \times \text{ПС}}{256 - \text{Н}} + K_3] \times \left(\frac{3}{10}\right) \times (\frac{K_5}{\text{Нж} + K_4})$	$K_1..K_5$ – коэффициенты значимости параметров. Задаются при конфигурировании; ПС – пропускная способность ПС = (10000000/ПС_i) * 256, где ПС_i – наименьшая пропускная способность всех выходных интерфейсов, входящих в состав маршрута, ведущего к сети назначения; Н – загрузка (наихудший показатель загрузки линка на всем пути, на основании packet rate и настроенной полосе пропускания на интерфейсе); З – суммарная задержка всего пути, З=$З_i$*256, $З_i$ - сумма всех задержек (delays) сконфигурированных на исходящих интерфейсах по пути в сеть назначения в десятках микросекунд; Нж - наихудший показатель надежности на всем пути

Для того, чтобы вычислить значения метрик при помощи измерителя снимем данные (dump-файлы) с маршрутизирующих устройств и подставим их в формулу. Рассчитаем значения и получим матрицу, представленную таблицей П3.3.

Таблица П3.3 - Текущая матрица метрик M

	$\mathbf{W_1}$	…	…	…	…	$\mathbf{W_m}$
$\mathbf{W_1}$	1	X^2_1	1	X^4_1	X^5_1	X^6_1
…	X^1_2	1	X^3_2	1	X^5_2	X^6_2
…	1	X^2_3	1	1	X^5_3	X^6_3
…	X^1_4	1	1	1	X^5_4	X^6_4
…	X^1_5	X^2_5	X^3_5	X^4_5	1	1
$\mathbf{W_m}$	X^1_6	X^2_6	X^3_6	X^4_6	1	1

Здесь, единицей отмечены те сети, которые являются непосредственно подключенными, как стандартное значение метрики «directly connected» (непосредственно присоединенные) в сетевой маршрутизации. Для связей внутри одной сети ($\mathbf{W_1}$-$\mathbf{W_1}$) метрику так же примем равной единице.

В случае, если строится эталонная матрица (измерители снимали данные с настроенной корпоративной сети при отсутствии ошибок в сети и при эмуляции типичной сетевой активности без вмешательства внешних помех), необходимо записать ее в модуль хранения эталонных состояний и вернуться к шагу 1. В противном случае (в случае, если полученная матрица является отображением текущего состояния КТС) необходимо продолжить выполнение алгоритма.

Шаг 4. Выполним сравнение полученной матрицы с эталонной.

Предположим, эталонная матрица ($M_{эт}$) имеет вид (таблица П3.4).

Таблица П3.4 - Эталонная матрица метрик $M_{эт}$

	W_1	…	…	…	…	W_m
W_1	1	Y^2_1	1	Y^4_1	Y^5_1	Y^6_1
…	Y^1_2	1	Y^3_2	1	Y^5_2	Y^6_2
…	1	Y^2_3	1	1	Y^5_3	Y^6_3
…	Y^1_4	1	1	1	Y^5_4	Y^6_4
…	Y^1_5	Y^2_5	Y^3_5	Y^4_5	1	1
W_m	Y^1_6	Y^2_6	Y^3_6	Y^4_6	1	1

Получим итоговую матрицу сравнения (таблица П3.5) L, где L[I,j] = {0,1} следующим образом:

$$\forall M[i,j]\ \exists L[i,j], \begin{cases} L[i,j] = 0 \leftrightarrow M[i,j] \neq Мэт\ [i,j] \\ L[i,j] = 1 \leftrightarrow M[i,j] = Мэт[i,j] \end{cases}$$

Таблица П3.5 - Матрица сравнения L

	W_1	…	…	…	…	W_m
W_1	1	L^2_1	1	L^4_1	L^5_1	L^6_1
…	L^1_2	1	L^3_2	1	L^5_2	L^6_2
…	1	L^2_3	1	1	L^5_3	L^6_3
…	L^1_4	1	1	1	L^5_4	L^6_4
…	L^1_5	L^2_5	L^3_5	L^4_5	1	1
W_m	L^1_6	L^2_6	L^3_6	L^4_6	1	1

Шаг 5. При помощи программ – измерителей «снимаются» с маршрутизирующих устройств необходимые пути передачи данных вида (Ui → Uq→ … → Ur→ Uj) по сети-отправителю и сети-получателю, на пересечении которых L[i,j] = 0. На основании полученной матрицы сравнения выполняется построе-

ние графа G=(U,V), в котором критичные маршруты выделяются цветом. Данные, полученные системой передаются для рассмотрения администратору безопасности. Выполняется переход к шагу 1.

