На правах рукописи

Мамаев Александр Владимирович

СИНТЕЗ РЕЗЕРВНОГО КОНТУРА УПРАВЛЕНИЯ СЛУЖБЫ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ НА ОСНОВЕ СЕТЕЙ ПЕТРИ

Специальность: 05.13.19 — методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Автор: _____

Москва — 2012

Работа выполнена в Национальном исследовательском ядерном университете «МИФИ» (НИЯУ МИФИ)

Научный руководитель:
Петрова Тамара Васильевна — кандидат технических наук, доцент кафедры «Криптология и дискретная математика»

Официальные оппоненты:
Конявский Валерий Аркадьевич — доктор технических наук,
Всероссийский научно-исследовательский институт проблем вычислительной техники и информатизации, заместитель директора по вопросам науки

Журин Сергей Игоревич — кандидат технических наук, доцент кафедры «Защита информации», Научно-исследовательский институт Систем Безопасности Федеральное государственное унитарное предприятие "Специальное научно-производственное объединение "Элерон", начальник лаборатории разработки информационных систем

Ведущая организация:
Институт информационных наук и технологий безопасности Российского государственного гуманитарного университета

Защита состоится «29» марта 2012 г. в 15 часов 00 минут на заседании диссертационного совета ДМ 212.130.08 в Национальном исследовательском ядерном университете «МИФИ»: 115409, г. Москва, Каширское ш., д.31. Тел. для справок: +7 (499) 323-95-26.

С диссертацией можно ознакомиться в библиотеке Национального исследовательского ядерного университета «МИФИ».

Отзывы в двух экземплярах, заверенные печатью, просьба направлять по адресу: 115409, г. Москва, Каширское ш., д.31, диссертационные советы НИЯУ МИФИ, тел.: +7 (499) 323-95-26.

Автореферат разослан «27» февраля 2012 г.

Ученый секретарь
диссертационного совета  Горбатов В.С.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. Широкое применение современных информационных технологий в правительственных организациях, банковских структурах, промышленности и других организациях привело к возникновению новых видов преступлений связанных с использованием средств вычислительной техники (СВТ) и различных технических средств. При этом внутри учреждений для обработки, хранения, передачи основных объемов информации повсеместно используются автоматизированные системы или пакеты прикладных программ. Обеспечение безопасности информации является одним из важных вопросов в области информационного обеспечения деятельности любой организации. Необходимым условием нормального существования и развития для них является защищенность, как от внешних, так и от внутренних угроз.

Исследование PricewaterhouseCoopers, крупнейшей в мире международной сети компаний, предлагающих профессиональные услуги в области консалтинга и аудита, проводимое на основе анкет показало, что в 2011 году в 55% случаев нарушители были внутри компании против 35% в 2009 году. Это свидетельствует о том, что проблемам внутренних угроз уделяется недостаточное внимание со стороны служб безопасности.

По данным исследования, проведенного российской компанией InfoWatch, утечка информации является одним из самых распространенных и опасных видов внутренних угроз. Средства защиты от несанкционированного доступа (НСД) здесь оказываются практически бесполезными, поскольку в качестве основного источника угрозы выступает внутренний нарушитель - пользователь информационной системы, имеющий вполне легальный доступ к конфиденциальной информации и применяющий весь арсенал доступных ему средств для того, чтобы использовать конфиденциальную информацию в своих интересах.

Существенным моментом является то, что внутренний нарушитель может получить доступ к инфраструктуре информационной системы, а значит и возможность совершения деструктивного воздействия на ее отдельные элементы или систему в целом.

При эксплуатации объекта информатизации (ОИ) неизбежно возникает вопрос о защищенности ОИ в целом и отдельных его составляющих в частности от реализаций угроз безопасности информации. Постоянное увеличение объемов конфиденциальной информации в организациях, непостоянство штата сотрудников, изменение бизнес-процессов — все это приводит к увеличению рисков утечки информации. Большие, сильно распределенные информационные системы крайне сложно контролировать службам безопасности. Системы комплексной защиты информации от утечек, активно развивающиеся в последнее время, призваны на помощь для решения данной проблемы. Однако не всегда компьютерная программа может сама распознать в действиях пользователя умышленную утечку информации. Как заявляют специалисты, такие системы защищают

ото всех случайных утечек и части умышленных, поэтому роль человека, сотрудника службы безопасности, остается крайне важной, и для ее выполнения система комплексной защиты информации от утечек должна максимально быстро и полно сообщать о подозрительных действиях пользователя. На рисунке 1 приведены данные из исследования компании InfoWatch, показывающие растущую тенденцию количества утечек информации.

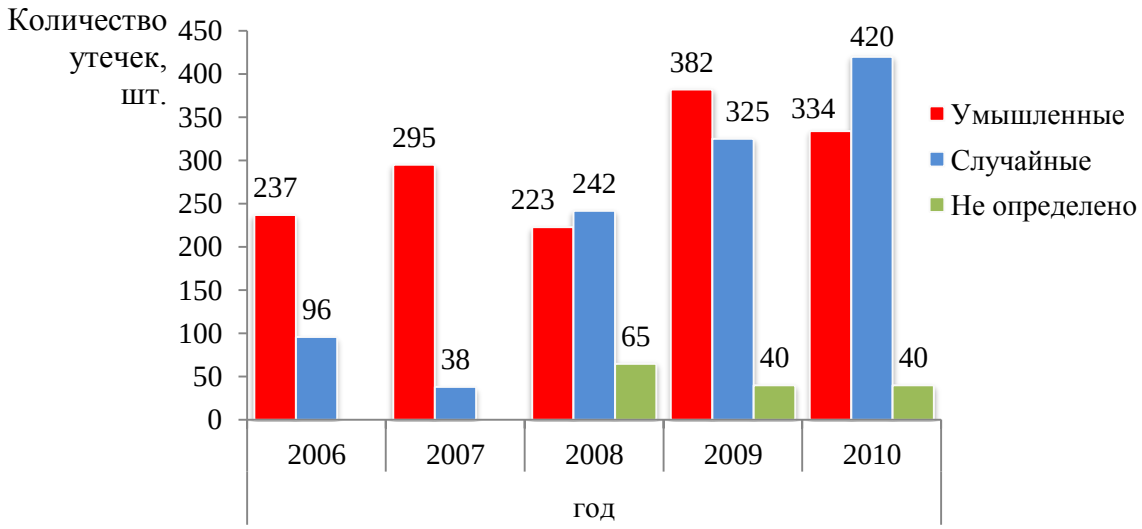


Рисунок 1 — Динамика утечек информации

Защита каждого объекта информатизации, а также подходы к ее реализации строго индивидуальны. Обеспечение информационной безопасности предполагает проведение целого комплекса организационных и технических мероприятий по обнаружению, отражению, ликвидации воздействий угроз различного рода. Даже одно слабое звено в системе безопасности, возникающее в результате какого-либо изъяна в ее организации, не позволит прочим звеньям в нужный момент противостоять возникшим угрозам.

