На правах рукописи

*НАСЫРОВ РАМИЛЬ ИЛЬГИЗОВИЧ*

# МАТЕМАТИЧЕСКИЕ МОДЕЛИ НАДЕЖНОСТИ И ТЕХНИЧЕСКОГО ОБСЛУЖИВАНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

05.13.18 – Математическое моделирование,
численные методы и комплексы программ

**АВТОРЕФЕРАТ**

диссертации на соискание ученой степени
кандидата технических наук

Казань 2008

Работа выполнена в Казанском государственном техническом университете им. А.Н. Туполева

Научный руководитель: доктор технических наук, профессор Глова Виктор Иванович

Официальные оппоненты: доктор технических наук, профессор Захаров Вячеслав Михайлович

доктор технических наук, профессор Латыпов Рустам Хафизович

Ведущая организация: Институт Проблем Информатики Академии Наук Республики Татарстан (ИПИ АН РТ), г. Казань

Защита состоится «31» октября 2008 г. в 15 часов на заседании диссертационного совета Д 212.079.01 в Казанском государственном техническом университете им. А.Н. Туполева по адресу: 420111, г. Казань, ул. К. Маркса, д. 10, зал заседаний Ученого совета.

С диссертацией можно ознакомиться в библиотеке Казанского государственного технического университета им. А.Н. Туполева.

Автореферат разослан «15» сентября



Ученый секретарь
диссертационного совета
доктор физико-математических наук, профессор П.Г. Данилаев

## ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. Важным этапом жизненного цикла сложной системы, в том числе и системы информационной безопасности, является эксплуатация и техническое обслуживание. Под программой эксплуатации системы понимают совокупность взаимосвязанных по месту, времени и содержанию работ для применения ее по назначению. Оптимальная программа эксплуатации заключается в обеспечении наилучшего применения системы по назначению. Причем, эта программа, по существу, является оптимальной программой управления в общей постановке задачи управления.

В настоящее время не разработаны универсальные методики расчета и модели стратегий технического обслуживания и диагностики средств защиты информации. Существующие методы не обеспечивают в полном объеме различные типы воздействия и не учитывают природу взаимодействия атакующего и информационной системы, что делает их неприменимыми для работы в реальных условиях. В то же время, рост сложности информационных систем, наличие в их составе уникального программного обеспечения и участие человека в процессе управления, обработки и передачи информации требует разработки новых методов расчета, моделей надежности и технического обслуживания систем защиты информации.

Таким образом, актуальной задачей является разработка методов оценивания качества средств защиты информации, математических моделей надежности и оптимальных стратегий их технического обслуживания, алгоритмов эффективного функционирования систем информационной безопасности с учетом их вероятностных характеристик. Решению этой задачи посвящена настоящая диссертация.

Объект исследования: надежность и техническое обслуживание систем защиты информации.

Предмет исследования: методы, модели и алгоритмы надежности, диагностики и стратегий технического обслуживания систем защиты информации.

Цель работы: повышение надежности и эффективности функционирования систем защиты информации на основе моделей и алгоритмов технического обслуживания и диагностики с позиций минимального риска.

Научная задача: построение научно-обоснованных моделей надежности, разработка алгоритмов диагностики и оптимальных стратегий технического обслуживания систем информационной безопасности.

Достижение поставленной цели и задачи потребовало решения вопросов:

- построения математических моделей потока отказов и восстановлений системы защиты информации, определения параметров функций распределения и вероятности реализации угрозы информационной безопасности при наличии потока угроз;
- разработки математических моделей технического обслуживания, контроля и диагностики систем информационной безопасности;
- исследования и построения моделей оптимальных стратегий технического обслуживания и управления рисками информационной безопасности;

- разработки методик определения показателей качества технического обслуживания и вопросов приложений математических моделей и алгоритмов к проблеме защиты банковской информации.

Методы исследования. Для решения обозначенных вопросов использованы методы теории надежности, математического моделирования, диагностики и технического обслуживания сложных систем.

Достоверность полученных результатов. Предложенные в диссертационной работе модели и алгоритмы обоснованы теоретическими решениями и не противоречат известным положениям других авторов. Практическая апробация и внедрение в эксплуатацию результатов работы подтвердили эффективность методов диагностики и технического обслуживания систем защиты информации.