Конец алгоритма.

Реализация данной модели представила модульную программную систему, реализованную в среде Java с использованием модулей, реализованных на языках Python и Bash.

Эксперименты, проведенные с реализованной системой, позволили сделать выводы о том, что за минимальное время методом простейшего сканирования маршрутизирующего оборудования КТС можно обнаружить факты возникновения инцидентов ИБ в сети, и выделить самые критичные зоны воздействия инцидента, и зоны, попавшие в область воздействия.

Время работы программы не составляет более 15 секунд, время обработки данных составляет не более 5 минут. Режим запуска программы в КТС подразумевается 2 раза в 1 час, однако в связи с тем, что программа ведет последовательный опрос оборудования, никакой дополнительной нагрузки на сетевые каналы она не несет, что позволяет выполнять подобное сканирование КТС круглосуточно, получая данные о вероятных инцидентах ИБ по требованию администратора ИБ, либо при выполнении определенных настроек ПО имеет функционал самостоятельно сигнализировать на АРМ администратора ИБ о вероятном инциденте ИБ.

Приложение 4. Алгоритм восстановления производительности КТС после обнаружения инцидента информационной безопасности

Алгоритм назначения на решение инцидентов ИБ, основанный на модели приоритетов, модели администратора КТС и алгоритме нахождения максимального паросочетания Куна – Манкреса.

Методика

Декомпозиция процесса управления инцидентами ИБ КТС позволяет выделить множество F элементарных прецедентов $f \in F$, будем называть их функциями администрирования (ФА). При решении инцидента f назначается на выполнение $a \in A$ - администратору безопасности КТС, здесь под A будем понимать множество сотрудников службы информационной безопасности предприятия, обладающих определенным уровнем квалификации (знаний, умений, навыков в выполнении каждой конкретной ФА).

Математически задачу оптимизации назначения ФА представим в виде двудольного графа $G'=(A',F';Y)$, где $A' \subseteq A$ – подмножество доступных администраторов ИБ КТС, $F' \subseteq F$ – подмножество ФА, требующих выполнения в рамках решения инцидентов ИБ, $Y=\{y_{ij}\}$ – множество ребер двудольного графа, $i = \overline{1,|A'|}$, $j = \overline{1,|F'|}$, $i>0$, $j>0$. Будем считать, что администратор ИБ может быть назначен на выполнение любой ФА, тогда $\beta^{a'}=|F'|$ - коэффициент инцидентности вершины $a' \in A'$, ФА может быть выполнена любым администратором ИБ, $\beta^{f'}=|A'|$, таким образом, $G'=(A',F';Y)$ является полным, $\forall\, a' \in A'$ и $f' \in F'$ $\exists y_{ij} \in Y$.

При решении поставленной задачи необходимо из множества $\beta = \sum_{j=1}^{|F'|} \beta_j^{f'}$ выбрать такое $F' \times A'$, которое наилучшим образом удовлетворяет заданному интегральному критерию эффективности T. Так как каждому $y_{ij} \in Y$ может быть поставлен некоторый показатель эффективности t^*_{ij}, задача оптимизации может быть сведена к классической задаче о назначениях, где интегральным критерием T будем считать суммарное время выполнения ФА в рамках технологического цикла решения инцидента ИБ КТС: $T = \sum_{i=1}^{|A'|} \sum_{j=1}^{|F'|} t^*{}_{ij} \rightarrow min$

Примем в качестве t^*_{ij} прогнозируемое время выполнения $f_j \in F'$ администратором ИБ $a_i \in A'$. Значение t^*_{ij} предлагается рассчитывать на основании индивидуальных профессиональных качеств администратора по формуле: $t^*_{ij} = \bar{t}_{ij} \cdot (1 + e^{\frac{1}{-\Delta d_{ij}}}(1 - K_{ij}))$, где $\bar{t}_{ij}$ – среднее время выполнения f_j администратором a_i; K_{ij} – показатель компетенции a_i по f_j; $\Delta d_{ij} = (d_{ij}^n - d_{ij}^{n-1})$ – интервал между временем последнего выполнения d_{ij}^{n-1} функции f_j администратором a_i и временем d_{ij}^n ее следующего назначения. Значение $\bar{t}_{ij}$ для цикла n будем рассчитывать по формуле: $\overline{t_{ij}} = \frac{\overline{t_{ij}}(n-1)+t_{ij}(n)}{2}$, в случае когда a_i не может исполнять f_j, $\overline{t_{ij}} = \infty$. За значение компетенции примем вероятность выполнения ФА за время не превышающее нормативное, $K_{ij} = p(t_{ij} \le \tilde{t}_j)$, где $\tilde{t}_j$ - норма времени f_j, t_{ij} – время последнего исполнения f_j администратором ИБ a_i.