Особое внимание должно уделяться безопасности критически важных объектов, на которых высока вероятность диверсий через внедренных агентов. Поэтому для построения надежной защиты необходимо выявить все возможные угрозы безопасности информации, оценить их опасность, способ их реализации и по этим данным определиться с требуемыми мерами и средствами защиты, а также оценить их эффективность.

Вопросами обеспечения безопасности информации от внутренних нарушителей занимаются как российские, так и зарубежные исследователи: Скиба В.Ю., Курбатов В.А., Лукацкий А.В., Костров Д.В., Джоунс Э. (Jones A.), Кулвил К. (Colwill C.), Мур А.(Moore A), Капелли Д. (Cappelli D.) и др.

Анализ систем защиты от утечки информации выявил их существенные недостатки, связанные с архитектурными особенностями в целом и работой контура управления в частности:

– отсутствие механизма резервирования канала передачи сообщений;

– отсутствие механизма контроля загрузки штатной операционной системы.

Автором работы предлагается новый подход к решению описанных выше проблем: создание резервного контура управления службы безопасности организации. Данный подход реализуется в системе мониторинга для защиты информации от утечки, которая использует разработанный резервный канал передачи тревожных сообщений. В свою очередь — это позволяет контролировать загрузку штатной операционной системы. Все эти решения обуславливают выбор темы исследования и подтверждают актуальность работы.

Объектом исследования являются системы мониторинга для защиты информации от внутреннего нарушителя.

Предмет исследования. Уязвимости систем мониторинга для защиты информации от внутреннего нарушителя, приводящие к бесконтрольной работе ЭВМ, и методы защиты.

Цель диссертационной работы. Повышение защищенности объектов информатизации путем блокировки питания ЭВМ при недопустимых параметрах загрузки операционной системы.

Для достижения поставленной цели необходимо:

– провести анализ существующих систем мониторинга для защиты информации от внутреннего нарушителя с целью выявления уязвимостей;
– построить модель нарушителя, провести анализ возможных способов несанкционированного съема информации;
– предложить методические основы в рамках концепции передачи низкочастотных сигналов по сети электропитания;
– разработать методику противодействия работе пользователя на неконтролируемой ЭВМ;
– разработать экспериментальные основы проверки теоретических результатов исследования;
– предложить способ оценки стойкости предложенного механизма защиты к деструктивным воздействиям;
– разработать аппаратно-программный комплекс, реализующий систему мониторинга для защиты информации от внутреннего нарушителя.

Научная задача заключается в синтезе резервного информационного канала контура управления службы безопасности в терминах теории сетей Петри для решения задачи достижимости заданной разметки.

Методы исследования. В исследовании использовались методы теории графов, сетей Петри, теории множеств, теории информационной безопасности и защиты информации.

Научная новизна работы состоит в следующем:

– предложена и исследована математическая модель систем мониторинга для защиты информации от внутреннего нарушителя в терминах тео-

рии сетей Петри. Построенная модель позволяет выявить уязвимости систем мониторинга, влияющие на стойкость к деструктивным воздействиям внутреннего нарушителя;

- построена математическая модель функционирования резервного канала передачи сигналов оповещения по сети электропитания ЭВМ, который позволяет обеспечить непрерывность работы контура управления службы безопасности;
- предложена методика противодействия временному отключению системы защиты, что позволяет исключить возможность работы пользователя на неконтролируемой ЭВМ.

Практическая ценность заключается в том, что реализован контур управления службы безопасности, который включает в себя новую систему мониторинга на основе аппаратно-программного комплекса передачи низкочастотных сигналов по сети электропитания ЭВМ. Полученный контур управления обеспечивает непрерывность защиты информации от утечки на стационарных персональных компьютерах и серверах.

Достоверность результатов исследования подтверждается формальными математическими выводами основных утверждений, сформулированных в работе, использованием известных проверенных на практике методов и результатами лабораторного эксперимента.

Внедрение результатов. Результаты диссертационной работы использованы в проектно-конструкторской деятельности ЗАО «Амулет», использованы в работе службы безопасности ООО «Еврокорр-2010», использованы в учебном курсе «Аппаратные средства вычислительной техники» кафедры «Криптология и дискретная математика» НИЯУ МИФИ.

Публикации и апробация работы. Основные положения диссертационной работы изложены в 8 публикациях, 4 из которых опубликованы в журналах, входящих в Перечень ВАК, и 4 тезисов научных докладов.

Структура работы. Работа состоит из введения, четырех глав, заключения и списка литературы, включающего 104 наименований. Текст диссертации изложен на 141 странице, включая 23 рисунка и 11 таблиц.

СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обосновывается актуальность темы диссертации, выделяются и формулируются цель и задачи исследования, описывается структурно-логическая схема диссертационной работы.

В **первой главе** представлены результаты анализа особенностей применения систем защиты от внутреннего нарушителя в рамках комплексного подхода к обеспечению безопасности информации. Системы мониторинга от утечки информации, являющиеся звеньями контура управления службы безопасности, исследуются с точки зрения архитектуры и функционального устройства, используемых методов и алгоритмов передачи сигналов.

Существующие системы защиты от утечки информации делятся на:

– шлюзовые;
– локальные;
– комбинированные.

Шлюзовые системы используются для анализа исходящего трафика и выявления несанкционированной передачи информации по электронной почте, в чатах, системах мгновенного обмена сообщениями и в различных сетевых протоколах. Как следует из названия, эти системы устанавливаются на шлюзе внутренней сети организации, что позволяет контролировать только заданный периметр безопасности.

Локальные системы используются для обеспечения безопасности информации на уровне рабочих станций. На защищаемых электронно-вычислительных машинах (ЭВМ) устанавливается специализированное контролирующее программное обеспечение, перехватывающее не только все формы электронных взаимодействий, но и клавиатурный набор, а также образы экрана. Это программное обеспечение обладает возможностями идентификации подозрительной активности пользователя (в том числе такой, которая может предшествовать краже сведений) и предоставляет аналитику набор отчетов, содержащих различные срезы информации, касающейся действий над конфиденциальными данными. Программные агенты таких систем могут также блокировать определенные действия пользователей, например, передачу файлов, запись определенной информации на внешние носители и доступ к определенным категориям вебсайтов.

Комбинированные системы сочетают в себе возможности как шлюзовых, так и локальных систем. Это позволяет контролировать максимальное количество каналов утечки информации и обеспечивает наибольший эффект от системы защиты. Для дальнейшего анализа были выбраны комбинированные системы, так как они сочетают достоинства и недостатки как шлюзовых, так и локальных систем.