Научная новизна работы заключается в следующем:

1) предложены новые математические модели надежности невосстанавливаемых и восстанавливаемых систем в контексте технического обслуживания, контроля и диагностики информационных систем, определены основные вероятностные показатели надежности, позволяющие анализировать эксплуатационные характеристики систем защиты информации;
2) впервые проанализирована модель и алгоритм оптимального управления системой защиты информации, подверженной атакам и обеспечивающей минимальный риск информационной безопасности;
3) разработаны новые математические модели оптимальных стратегий технического обслуживания и контроля систем защиты информации, в которых предусматривается проведение плановых предупредительных профилактик и внеплановых восстановительных работ при появлении каналов несанкционированного доступа к информации;
4) впервые проанализирована стратегия оптимального управления рисками информационной безопасности на основе данных о состоянии системы защиты информации в моменты контроля;
5) разработаны методики определения показателей качества технического обслуживания систем защиты информации, эксплуатируемых в соответствии с оптимальными стратегиями.

Теоретическая значимость работы заключается в разработке:

1) модели, расширяющей возможности получения знаний о характеристиках надежности и технического обслуживания систем защиты информации;
2) алгоритмов, реализующих оптимальные стратегии технического обслуживания систем защиты информации.

Практическая ценность работы заключается в разработке методик анализа надежности, выборе эксплуатационных показателей качества, в разработке инженерных методик реализации оптимальных стратегий технического обслуживания, диагностики и управления рисками систем информационной безопасности.

По проблеме диссертационной работы опубликовано 14 работ, в том числе 2 статьи в журнале из списка, рекомендованного ВАК РФ, 5 статей и 7 тезисов докладов.



С целью апробации основные результаты диссертационной работы докладывались и обсуждались на следующих конференциях: всероссийской (с международным участием) молодежной научной конференции «XI Туполевские чтения»

(Казань, 2003); международной молодежной научной конференции «Туполевские чтения», посвященной 1000-летию города Казани (Казань, 2005); четвертой ежегодной международной научно-практической конференции «Инфокоммуникационные технологии глобального информационного общества» (Казань, 2006); международной молодежной научной конференции «XIV Туполевские чтения» (Казань, 2006); десятом юбилейном молодежном международном форуме «Радиоэлектроника и молодежь в XXI ст.» (Харьков, 2006); пятой ежегодной международной научно-практической конференции «Инфокоммуникационные технологии глобального информационного общества» (Казань, 2007); международной молодежной научной конференции «XV Туполевские чтения» (Казань, 2007); всероссийской научной конференции «Информационные технологии в науке, образовании и производстве» (Казань, 2007).

Реализация результатов работы. Результаты исследования:

- прошли успешную апробацию в Департаменте информационных технологий ОАО «АК БАРС» БАНК и внедрены в промышленную эксплуатацию для мониторинга и расследования инцидентов информационной безопасности локальной вычислительной сети банка.
- прошли успешную апробацию в ООО КБЭР «Банк Казани» и внедрены в промышленную эксплуатацию.
- внедрены в учебный процесс Казанского государственного технического университета им. А.Н.Туполева и используются при изучении материалов дисциплин «Комплексные системы защиты информации» и «Организационное обеспечение систем защиты информации» для специальностей: 090103 – «Организация и технология защиты информации», 090104 – «Комплексная защита объектов информатизации» и 090106 – «Информационная безопасность телекоммуникационных систем».

Пути дальнейшей реализации. Разработанные модели надежности систем защиты информации, оптимальных стратегий их технического обслуживания и управления рисками информационной безопасности планируется использовать в системах защиты информации вычислительных сетей предприятий для повышения их эффективности.

На защиту выносятся следующие результаты:

- математические модели надежности, эксплуатации, технического обслуживания и контроля восстанавливаемых и невосстанавливаемых систем защиты информации;
- модели и алгоритм оптимального управления системой защиты информации, обеспечивающие минимальный риск информационной безопасности;
- математические модели оптимальных стратегий технического обслуживания и контроля систем защиты информации, стратегий оптимального управления рисками информационной безопасности на основе данных о состоянии системы защиты информации в моменты контроля;
- инженерные методики определения показателей качества технического обслуживания систем защиты информации, эксплуатируемых в соответствии с оптимальными стратегиями.

Структура и объем диссертации. Диссертация изложена на 162 страницах машинописного текста, содержит 21 рисунок, 3 таблицы, состоит из введения, че-

тырех глав, заключения, списка использованной литературы из 101 наименований на 10 страницах.

Сведения о личном вкладе автора. Разработаны математические модели надежности в контексте диагностики и технического обслуживания систем защиты информации, определены основные параметры надежности, предложены модели и алгоритмы оптимального управления рисками информационной безопасности, реализованы модели и алгоритмы оптимальных стратегий технического обслуживания при появлении каналов несанкционированного доступа к информации, проведены прикладные исследования для оценки эффективности разработанных моделей и алгоритмов при решении практических задач.