Алгоритм назначения ФА

Шаг 1. Сформируем матрицу $A'F'$, отражающую бинарное отношение A' и F', каждая упорядоченная пара которого выражена t^*_{ij}:

Шаг 2. Особенность решаемой задачи назначения заключается в том, что за один цикл администрирования будет исполняться некоторое подмножество $F'' \subseteq F'$, соответствующее $|A'|$.

Если $|F'| \le |A'|$ - случай, при котором рассматриваемый цикл последний или решение инцидентов происходит за единственный цикл. Выберем подмножество F"⊂F' для решения, $|F''| = |F'|$. Переход к шагу 3.

Если $|F'| > |A'|$ - случай, при котором решение инцидентов происходит за более чем один цикл и рассматриваемый цикл не последний. Сформируем очередь решения инцидентов, выстроив подмножество F' в соответствии со значениями приоритетов, выберем из очереди $F'' \subset F'$ с наибольшим приоритетом так, чтобы $|F''| = |A'|$. Переход к шагу 3.

Шаг 3. Построим подграф $G''(A';F'';Y)$ двудольного графа $G'(A';F';Y)$ для

цикла исполнения ФА (рисунок П4.1 и П4.2). Переход к шагу 4.

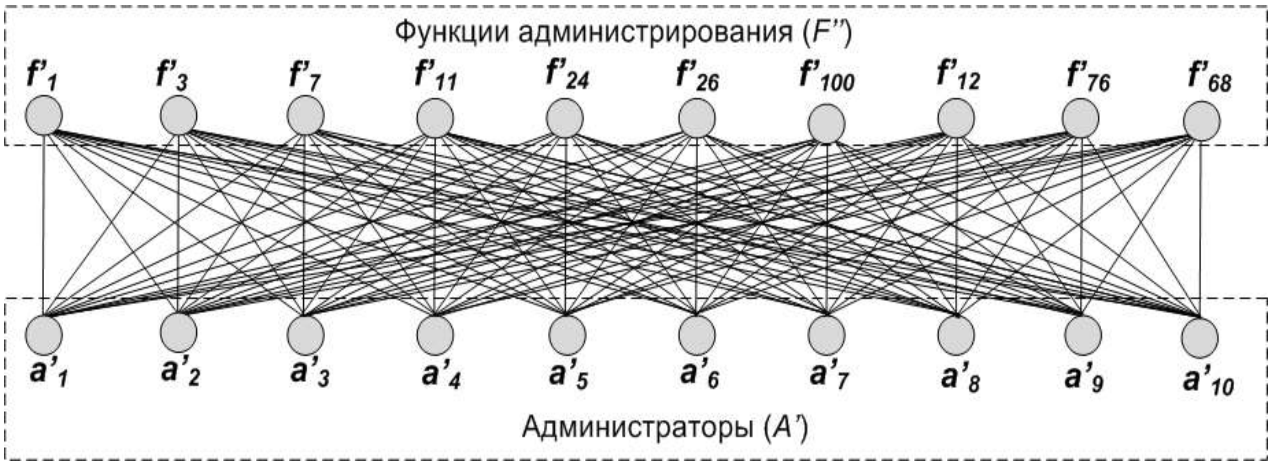


Рисунок П4.1 - Подграф *G''(A';F'';Y), |F''|=|A'|*

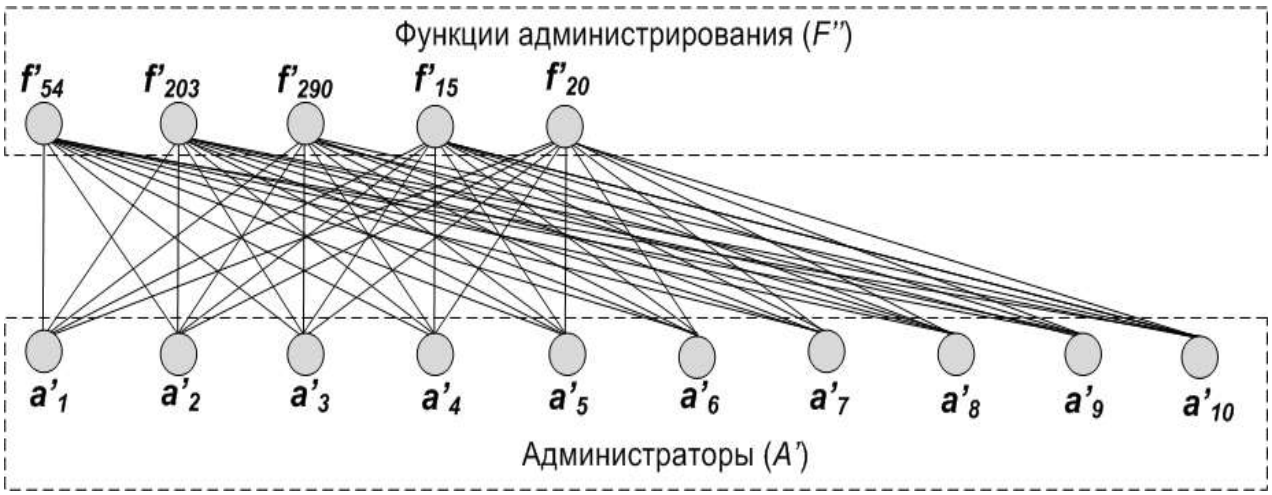


Рисунок П4.2 - Подграф *G''(A';F'';Y), |F''|<|A'|*

Шаг 4. Построим квадратную матрицу $A'F''=(t^*_{|F''|,|A'|})$ размером $|A'|$. Если $|F''|<|A'|$, то дополним матрицу нулевыми столбцами. Прогнозируемое время t^* ФА рассчитывается с учетом ФА, назначенных администратору ИБ на предыдущих циклах (для случаев $|F'|>|A'|$).