Примерами комбинированных систем, представленных на российском рынке, являются:

– InfoWatch Traffic Monitor (российская компания «InfoWatch»);
– SecurIT Zgate и Zlock (российская компания «SecurIT»);
– Secure Tower (российская компания «Falcongaze»);
– Symantec DLP (компания из США «Symantec»);
– Websense DSS (компания из США «Websense»);
– Trend Micro DLP (компания из Японии «Trend Micro»);
– McAfee Host DLP (компания из США «McAfee»).

Система мониторинга должна обеспечивать контроль над всеми действиями пользователя на всем протяжении работы защищаемой ЭВМ. Это говорит о необходимости функционирования до запуска ОС, чтобы контролировать загрузку штатной ОС, а также об использовании такого резервного канала передачи сигналов, который работает всегда, пока включена защищаемая ЭВМ.

В таблице 1 представлены результаты сравнения систем мониторинга в выбранных продуктах по основным параметрам, которые напрямую указывают на низкую стойкость к деструктивным действиям возможного нарушителя.

По результатам проведенного исследования было выявлено, что выбранные системы мониторинга используют локально-вычислительную сеть в качестве единственного канала передачи тревожных сообщений в службу безопасности и работают только с момента старта штатной операционной системы (ОС), что, при деструктивных воздействиях внутреннего нарушителя, может привести к утечке информации.

Таблица 1 — Сравнение систем мониторинга

Название системы защиты	Контроль работы агента	Функционирование до запуска ОС	Аппаратно-программная реализация	Гарантированная передача сообщений
InfoWatch Traffic Monitor	+	–	+	–
SecurIT Zgate и Zlock	+	–	–	–
Secure Tower	+	–	–	–
Symantec DLP	+	–	–	–
Websense DSS	+	–	+	–
Trend Micro DLP	+	–	+	–
McAfee Host DLP	+	–	+	–
Авторская система	+	+	+	+

Таким образом, необходимо разработать такую систему мониторинга, которая позволит гарантированно доставлять тревожные сообщения в службу безопасности на всем протяжении работы защищаемой ЭВМ. Для резервного канала передачи сообщений необходимо использовать сеть электропитания, как единственный общий ресурс, совместно использующийся с защищаемой ЭВМ.

Во **второй главе** представлены результаты исследования проблем построения системы мониторинга для защиты от утечки информации с использованием теории графов, теории сетей Петри и теории множеств. Построена модель нарушителя.

Основным нарушителем является внутренний нарушитель с правами легитимного пользователя, подрабатывающий или внедренный, т.е. преследующий корыстные цели при совершении действий, приводящих к утечке информации в обход системы защиты. Внутренний нарушитель имеет доступ к работе со штатными средствами автоматизированных систем (АС) и СВТ как части АС.

По своим возможностям может воздействовать на программное обеспечение системы и на конфигурацию оборудования, не раскрывая себя, что, исходя из Руководящего документа «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к инфор-

мации», соответствует третьему уровню нарушителя. Ввиду наличия службы безопасности внутренний нарушитель не может вносить/выносить оборудование через защищаемый периметр.

Угрозы утечки информации, связанные с действиями внутреннего нарушителя, можно разделить на 2 класса:

– угрозы, направленные на получение возможности работать с данными в нештатной операционной системе;

– угрозы, направленные на нарушение работоспособности канала передачи тревожных сообщений с защищаемой ЭВМ в службу безопасности.

Реализация данных угроз приводит к тому, что нарушается работа контура управления службы безопасности, а значит, информация на ЭВМ оказывается потенциально незащищенной.

В результате проведенного анализа возможных действий нарушителя были сформулированы следующие требования, предъявляемые к разрабатываемой системе мониторинга для защиты информации от утечки:

– наличие резервного канала передачи тревожных сообщений;

– резервный канал не должен требовать создания новой среды передачи сигналов;

– гарантированная передача сигналов оповещения о противоправных действиях пользователя на всем протяжении работы защищаемой ЭВМ;

– наличие механизма контроля работоспособности системы мониторинга.

В работе предложены математические модели, интерпретирующие работу системы мониторинга, как в штатном режиме, так и при действиях внутреннего нарушителя. Данные модели построены в терминах теории сетей Петри.

В данных сетях используются следующие состояния и переходы:

– состояние $\mathbf{p_1}$ «наличие электропитания» характеризующее главный ресурс, необходимый для функционирования ЭВМ;

– состояние $\mathbf{p_2}$ «наличие штатной ОС» отражающее необходимость контроля загружаемой пользователем системы;

– состояние $\mathbf{p_3}$ «штатная работа ОС» соответствующее состоянию защищаемой ЭВМ, работающей в соответствии с требованиями политик безопасности;

– состояние $\mathbf{p_4}$ «тревога» характеризующее момент регистрации нарушения политики безопасности;

– состояние $\mathbf{p_5}$ «тревожное сообщение готово к отправке» означающее готовность системы мониторинга к отправке сообщения в службу безопасности по работающему каналу передачи;

– состояние $\mathbf{p_6}$ «канал передачи работает» характеризующее независимость функционирования сети передачи от защищаемой ЭВМ;

– состояние $\mathbf{p_7}$ «сообщение получено» отражающее получение тревожного сообщения службой безопасности;

– состояние $\mathbf{p_8}$ «наличие нештатной ОС» соответствующее реализации внутренним нарушителем первого класса угроз;

– состояние $\mathbf{p_9}$ «канал передачи не работает» соответствующее реализации внутренним нарушителем второго класса угроз;

– переход $\mathbf{t_1}$ «загрузка штатной ОС» использующийся для описания процесса включения защищаемой ЭВМ;

– переход $\mathbf{t_2}$ «нарушение политик безопасности» отображающий выявление системой защиты нештатных действий пользователя;

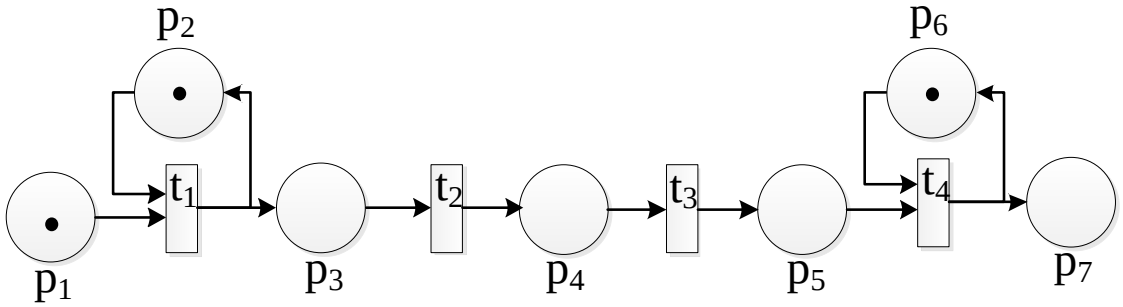
– переход $\mathbf{t_3}$ «создание тревожного сообщения» характеризующий процесс подготовки сообщений с кодом тревоги и номером защищаемой ЭВМ;