На основе разработанных моделей и алгоритмов предложены методики для мониторинга и расследования инцидентов информационной безопасности локальной вычислительной сети банка с использованием системы CS MARS, методики для определения показателей качества технического обслуживания и управления рисками системы защиты информации локальной вычислительной сети банка, эксплуатируемой в соответствии с предложенными стратегиями.

## СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность темы проводимых исследований, сформулирована цель работы, приведена структура диссертации.

В первой главе рассматриваются общие вопросы надежности и технического обслуживания систем защиты информации (СЗИ). Анализируются математические модели функционирования данных систем с позиций теории надежности, рассмотрены стохастические марковские и полумарковские модели эффективности, приводятся оценки надежности и среднего времени безотказного функционирования исследуемой системы. Показано, что использование вероятностного подхода позволяет оценить средний риск принимаемого системой решения в процессе ее эксплуатации. Показано, что хотя надежность системы защиты информации закладывается уже на этапе ее проектирования, тем не менее, даже в условиях оптимального проектирования фаза эксплуатации и технического обслуживания остается весьма сложной и трудно прогнозируемой. Доказывается необходимость разработки вероятностных моделей, алгоритмов и стратегий технического обслуживания, в том числе оптимальных, обеспечивающих на этапе эксплуатации выполнение поставленных перед системой защиты задач. Ставится задача по разработке моделей и алгоритмов технического обслуживания и диагностики СЗИ.

Под надежностью СЗИ понимается ее свойство безотказно выполнять возложенные на нее функции в течение заданного промежутка времени. Хотя отказ любой технической системы – это случайное событие, приводящее к невозможности выполнения системой возложенных на нее функций, в системах защиты информации с отказом связан не только переход системы в состояние неработоспособности, но и обнаружение в ней уязвимости, приводящей к возможности несанкционированного доступа (НСД) к информации.

С отказами системы защиты информации связаны такие понятия, как интенсивность отказов $\lambda$ (среднее число отказов в единицу времени) и среднее время восстановления системы защиты после отказа $T_в$.

В течение всего времени восстановления систему защиты информации можно считать отказавшей, а защищаемый объект незащищенным.

Под интенсивностью восстановления системы защиты после отказа понимают интенсивность устранения в ней уязвимостей в единицу времени.

$$\mu = 1/T_в$$

Для увеличения надежности встроенной СЗИ применяется резервирование, т.е. включение в ее состав добавочных механизмов защиты. Резервирование должно использоваться при построении эффективной СЗИ.

Под эффективностью СЗИ понимается степень соответствия результатов защиты информации поставленной цели. Для количественной оценки эффективности необходимо решать задачу многокритериальной оптимизации.

Пусть $Z$ – защищенность системы:

$$Z = f(C_{инф}, P_{взл}, Ц_{СЗИ}, П),$$

где $C_{инф}$ – стоимость защищаемой информации;

$P_{взл}$ – вероятность взлома;

$Ц_{СЗИ}$ – стоимость СЗИ;

$П$ – производительность системы.

Тогда задача оптимизации состоит в обеспечении максимального уровня защищенности информации при минимальной стоимости системы защиты и минимальном влиянии ее на производительность системы:

$$Z^{opt} = maxZ(C_{инф}, P_{взл}, Ц_{СЗИ}, П).$$

В качестве основного критерия защищенности используется коэффициент защищенности $D$, показывающий относительное уменьшение риска в защищенной системе по сравнению с незащищенной системой:

$$D = \left(1 - \frac{R_{защ}}{R_{нез}}\right) \times 100\%,$$

где $R_{защ}$ – риск в защищенной системе;

$R_{нез}$ – риск в незащищенной системе.

Функционирование СЗИ можно рассматривать, как марковский процесс, характеризующийся конечным множеством возможных состояний и переходами системы защиты из одного состояния в другое, однозначно определяющих состояние системы в каждый момент времени.

Пусть имеем следующее множество состояний СЗИ:

$S_1$ – нет запросов на реализацию функции защиты от НСД, средство защиты информации от НСД работоспособно и решает тест-задачу;

$S_2$ – нет запросов, СЗИ отказало и находится на восстановлении;

$S_3$ – нет запросов, СЗИ отказало, решается тест-задача, отказ не обнаружен;

$S_4$ – отрабатывается поступивший запрос на работоспособном СЗИ;

$S_5$ – отрабатывается поступивший запрос на реализацию функции защиты информации от НСД на отказавшем техническом СЗИ;

$S_6$ – есть запрос, но отказавшее СЗИ находится на восстановлении.