Шаг 5. Применяя алгоритм Куна-Манкреса к $A'F''$ получаем решение с минимальным суммарным прогнозируемым временем восстановления производительности КТС.

Шаг 6. Если все требующие решения ФА выполнены, то завершить алго-

ритм, иначе перейти к шагу 2.

Конец алгоритма.

Экспериментальная часть

Для исследования характеристик процессов восстановления производительности КТС была поставлена серия имитационных экспериментов в среде AnyLogic. Входные данные имитационной модели: $|S|$ = 1000 элементов; $A'F'$ - матрица прогнозируемого времени выполнения ФА администраторами; G' - взвешенный граф КТС.

Экспериментальное исследование №1

Цель эксперимента №1 - исследовать влияние разработанного алгоритма на изменение времени восстановления производительности КТС.

Условия эксперимента:

- решение инцидентов ИБ реализуется одновременно пятью администраторами ИБ;

- каждый администратор единовременно выполняет одну ФА;

- каждый из администраторов может быть назначен на решение любой ФА;

- время выполнения ФА для администраторов различно;

- единица модельного времени усл.час;

- время моделирования – 4320 усл.час.

Анализ полученных данных: на рисунке П4.3 результаты представлены двумя диаграммами прироста производительности КТС в период ее восстановления. Значение 70% от максимальной производительности при разработанном алгоритме достигается уже через 1,9 усл.часа (по сравнению с классической процедурой – 2,4 усл.час). Кроме того, 100% производительности при разработанном алгоритме назначения администраторов достигается в среднем за 3,1 усл.час (по сравнению с классической процедурой – 3,7 усл.час).