– переход $\mathbf{t_4}$ «передача сообщения» использующийся для отображения процесса передачи сообщения с защищаемой ЭВМ в службу безопасности;

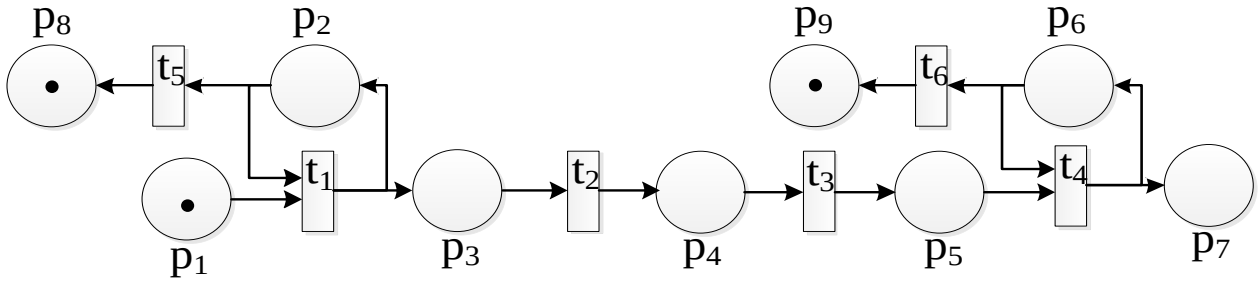
– переход $\mathbf{t_5}$ «изменение/блокирование штатной ОС» соответствующий действиям внутреннего нарушителя при реализации первого класса угроз;

– переход $\mathbf{t_6}$ «деструктивное воздействие на канал передачи» соответствующий действиям внутреннего нарушителя при реализации второго класса угроз.

Модель, интерпретирующая процесс функционирования системы мониторинга, представлена на рисунке 2, *а*. На представленной сети Петри, выявленные уязвимости систем мониторинга отражены в состояниях $\mathbf{p_2}$ и $\mathbf{p_6}$. На рисунке 2, *б* представлена обобщенная модель, интерпретирующая процесс функционирования системы мониторинга с учетом воздействий внутреннего нарушителя.



а



б

Рисунок 2 — Сети Петри, интерпретирующие процесс функционирования системы мониторинга в случае отсутствия воздействия (*а*) и присутствия (*б*)

Анализ полученных моделей показал, что в случае *2, а* выполняется условие $\mathbf{p_7}$ «сообщение получено», а в случае *2, б* — нет, что подтверждает выявленные уязвимости рассматриваемых систем.

Постановка задачи. Необходимо построить такую сеть Петри, интерпретирующую процесс функционирования системы мониторинга, с учетом воздействий внутреннего нарушителя, в которой решалась бы задача достижимости заданной разметки.

Для достижения поставленной задачи используется обобщенная модель, которая дополняется соответствующими состояниями и переходами так, чтобы свободный язык сети Петри включал хотя бы одно слово приводящее к выполнению условия $\mathbf{p_7}$, где $\mathbf{p_7}$ соответствует состоянию «сообщение получено».

$$\mathbf{L(N)=\{\exists \tau \in T |\ \exists M \in R(N): M_0[\tau\rangle M, \exists M' \in R(N): M' = (0,0,0,0,0,0,1,0,0,0,0,0) | M \geq M'\},} \quad \mathbf{(1)}$$

где **N —** сеть Петри, **L(N) —** множество последовательностей срабатываний сети **N** или свободный язык сети **N**, **τ —** слово в алфавите **T**, **M** — разметка сети **N, R(N)** — множество разметок сети **N.**

Предлагается дополнить сеть Петри, интерпретирующую процесс функционирования системы мониторинга в случае присутствия воздействий внутреннего нарушителя, следующими состояниями и переходами:

- $\mathbf{p_{10}}$ — сторожевой таймер включен;
- $\mathbf{p_{11}}$ — сообщение для резервного канала передачи готово;
- $\mathbf{p_{12}}$ — резервный канал передачи работает;
- $\mathbf{t_7}$ — подача электричества, включение ЭВМ;
- $\mathbf{t_8}$ — срабатывание сторожевого таймера;
- $\mathbf{t_9}$ — передача сообщений по резервному каналу.

Состояние $\mathbf{p_{10}}$ «сторожевой таймер включен» характеризует механизм защиты от НСД, в результате действий внутреннего нарушителя, направленных на получение возможности работать с данными в нештатной операционной системе. Работа «сторожевого таймера» позволяет оповещать службу безопасности о соответствующих действиях внутреннего нарушителя.

Состояние $\mathbf{p_{11}}$ «сообщение для резервного канала передачи готово» характеризует механизм резервирования канала передачи тревожных сообщений с защищаемой ЭВМ в службу безопасности.

Состояние $\mathbf{p_{12}}$ «резервный канал передачи работает» характеризует физическую среду канала передачи.

Переход $\mathbf{t_7}$ «подача электричества, включение ЭВМ» используется для того, чтобы подчеркнуть необходимость использования такого канала передачи, который будет работать всегда, пока работает защищаемая ЭВМ.

Переход $\mathbf{t_8}$ «срабатывание сторожевого таймера» используется для отображения процесса оповещения службы безопасности при срабатывании механизма «сторожевого таймера».

Переход $\mathbf{t_9}$ «передача сообщений по резервному каналу» используется для отображения процесса передачи сообщения с защищаемой ЭВМ в службу безопасности при не работающем основном канале передачи.

Таким образом, в виде модели, интерпретирующей процесс функционирования дополнительного канала передачи сигналов оповещения по сети электропитания ЭВМ в рамках работы системы мониторинга, предлагается использовать сеть Петри следующего вида: $\mathbf{N=(P,T,F,M_0)}$, где $\mathbf{P=\{p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8, p_9, p_{10}, p_{11}, p_{12}\}}$ — множество состояний, $\mathbf{T=\{t_1, t_2, t_3, t_4, t_5, t_6, t_7, t_8, t_9\}}$ — множество переходов, **F** — функция инцидентности, которая задается с помощью таблицы 2 и таблицы 3, в которых на пересечении строки x и столбца y стоит число **F(x,y)**.