Тогда граф переходов модели можно представить, как показано рисунке 1.

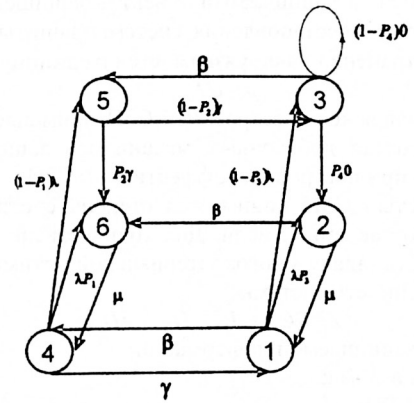


Рис. 1. Граф переходов технического средства защиты информации от несанкционированного доступа

В рамках данной модели надежность реализации функции системы защиты информации от НСД рассчитывается по формуле:

$$D = \frac{\Delta_4 p_{41}}{\Delta_4 p_{41} + \Delta_5 p_{53}}.$$

Оценка надежности позволяет осуществить сравнение различных вариантов построения системы защиты информации и выбрать лучший из них.

Для оценки эффективности СЗИ можно также использовать вероятностный подход, который позволяет еще на стадии проектирования прогнозировать средний риск принимаемого системой решения:

$$R=P(A_{10})\times r_{10}+P(A_{01})\times r_{01}=P(1-P_d)\times r_{10}+(1-P)P_{\text{|}}\times r_{01},$$

где $P(A_{10})$ – вероятность события, когда система выдает решение “информации нет” при наличии на ее входе достоверной информации;

$P(A_{01})$ – вероятность события, когда система выдает решение “информация есть” при отсутствии на ее входе достоверной информации;

$P$ – вероятность наличия достоверной информации на входе системы;

$P_d$ – вероятность принятия системой правильного решения;

$P_{\text{|}}$ - вероятность принятия системой неправильного решения, соответствующая событиям $A_{10}$ и $A_{01}$;

$r_{10}$ и $r_{01}$ – стоимость принятия системой решений, соответствующих событиям $A_{10}$ и $A_{01}$.

Выбор величин $r_{10}$ и $r_{01}$ производится с помощью экспертных методов.

Важнейший этап жизненного цикла информационных систем, в том числе СЗИ – эксплуатация и техническое обслуживание. Наличие квалифицированного технического обслуживания на этапе эксплуатации информационной системы является необходимым условием для исполнения поставленных перед ней задач. Обеспечение защиты информации происходит в условиях случайного воздействия самых разных факторов. Оценка эффективности защиты должна обязательно учитывать как объективные обстоятельства, так и вероятностные факторы.

Эти причины актуализируют необходимость разработки методов, моделей, алгоритмов и реализующих их программных комплексов автоматизированного мониторинга и формирования данных для реализации оптимальных стратегий технического обслуживания и контроля системы защиты с позиций минимального риска. В основу диссертационной работы положены фундаментальные понятия и положения теории надежности и эффективности систем защиты информации, непосредственно связанной с другими системными свойствами, в том числе качеством, надежностью, управляемостью, помехозащищенностью, устойчивостью.

Во второй главе описываются модели процессов функционирования систем защиты информации. В качестве характеристики, как способности системы защиты отражать атаки на информационную систему, вводится понятие порога, определяющего прочность преграды и длительность ее преодоления. Показывается, что вероятность обнаружения в системе защиты уязвимостей при наличии порогового уровня определяется вероятностью перехода и временем жизни системы в надпороговом состоянии. Для моделей многоуровневых и многозвенных защит вычисляются вероятности отказов и восстановлений систем в единицу времени, как вероятности переходов в единицу времени в надпороговое и подпороговое состояния. Определяются вероятности реализации угрозы информационной безопасности при наличии потока угроз. Рассматриваются вопросы оптимального управления системой защиты информации, обеспечивающего минимальный ущерб информационной системе.

При оценке возможности реализации угроз информационной безопасности (ИБ) пользуются подходом, основанным на введении моделей многозвенных и многоуровневых защит.

Модель многозвенной защиты представлена на рисунке 2.

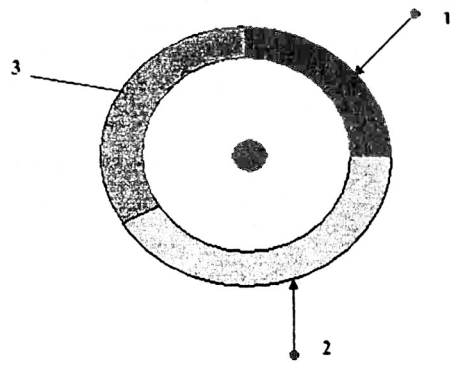


Рис. 2. Модель многозвенной защиты

Выражение для оценки прочности многозвенной защиты:

$$P_{СЗИ} = \min\{P_{СЗИ_1},...,P_{СЗИ_k}\},$$

где $P_{СЗИ_j}$ – прочность $j$-й преграды.