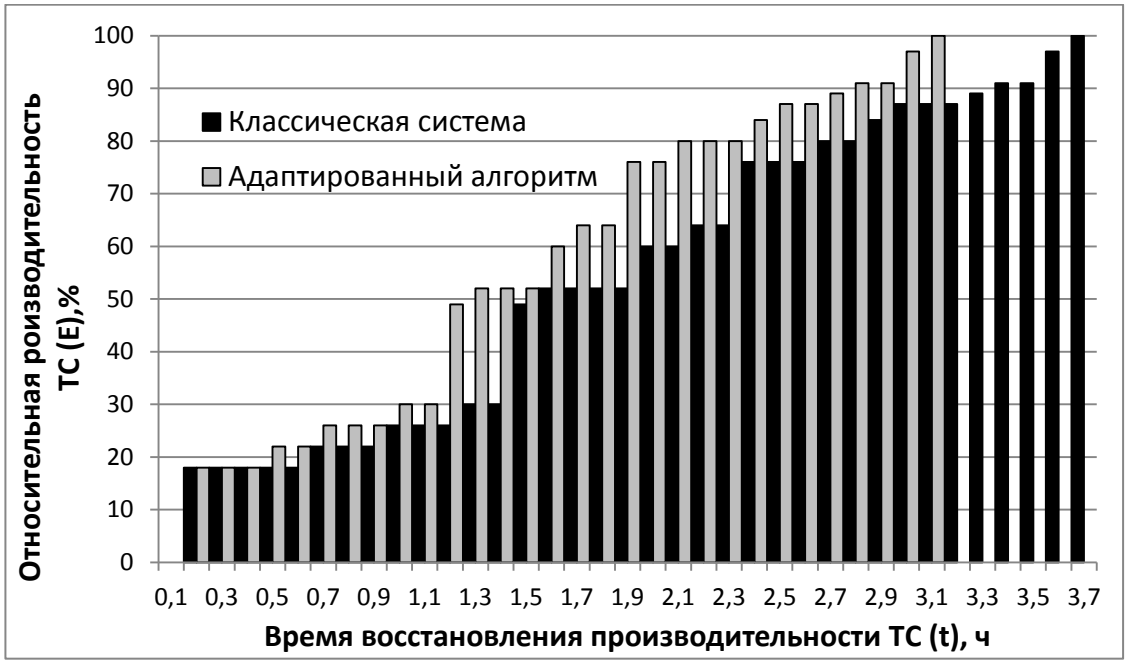


Рисунок П4.3 – Прирост производительности КРИВС

Очевидными причинами снижения времени цикла восстановления производительности КТС являются снижение среднего времени исполнения ФА, балансировка загрузки множества администраторов ИБ КТС.

Экспериментальное исследование №2

Цель эксперимента №2 - исследование зависимости выигрыша в приросте производительности КТС при применении разработанного алгоритма назначения администраторов в условиях различного количества обрабатываемых инцидентов ИБ.

Результаты серии опытов, демонстрирующих зависимость среднего выигрыша в приросте производительности КТС в зависимости от количества инцидентов ИБ представлены на рисунке П4.4. Из графика видно, что внедрение алгоритма назначения администраторов и методики формирования очереди решения инцидентов способствует увеличению прироста производительности КТС, значение которого увеличивается с увеличением количества решаемых инцидентов.

Результаты моделирования показали, что выигрыш в приросте производи-

тельности при применении разработанного подхода в формировании очереди ремонтно-восстановительных работ зависит от количества одновременно решаемых инцидентов, применение разработанного алгоритма и модели администратора ИБ позволяют сократить время цикла восстановления производительности КТС в среднем на 16%.

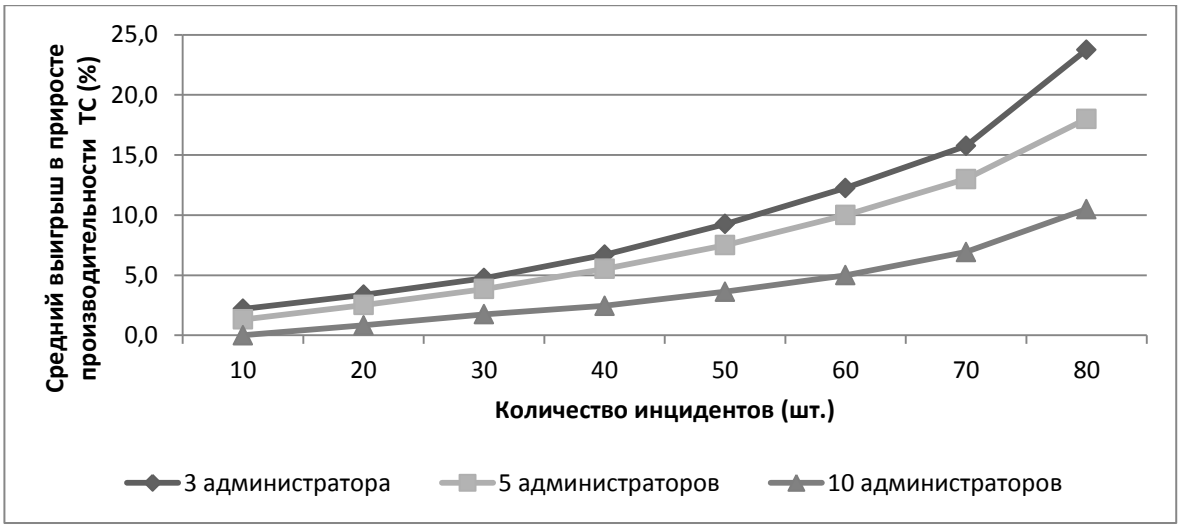


Рисунок П4.4 - Зависимость среднего выигрыша в приросте производительности в зависимости от количества инцидентов ИБ