Таблица 2 — Значения выходной функции

Переходы	**Состояния**											
	$\mathbf{p_1}$	$\mathbf{p_2}$	$\mathbf{p_3}$	$\mathbf{p_4}$	$\mathbf{p_5}$	$\mathbf{p_6}$	$\mathbf{p_7}$	$\mathbf{p_8}$	$\mathbf{p_9}$	$\mathbf{p_{10}}$	$\mathbf{p_{11}}$	$\mathbf{p_{12}}$
$\mathbf{t_1}$	0	**1**	**1**	0	0	0	0	0	0	0	0	0
$\mathbf{t_2}$	0	0	0	**1**	0	0	0	0	0	0	0	0
$\mathbf{t_3}$	0	0	0	0	**1**	0	0	0	0	0	**1**	0
$\mathbf{t_4}$	0	0	0	0	0	**1**	**1**	0	0	0	0	0
$\mathbf{t_5}$	0	0	0	0	0	0	0	**1**	0	0	0	0
$\mathbf{t_6}$	0	0	0	0	0	0	0	0	**1**	0	0	0
$\mathbf{t_7}$	0	0	0	0	0	0	0	0	0	**1**	0	**1**
$\mathbf{t_8}$	0	0	0	**1**	0	0	0	0	0	**1**	0	0
$\mathbf{t_9}$	0	0	0	0	0	0	**1**	0	0	0	0	**1**

Таблица 3 — Значения входной функции

Состояния	**Переходы**								
	$\mathbf{t_1}$	$\mathbf{t_2}$	$\mathbf{t_3}$	$\mathbf{t_4}$	$\mathbf{t_5}$	$\mathbf{t_6}$	$\mathbf{t_7}$	$\mathbf{t_8}$	$\mathbf{t_9}$
$\mathbf{p_1}$	0	0	0	0	0	0	**1**	0	0
$\mathbf{p_2}$	**1**	0	0	0	**1**	0	0	0	0
$\mathbf{p_3}$	0	**1**	0	0	0	0	0	0	0
$\mathbf{p_4}$	0	0	**1**	0	0	0	0	0	0
$\mathbf{p_5}$	0	0	0	**1**	0	0	0	0	0
$\mathbf{p_6}$	0	0	0	**1**	0	**1**	0	0	0
$\mathbf{p_7}$	0	0	0	0	0	0	0	0	0
$\mathbf{p_8}$	0	0	0	0	0	0	0	0	0
$\mathbf{p_9}$	0	0	0	0	0	0	0	0	0
$\mathbf{p_{10}}$	**1**	0	0	0	0	0	0	**1**	0
$\mathbf{p_{11}}$	0	0	0	0	0	0	0	0	**1**
$\mathbf{p_{12}}$	0	0	0	0	0	0	0	0	**1**

Начальная разметка $\mathbf{M_0}$ задается следующим образом: $\mathbf{M_0(p_1)=1}$, $\mathbf{M_0(p_2)=0}$, $\mathbf{M_0(p_3)=0}$, $\mathbf{M_0(p_4)=0}$, $\mathbf{M_0(p_5)=0}$, $\mathbf{M_0(p_6)=0}$, $\mathbf{M_0(p_7)=0}$, $\mathbf{M_0(p_8)=1}$, $\mathbf{M_0(p_9)=1}$, $\mathbf{M_0(p_{10})=0}$, $\mathbf{M_0(p_{11})=0}$, $\mathbf{M_0(p_{12})=0}$, или в векторной форме: $\mathbf{M_0=(1,0,0,0,0,0,0,0,1,1,0,0,0)}$. На рисунке 3 представлено графическое изображение предлагаемой модели.

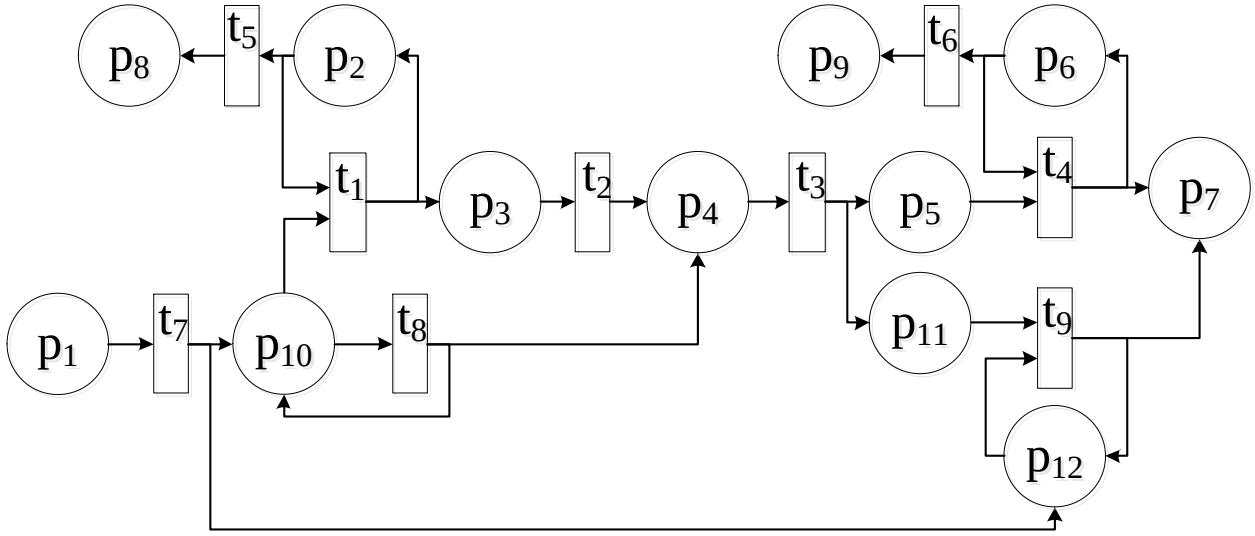


Рисунок 3 — Сеть Петри, интерпретирующая процесс функционирования системы мониторинга при наличии резервного канала передачи

Для анализа построенной сети Петри используется метод полного покрывающего дерева, которое показывает ее динамику функционирования. На рисунке 4 представлено полное покрывающее дерево.