Модель многоуровневой защиты представлена на рисунке 3.

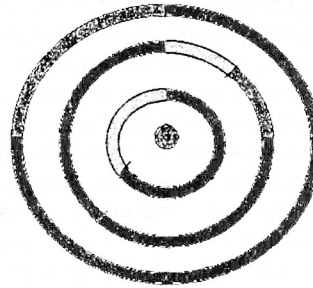

Рис. 3. Модель многоуровневой защиты

Суммарная прочность дублирующих преград определяется по формуле:

$$P_{\Sigma} = 1 - \prod_{i=1}^{m} \left(1 - P_{CЗИ}^{i}\right),$$

где $i$ – порядковый номер преграды;

$m$ – количество дублирующих преград;

$P_{CЗИ_i}$ – прочность $i$-той преграды.

Введение порога позволяет ввести два важнейших параметра, характеризующих систему защиты информации – интенсивность отказов λ и интенсивность восстановлений μ. Показано, что основные характеристики надежности системы защиты информации выражаются через параметры λ и μ. Поэтому найдены в явном виде выражения для параметров экспоненциальной функции распределения длительности выброса случайного процесса за заданный уровень (длительность восстановления), а также функции распределения длительности между соседними выбросами (длительность безотказной работы). Для вычисления вероятности λ и μ использовался метод ансамблей и предполагалось, что в стационарных условиях потоки отказов и восстановлений системы защиты совпадают. Выражение для оценки прочности многозвенной защиты с позиций надежности определяет вероятность безотказной работы и имеет вид:

$$\mathrm{P}_{\tilde{N}\zeta\dot{E}} \approx \prod_{i=1}^{k} \frac{\mu_i}{\lambda_i + \mu_i},$$

где

$$\lambda_i = \omega_{0i} e^{-\frac{u_i^2}{2}} \left[\frac{1}{2}\Phi(u_i)\right]^{-1}; \quad \mu_i = \omega_{0i} e^{\frac{u_i^2}{2}} \left[1 - \frac{1}{2}\Phi(u_i)\right]^{-1},$$

$$u_i = \frac{a_i}{\sigma_i^2}; \qquad \Phi(u) = \sqrt{\frac{2}{\pi}} * \int_{u}^{\infty} e^{-\frac{u^2}{2}} du.$$

В многоуровневой системе защиты дублирующие преграды соединены параллельно в смысле надежности и тогда отказ системы наступает в случае, когда отказывают все входящие в систему элементы. В частотности, когда все дублирующие уровни равнонадежны:

$$Q_{\Sigma} = 1 - P_{\Sigma} = \prod_{i=1}^{m} \left(1 - P_{СЗИ'}\right) = \left(1 - P_{СЗИ}\right)^{m}.$$

Найдены выражения для вероятностей реализации угрозы ИБ при наличии потока угроз. Определены рекуррентные соотношения, позволяющие, при необходимости, определить число систем ансамбля, которые за время $t$ интересующее число раз пересекли порог (подверглись атаке определенное число раз):

$$n_{k+1} = e^{-\mu t} \int_0^t e^{\mu t} \lambda p_k(t) dt; p_{k+1} = e^{-\lambda t} \int_0^t e^{\lambda t} \mu n_k(t) dt,$$

причем

$$n_0(t) = n_r e^{-\mu t}; p_0(t) = p_r e^{-\lambda t};$$

При условии, что для потоков выполняются соотношения $\mu n_k(t) = \lambda p_k(t)$, для любого номера $k$ и момента времени $t$, в явном виде находим:

$$p_{k+1}(t) = e^{-\lambda t} \int_0^t e^{\lambda t} \lambda p_k(t) dt = e^{-\lambda t} \int_0^t \lambda^{k+1} \frac{t^k}{k!} p_r dt = e^{-\lambda t} \frac{\lambda^{k+1} t^{k+1}}{(k+1)!} p_r.$$

Вероятности $F_k$ нахождения системы в надпороговой области за время наблюдения $t$ не менее $k$ раз определяются из выражения:

$$F_k = 1 - \sum_{j=0}^{k-1} \frac{(\lambda t)^j}{j!} e^{-\lambda t}.$$

Проанализировано поведение систем защиты информации во времени и их временная селекция, когда система защиты не только перейдет в надпороговое состояние, но и продержится там непрерывно некоторое время $\tau$, которое заранее определено и зафиксировано.