Приложение 5. Копии актов о внедрении результатов диссертации

УТВЕРЖДАЮ
Председатель комитета информатизации,
связи и телекоммуникаций администрации
Владимирской области

_____ Петров А.А.
"__" _____ 20__ г.

г. Владимир

АКТ

внедрения результатов работы
Мишина Дениса Вячеславовича, Монаховой Марии Михайловны
"Система документированного обеспечения администрирования корпоративной сети передачи данных"

Комиссия в составе: заместитель председателя комитета информатизации Коровушкин М.Н., заведующий каф. ИЗИ д.т.н. профессор Монахов М.Ю. составили настоящий акт о том, что результаты работы "Система документированного обеспечения администрирования корпоративной сети передачи данных" использованы в сети передачи данных администрации Владимирской области (СПД АВО):

1. Разработан типовой комплект технической документации на СПД АВО «Информатика и защита информации», включающий информационно-техническую, информационно-графическую и организационно-правовую документацию;
2. Разработаны и внедрены решения по автоматизации процессов функционирования системы документированного обеспечения администрирования корпоративной сети передачи данных.

Использование указанных результатов позволяет: повысить ответственность персонала в сфере информационной безопасности кафедры; сократить затраты на проведение профилактических и восстанавливающих мероприятий; сохранить текущую работоспособность СПД АВО.

Члены комиссии:
_____ Коровушкин М.Н.

_____ Монахов М.Ю.

МП

УТВЕРЖДАЮ
Главный инженер
ООО «НПП «ИНПРОКОМ»
_____Куковякин А.Г.

АКТ ВНЕДРЕНИЯ

результатов диссертационной работы Монаховой М.М. «Модели и алгоритмы контроля инцидентов информационной безопасности в корпоративной телекоммуникационной сети»

Следующие результаты диссертационной работы использованы в технических мероприятиях Инженерно-промышленной компании НПП «ИНПРОКОМ»:

1. Методика определения существенных факторов возникновения инцидентов ИБ в корпоративной сети предприятия.
2. Комплекс организационно-технических мероприятий и программных средств учета телекоммуникационных ресурсов корпоративной сети.

Использование разработанных средств позволяет снижать среднее время выполнения функции устранения инцидента - на 25%.

Начальник ОИТ Силаев М.И.

УТВЕРЖДАЮ
Начальник ИВЦ
ОАО ВЗ «Электроприбор»
Филичкин А.А.

30.07.2016

АКТ

об использовании результатов диссертационной работы Монаховой М.М. «Модели и алгоритмы контроля инцидентов информационной безопасности в корпоративной телекоммуникационной сети»

Следующие результаты, полученные в диссертационной работе Монаховой М.М., использованы в работах по обеспечению информационной безопасности корпоративной сети ОАО «Владимирский завод «Электроприбор»:

1. Информационное и программное обеспечение системы администрирования корпоративной сети, включающее программные модули для расчета значимости элементов корпоративной сети, контроля нарушений Политики информационной безопасности сети.
2. Методика оценки уровня защищенности корпоративной сети предприятия.
3. Комплекс организационно-технических мероприятий и программных средств учета телекоммуникационных ресурсов корпоративной сети.

Инженер по АСУ 30.07.16 Кулаков М.А.

«УТВЕРЖДАЮ»
Первый проректор, проректор
по научной и инновационной работе ВлГУ,
д.ф-м.н., профессор
_____ В.Г. Прокошев
_____ 2016 г.

АКТ ВНЕДРЕНИЯ
результатов диссертационной работы

Материалы диссертационной работы Монаховой Марии Михайловны «Модели и алгоритмы контроля инцидентов информационной безопасности в корпоративной телекоммуникационной сети», представленной на соискание ученой степени кандидата технических наук, были внедрены в учебный процесс кафедры радиотехники и радиосистем ВлГУ при подготовке бакалавров по направлению 11.03.02 - «Инфокоммуникационные технологии и системы связи» и используются для методического обеспечения лабораторного практикума дисциплин «Компьютерные сети», «Аппаратура и средства защиты информации», «Методы защиты информации».

Заведующий кафедрой
радиотехники и радиосистем ВлГУ
д.т.н., проф.

Никитин О.Р.