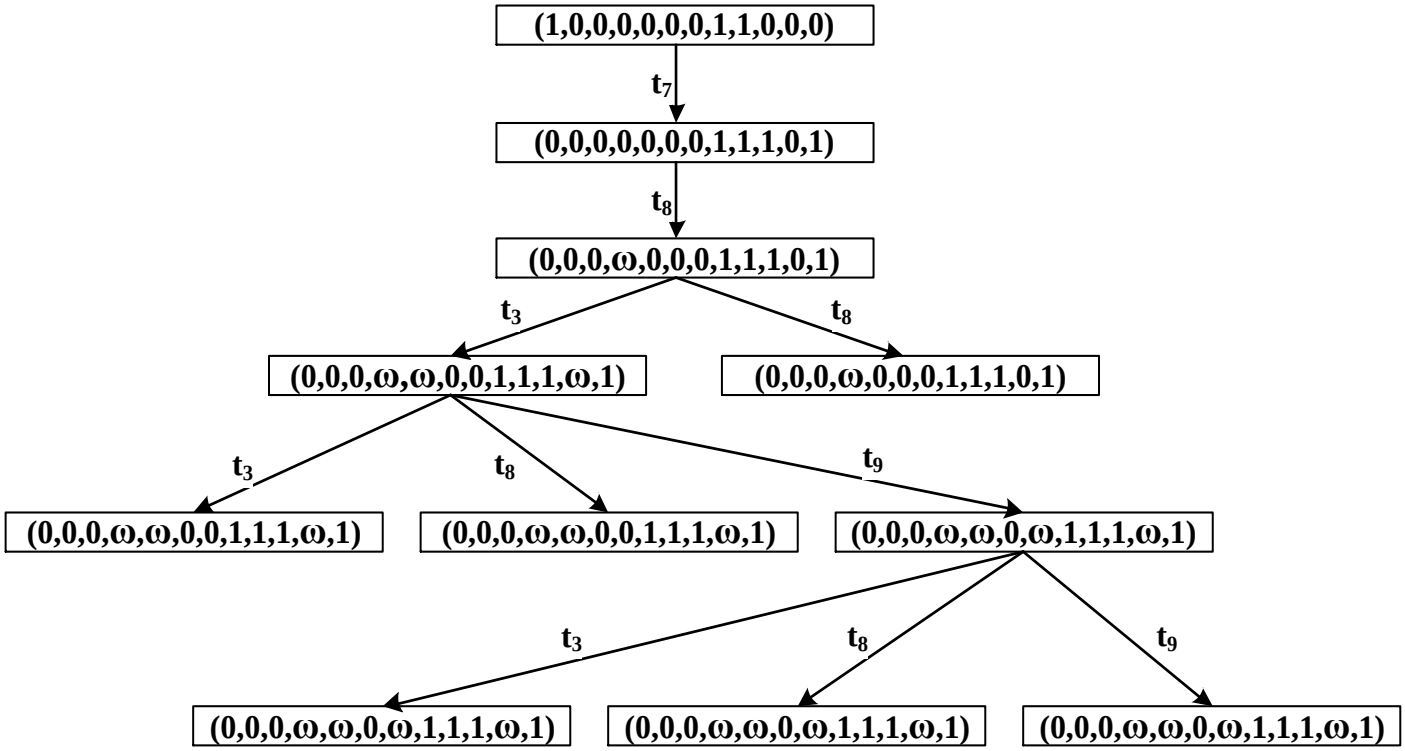


Рисунок 4 — Полное покрывающее дерево сети **N**

Свободный язык предложенной сети включает слова: **L(N)={λ, t_7, t_7t_8, $t_7t_8t_3$, $t_7t_8t_8$, $t_7t_8t_3t_3$, $t_7t_8t_3t_8$, $t_7t_8t_3t_9$, $t_7t_8t_3t_9t_3$, $t_7t_8t_3t_9t_8$, $t_7t_8t_3t_9t_9$, ...}**. Так как данная сеть не является ограниченной, то множество достижимых разметок **R(N)** бесконечно. Как видно из рисунка, разметка **M** удовлетворяет условию **M=(0,0,0,ω,ω,0,ω,1,1,1,ω,1) ≥ M'=(0,0,0,0,0,0,1,0,0,0,0,0)**, причем $\mathbf{M_0[\tau\rangle M}$, где слово $\boldsymbol{\tau = t_7 t_8^n t_3^n t_9^n \in L(N)}$, **n≥1.** Таким образом, полученное слово **τ** является решением уравнения **(1)**, а предлагаемая сеть отвечает поставленной задаче достижимости заданной разметки.

Предлагаемая методика противодействия временному отключению системы защиты для исключения возможности работы пользователя на неконтролируемой ЭВМ реализуется за счет следующей последовательности шагов:

- на предварительном этапе:
  1. обеспечить физическую охрану ЭВМ;
  2. выработать политики безопасности;
  3. установить сервер службы безопасности;
- на основном этапе:
  4. установить аппаратную составляющую системы мониторинга;
  5. установить программную составляющую системы мониторинга;
  6. настроить политики безопасности;
  7. настроить время срабатывания механизма сторожевого таймера;
  8. установить программную составляющую системы мониторинга на сервере безопасности;
  9. подключить сервер безопасности к каналам передачи сообщений;
  10. следить за сообщениями с защищаемых ЭВМ;
  11. блокировать питание ЭВМ при недопустимых параметрах загрузки ОС;
  12. обеспечить оперативное реагирование на сигнал тревоги.

В **третьей главе** диссертационной работы предложена архитектура аппаратно-программного комплекса, реализующего систему мониторинга для защиты информации от утечки.

Система мониторинга состоит из следующих функциональных модулей:

- модуль создания тревожных сообщений;
- модуль контроля работоспособности системы мониторинга;
- модуль хранения политик безопасности и настроек системы мониторинга;
- модуль передачи сообщений по ЛВС;
- модуль передачи сообщений по сети электропитания;
- канал передачи сигнала по сети электропитания;
- модуль обработки получаемых сообщений.

Общая архитектура аппаратно-программного комплекса представлена на рисунке 5.