Такой подход может оказаться полезным для многозвенных и многоуровневых защит, способных обнаруживать и блокировать несанкционированный доступ (контролируемые преграды).

Уравнение «сохранения» для стационарной возрастной плотности надпороговых систем имеет вид:

$$\mu(\tau)\rho(\tau) + d\rho(\tau)/d\tau = 0.$$

Его решением служит выражение:

$$\rho(\tau) = V_r \times \exp(-\int_0^{\tau} \mu(\tau) d\tau),$$

где $\rho(\tau)$ – плотность распределения числа систем в надпороговом состоянии по возрасту, $\mu(\tau)$ – вероятность перехода системы в единицу времени (интенсивность восстановления) из надпорогового состояния в подпороговое, $V_r$ – поток по различным возрастным группам:

$$V_r = \int_0^{\infty} \mu(\tau)\rho(\tau) d\tau.$$

Получено выражение для функции распределения $f(\tau)$ длительности пребывания системы над заданным уровнем в зависимости от вероятности перехода $\mu(\tau)$, которое имеет вид:

$$f(\tau)=\mu(\tau)\exp\left(-\int_0^{\tau}\mu(\tau)d\tau\right).$$

Совокупность рассмотренных выше моделей позволяет в значительной мере охватить проблемы оценки возможности реализации угроз ИБ.

Фундаментальной проблемой информационной безопасности является определение баланса между стоимостью и эффективностью СЗИ с точки зрения пользователя. Предполагается, что существует область экономически оптимальных СЗИ, обеспечивающих наименьший риск собственника информации. В качестве меры риска понимаются ожидаемые суммарные потери в процессе защиты информации в течение определенного периода времени.

Рассмотрена модель функционирования системы защиты информации, подверженной отказам и проанализирован алгоритм оптимального управления такой системой, обеспечивающий минимальный ущерб. Предполагается, что информационная система характеризуется рисками интенсивности $r(t)$ и может отказывать с интенсивностью $h(t)$. После отказа система больше не используется. В процессе эксплуатации в систему можно вкладывать средства с интенсивностью $p(t)$, в результате чего интенсивность отказов становится равной $h_p(t)=\psi(p(t))*h(t)$, где $\psi$ – убывающая выпуклая функция, причем $\psi(0)=1$. Требуется найти управление $p(t)$, минимизирующее риск информационной системы.

Для решения поставленной задачи требуется минимизировать функционал:

$$J=\int_0^{\infty}\left(r(t)-R[p(t)]\right)e^{-\delta t}S_p(t)dt,$$

где

$$S_p(t)=\exp\left\{-\int_0^{t}h_p(u)du\right\}.$$

Эта задача решается с помощью принципа максимума Понтрягина. Оптимальное управление СЗИ, обеспечивающее минимальное значение риска, описывается ключевым уравнением:

$$\frac{dp}{dt}=\frac{R'(p)\psi'(p)h(t)\left[\delta+\psi(p)h(t)\right]+R'(p)\psi'(p)h'(t)+\left[\psi(p)h(t)\right]\left[\psi(t)-R(p)\right]}{R''(p)\psi'(p)h(t)-R'(p)\psi''(p)h(t)}.$$

Решение этого уравнения дает оптимальное управление, если оно существует. Проанализированы решения этого уравнения для частных случаев.

В третьей главе исследуются стратегии технического обслуживания, контроля и диагностики систем защиты информации на основе введенных показателей качества их функционирования Вводится понятие оптимальной стратегии, обеспечивающей экстремальные значения показателей качества. Анализируются различные варианты стратегий по «наработке» и состоянию. Предлагаются алгоритмы контроля и диагностики системы защиты на основе эволюции вектора состояния системы в фазовом пространстве. Доказывается, что рационально организованное профилактическое обслуживание является одним из основных средств повышения надежности систем защиты информации в процессе их эксплуатации.

Рассмотрена стратегия, в которой полное восстановление системы защиты информации проводится только после самостоятельного проявления отказа. В этой стратегии состояние системы описывается регенерирующим случайным процессом x(t), состояние которого изменяется детерминировано, причем, моменты перехода из состояний $E_2$ (аварийно-профилактические работы) и $E_1$ (простой системы в состоянии отказа) в состояние $E_0$ (исправное состояние) являются для процесса моментами регенерации.

Здесь проводятся только внеплановые аварийно-профилактические работы в результате обнаружения каналов утечки информации. Обнаружение таких каналов и их индикация происходит через некоторое случайное время, распределенное по закону Ф(x). Система новая в момент t=0, работает до отказа (до взлома СЗИ или иного сбоя в ее работе) в течение случайного времени, распределенного по закону F(x). Далее, от момента появления отказа до его проявления СЗИ в течение случайного времени не выполняет возложенных на нее функций, происходит утечка информации. В случайный момент времени начинается профилактический ремонт и восстановление СЗИ, который длится случайное время, после которого СЗИ полностью обновляется. По окончании восстановительных работ весь процесс функционирования системы и ее обслуживания полностью повторяется. Для этой стратегии технического обслуживания СЗИ определены:

- средняя длительность периода между точками регенерации:

$$M\widetilde{X} = \sum_{l=0}^{2} MX^{(n)} = T_0 + T_n + T_{\grave{a}\ddot{i}};$$

- коэффициент готовности:

$$K_{\tilde{A}} = \frac{MX^{(0)}}{M\widetilde{X}} = \frac{T_0}{T_0 + T_n + T_{\grave{a}\ddot{i}}};$$

- удельные потери в единицу времени безотказной работы:

$$C = \frac{1}{T_0}\left(c_n T_n + c_{an} T_{an}\right),$$

где $c_n$ – потери в единицу времени в результате появления каналов НСД;
$c_{an}$ – потери в единицу времени, связанные с восстановлением СЗИ;
$T_n$ – среднее время простоя системы в нерабочем состоянии;
$T_{an}$ – средняя длительность аварийно-профилактического ремонта;
$T_o$ – среднее время безотказной работы системы.

При эксплуатации СЗИ по данной стратегии необходимо учитывать, что:

- в системе не проводятся предупредительные восстановительные работы, поэтому, задача ограничивается только получением численных значений показателей качества;
- для определения коэффициентов готовности и стоимостных потерь достаточно знать только средние характеристики, в частности, среднее время безотказной работы;
- если утечка информации проявляется мгновенно, необходимо считать $T_n=0$; если появившиеся каналы НСД самостоятельно не обнаруживаются ($T_n=\infty$), то такую систему эксплуатировать с использованием рассмотренной стратегии нельзя, так как в этом случае $K_Г=0$ и $C=\infty$.

Проанализирована стратегия, в которой полное восстановление СЗИ проводится либо в моменты появления канала НСД, либо в заранее назначенный календарный момент времени. Здесь в СЗИ возможно проведение плановых предупредительных профилактических и внеплановых аварийно-профилактических работ при появлении каналов НСД. Предполагалось, что индикация утечки информации по каналам НСД или отказ СЗИ происходит мгновенно. Вектор состояния x(t) регенерирующего случайного процесса может принимать значения $E_0$ (СЗИ работоспособна), $E_1$ (произошла утечка информации и проводится внеплановое восстановление СЗИ), $E_2$ (проводится плановая профилактика СЗИ).

Коэффициент готовности СЗИ:

$$K_{\hat{A}}(\tau) = \frac{\int_0^{\tau} \overline{F}(x)dx}{M\widetilde{X}} = \frac{\int_0^{\tau} \overline{F}(x)dx}{\int_0^{\tau} \overline{F}(x) + T_{nn}\overline{F}(\tau) + T_{an}F(\tau)}.$$

Здесь в числителе выражения стоит среднее время безотказной работы системы за период между соседними точками регенерации процесса x(t), а в знаменателе – средняя длительность этого периода.

Средние удельные затраты на обслуживание СЗИ:

$$C(\tau) = \frac{c_{nn}T_{nn}\overline{F}(\tau) + c_{an}T_{an}F(\tau)}{\int_0^{\tau} \overline{F}(x)dx}.$$

Даная величина равна отношению средних затрат за период между точками регенерации к среднему времени безотказной работы СЗИ за этот период.

Рассмотренная стратегия может быть использована только для систем, в которых происходит мгновенное обнаружение взлома СЗИ или мгновенная индикация появления каналов НСД к информации.