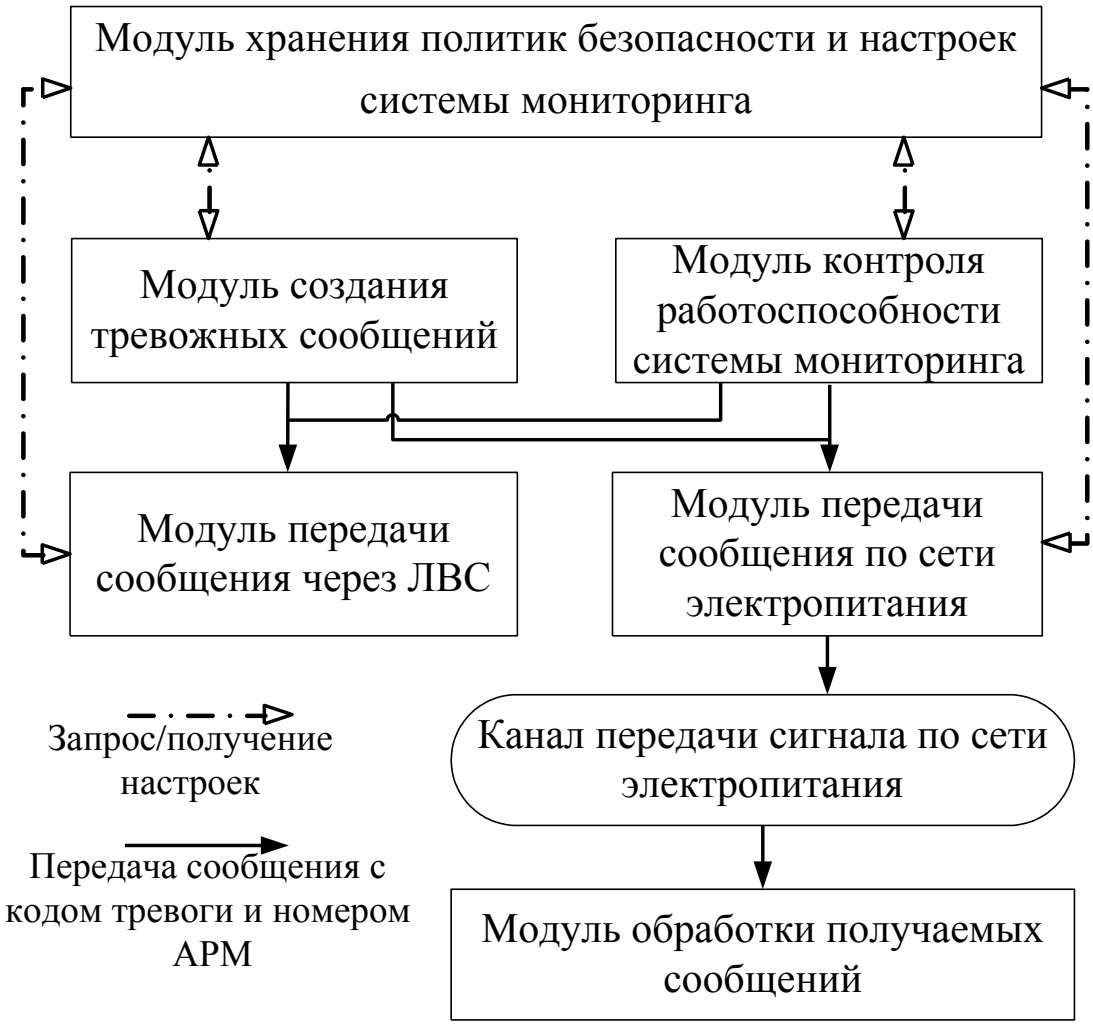


Рисунок 5 — Архитектура аппаратно-программного комплекса

Модуль создания тревожных сообщений получает сигналы тревоги от агентов системы защиты, установленной на защищаемой ЭВМ, регистрирует события в журналах и создает тревожные сообщения в соответствии с действующими политиками безопасности.

Модуль контроля работоспособности системы мониторинга осуществляет постоянный контроль модулей системы мониторинга, установленных на защищаемой машине.

Модуль хранения политик безопасности и настроек системы мониторинга отвечает за хранение политик безопасности и настроек системы мониторинга, которые используются остальными модулями установленными на защищаемой ЭВМ.

Модуль передачи сообщений по ЛВС выполняет отправку тревожных сообщений по основному каналу взаимодействия системы мониторинга с другими службами и системами безопасности организации.

Модуль передачи сообщений по сети электропитания выполняет отправку тревожных сообщений по резервному каналу передачи сигналов системы мониторинга, обеспечивающему гарантированную доставку сигналов тревоги в службу безопасности.

Канал передачи сигнала по сети электропитания осуществляет передачу тревожных сообщений на сервер службы безопасности организации с защищаемой ЭВМ на всем протяжении ее работы.

Модуль обработки получаемых сообщений получает тревожные сообщения с защищаемых ЭВМ, регистрирует события в журналах, выводит на экран соответствующую индикацию.

В **четвертой главе** представлены результаты создания аппаратно-программного комплекса, реализующего систему мониторинга для защиты информации от утечки. Описана схема аппаратной составляющей комплекса. Приведено описание канала передачи низкочастотных сигналов по сети электропитания, процесса передачи и получения сообщений. Описан процесс взаимодействия между уровнем операционной системы и микропрограммой BIOS.

В главе приводятся результаты тестирования реализованной системы мониторинга для защиты информации от утечки. На собранном стенде, состоящем из нескольких защищаемых ЭВМ и сервера безопасности, осуществлялась штатная работа системы мониторинга с имитацией нарушений политик безопасности.

Для оценки стойкости системы защиты к деструктивным воздействиям внутреннего нарушителя и проверки критерия гарантированной передачи тревожных сообщений использовалась «Модель системы защиты с полным перекрытием». Система защиты представляется в виде пятикортежного набора **S={O,T,M,V,B}**, где **O** - набор защищаемых объектов; **T** - набор угроз; **M** - набор средств обеспечения безопасности; **V** - набор уязвимых мест - отображение **T×O** на набор упорядоченных пар $\mathbf{V_i}=<\mathbf{t_i}\ \mathbf{o_j}>$, представляющих собой пути проникновения в систему; **B** - набор барьеров - отображение **V×M** или **T×O×M** на набор упорядоченных троек $<\mathbf{t_i}\ \mathbf{o_j}\ \mathbf{m_k}>$, представляющих собой точки, в которых требуется осуществлять защиту в системе.

Система защиты является стойкой к деструктивным воздействиям внутреннего нарушителя и гарантирующей передачу тревожных сообщений в том случае, когда на каждый возможный путь проникновения имеется средство защиты. Критерий стойкости: $\forall < \mathbf{t_i}\ \mathbf{o_j} > \in \mathbf{V}, \exists < \mathbf{t_i}\ \mathbf{o_j}\ \mathbf{m_k} > \in B$.

В соответствии с предложенной моделью нарушителя реализовывались следующие угрозы:

- $\mathbf{t_1}$ загрузка ОС с внешних носителей;
- $\mathbf{t_2}$ загрузка ОС в безопасном режиме
- $\mathbf{t_3}$ деструктивное воздействие на физические каналы передачи данных;
- $\mathbf{t_4}$ деструктивное воздействие на сетевое оборудование;
- $\mathbf{t_5}$ атаки типа «отказ в обслуживании».

В качестве объекта рассматривалась вся информация, хранимая на данной ЭВМ. Полученные пути проникновения успешно блокировались средствами разработанного резервного контура управления службы безопасности. Множе-

ство отношений угроза-барьер-объект образует граф, изображенный на рисунке 6.

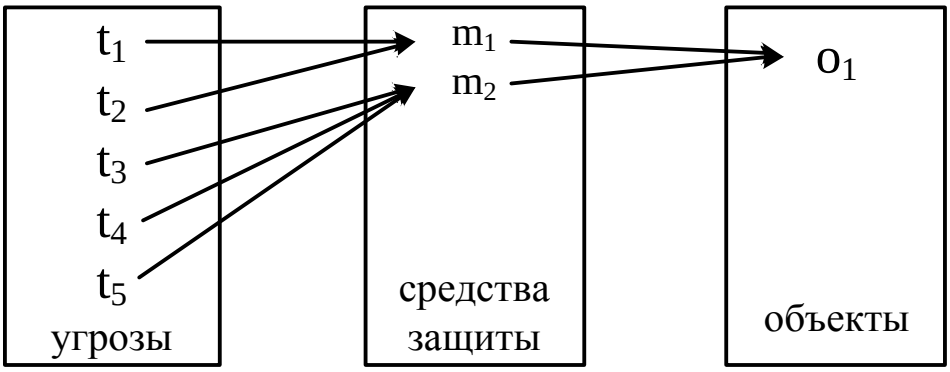


Рисунок 6 — Граф угроза-барьер-объект

Таким образом, в отличие от систем мониторинга, рассмотренных в первой главе, авторская система в результате своего применения, позволяет контролировать загрузку штатной ОС и гарантировать доставку сигналов тревоги в службу безопасности, оставаясь стойкой к деструктивным воздействиям внутреннего нарушителя. В главе приводятся примеры практического применения результатов работы для решения конкретных прикладных задач в трёх проектах.

Элементы разработанного аппаратно-программного комплекса, реализующего систему мониторинга, а именно:

- модуль передачи сообщений по сети электропитания;
- канал передачи сигнала по сети электропитания;
- модуль обработки получаемых сообщений;

были использованы при создании систем оповещения ЗАО «Амулет». При конструировании систем инженерно-технической защиты, для передачи сигналов с устройств прокладываются специальные линии передачи. Предложенные методические основы в рамках концепции передачи сигналов по сети электропитания позволяют не тратить ресурсы на прокладывание новых линий передачи, а использовать штатные, без ущерба надежности систем.

Разработанная методика внедрена в службе безопасности ООО «Еврокорр-2010». При рассмотрении вопроса противодействия обходу имеющейся системы защиты информации от утечки была использована разработанная модель нарушителя и методика противодействия временному отключению системы защиты. Это позволило сократить расходы на защиту одной ЭВМ в 3-5 раз. При дальнейшей эксплуатации новой системы было выявлено несколько попыток загрузки ОС с внешних носителей.

Результаты диссертационной работы использованы на кафедре «Криптология и дискретная математика» НИЯУ МИФИ в рамках учебного курса «Аппаратные средства вычислительной техники». Создана лабораторная работа, позволяющая слушателям курса получить знания о способах защиты информации от утечек в условиях деструктивных воздействий внутреннего нарушителя.

В **заключении** приведены основные результаты диссертационной работы, а также представлены выводы, полученные в ходе выполнения работы.

ОСНОВНЫЕ ВЫВОДЫ И РЕЗУЛЬТАТЫ РАБОТЫ

1. Проведен анализ существующих систем мониторинга для защиты информации от внутреннего нарушителя. Обоснована необходимость создания новой системы мониторинга, использующей сеть электропитания в качестве резервного канала передачи тревожных сообщений.

2. Построена модель нарушителя, осуществляющего несанкционированный съем информации, которая позволила провести анализ возможных способов преодоления системы мониторинга, вследствие чего была обоснована возможность и предложены методические основы в рамках концепции передачи низкочастотных сигналов по сети электропитания.

3. Предложена математическая модель систем мониторинга для защиты информации от внутреннего нарушителя в терминах теории сетей Петри, которая позволяет выявить уязвимости систем мониторинга, влияющие на стойкость к деструктивным воздействиям внутреннего нарушителя.

4. Построена математическая модель функционирования резервного канала передачи сигналов оповещения по сети электропитания ЭВМ, который позволяет обеспечить непрерывность работы контура управления службы безопасности.

5. Разработана методика противодействия работе пользователя на неконтролируемой ЭВМ.

6. Предложена архитектура аппаратно-программного комплекса, реализующего систему мониторинга для защиты от утечки информации. Реализован контур управления службы безопасности, который включает в себя новую систему мониторинга на основе аппаратно-программного комплекса передачи низкочастотных сигналов по сети электропитания ЭВМ.

7. Реализованный аппаратно-программный комплекс использован при создании систем оповещения ЗАО «Амулет». При конструировании систем инженерно-технической защиты, для передачи сигналов с устройств прокладываются специальные линии передачи. Предложенные методические основы в рамках концепции передачи низкочастотных сигналов по сети электропитания позволяют не тратить ресурсы на прокладывание новых линий передачи, а использовать штатные, без ущерба надежности систем.

8. Разработанная методика применена в службе безопасности ООО «Еврокорр-2010». Ее использование позволило сократить расходы на защиту одной ЭВМ в 3-5 раз. При дальнейшей эксплуатации новой системы было выявлено несколько попыток загрузки ОС с внешних носителей.

9. Проведенный анализ систем защиты информации от утечки для случаев отсутствия и присутствия деструктивного воздействия внутреннего нарушителя был использован при создании лабораторных работ учебного курса «Аппаратные средства вычислительной техники» кафедры «Криптология и дискретная математика» НИЯУ МИФИ.

ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

1. Н. П. Лаврентьев, А. В. Мамаев Анализ систем комплексной защиты информации от утечек с целью закрытия возможных уязвимостей. М. БИТ №4 2009 – с. 117-119

2. А. В. Мамаев Повышение надежности систем комплексной защиты информации от внутреннего нарушителя. М. БИТ №1 2011 – с. 111

3. А. В. Мамаев Надежны ли системы комплексной защиты информации от утечек против умышленного инсайда? М. Научная Сессия НИЯУ «МИФИ» Сборник аннотаций. 2011 – с. 163-164

4. А. В. Мамаев Проблема временной потери контроля за ПЭВМ в системах комплексной защиты информации. XIV Международная телекоммуникационная конференция студентов и молодых учёных «Молодёжь и наука». Тезисы докладов. Ч. 3. М.:,НИЯУ МИФИ, 2011 – с. 224

5. А. В. Мамаев Использование низкочастотного активного канала передачи сигналов в системах комплексной защиты информации от утечек. М. БИТ №2 2011г. – с. 83-89

6. А. В. Мамаев Программно-аппаратная реализация низкочастотного активного канала передачи сигналов в системах комплексной защиты информации от утечек. М. БИТ №4 2011 – с. 134-137

7. А. В. Мамаев Использование сети электропитания ЭВМ в качестве резервного канала передачи сигналов оповещения DLP-систем. XV Международная телекоммуникационная конференция студентов и молодых учёных «Молодёжь и наука». Тезисы докладов. Ч. 3. М.:,НИЯУ МИФИ, 2012 – с. 182-183

8. А. В. Мамаев Повышение надежности систем комплексной защиты информации от утечек. М. Научная Сессия НИЯУ «МИФИ» Сборник аннотаций. 2012 – с. 173

Личный вклад автора в работе, написанной в соавторстве, состоит в следующем: [1] — проведение сравнительного анализа систем защиты от утечек.