Исследована стратегия, в которой полное восстановление СЗИ проводится только в заранее назначенные календарные моменты времени независимо от отказов системы. Данная стратегия применима к информационным системам, в том числе к СЗИ, для которых невозможно обнаружить отказ в момент его появления и, следовательно, невозможно мгновенно начать восстановительные работы. Для таких систем необходимо предусматривать проведение плановых восстановительных работ. Случайный процесс x(t) принимает значения $E_0$ (система работоспособна), $E_1$ (система неработоспособна и простаивает в состоянии отказа), $E_2$ (проводится плановый аварийно-профилактический ремонт), $E_3$ (проводится плановая профилактика). Тогда коэффициент готовности:

$$K_{\hat{A}} = \frac{\int_0^{\tau} \overline{F}(x)dx}{\tau + T_{nn} + (T_{an} - T_{nn})F(x)}.$$

Средние удельные затраты за единицу времени работы СЗИ:

$$C(\tau)=\frac{c_n\int_0^{\tau}F(x)dx+c_{nn}T_{nn}+(c_{nn}T_{nn}-c_{an}T_{an})F(\tau)}{\int_0^{\tau}\overline{F}(x)dx},$$

где $c_n$ – потери за единицу времени проведения предупредительной профилактики СЗИ;

$c_{an}$ – потери за единицу времени проведения планового аварийно профилактического ремонта СЗИ.

Рассматриваемая стратегия может быть использована только для систем, в которых нет самостоятельной индикации о взломе СЗИ и появлении каналов НСД. Истинное состояние СЗИ становится известным только через некоторое время после начала профилактических восстановительных работ.

При реализации политики ИБ предприятия большое значение уделяется анализу и управлению рисками, как вероятностным процессом. Управляющее воздействие на СЗИ должно осуществляться либо в соответствии с программой эксплуатации, которую составляют заранее, исходя из априорных сведений о системе, либо в виде так называемой позиционной стратегии, соответствующей управлению состоянием СЗИ (а, следовательно, и рисками ИБ) по принципу обратной связи. В последнем случае управляющее воздействие на СЗИ формируется апостериорно на основании дополнительной информации о состоянии системы, которая становится известной при измерении параметров ее состояния в процессе эксплуатации. Проблема снижения рисков достигается выбором оптимальных стратегий эксплуатации и обслуживания системы защиты информации.

В произвольный момент времени $t$ состояние системы может быть описано вектором $\vec{X}(t)$. Пусть $A=\{A_1, A_2, A_3\}$ – множество состояний системы:

$A_1$ – подобласть, в которой СЗИ способна выполнять возложенные на нее функции с заданным уровнем эффективности без проведения восстановительных работ или работ по техническому обслуживанию;

$A_2$ – подобласть, в которой СЗИ еще способна выполнять задачу с заданным уровнем эффективности, но должна пройти техническое обслуживание и быть возвращена в начальное состояние;

$A_3$ – подобласть, в которой СЗИ не может выполнять стоящую перед ней задачу с заданной эффективностью.

Выбор стратегии обслуживания СЗИ полностью определяется разбиением области $A$ на три непересекающихся подобласти $A_1$, $A_2$, $A_3$, при попадании в которые принимается решение о продолжении наблюдения, проведении предупредительной профилактики или аварийно-профилактического ремонта. Задача сводится к определению таких областей $A_1^*$, $A_2^*$, $A_3^*$ ($A_1^* \cup A_2^* \cup A_3^* = A$) для которых достигается минимум средних удельных затрат и, как следствие, минимум риска информационной безопасности.

Оптимальное разбиение ($A_1^*$, $A_2^*$, $A_3^*$) основано на использовании леммы Дуба. Оптимальное правило остановки (нахождение оптимальной границы между областями $A_1$ и $A_2$) определяется неравенством:

$$P\left\{\left\{\vec{X}(t_k),t_k\right\}\in A_3 / \left[\left\{\vec{X}(t_i),t_i\right\}, i=\overline{0,k-1}\right]\right\}\le \frac{C_1}{(C_2-C_1)(k-1)},$$

где $C_1$ – средние затраты на проверку системы; затраты $C_2$ связанны с невыполнением СЗИ задачи (при $\bar{X}(t) \in \dot{A}_3$) и появлением уязвимости, потерей (утечкой) информации через каналы НСД, внесением исправлений в ПО и восстановлением самой СЗИ.

Очевидно, всегда $C_2 > C_1$. Любая точка $\{\bar{X}(t_{k-1}), t_{k-1}\}$, для которой выполняется данное неравенство, принадлежит области $A_1$.

Работоспособность приведенного алгоритма проиллюстрирована на примере систем защиты информации с избыточностью.

В процессе технического обслуживания наиболее сложной является задача диагностики системы защиты информации. Рассматриваемые в диссертации методы контроля и диагностики позволяют увеличить число обнаруживаемых каналов несанкционированного доступа к информации и создать методы экспресс диагностики СЗИ. В предлагаемых алгоритмах контроля и диагностики работоспособность СЗИ контролируется постоянно с помощью аппаратно-программных средств встроенного контроля. Из-за уменьшения числа измеряемых параметров и времени на их обработку появляются возможности проведения более оперативной экспресс диагностики состояния объектов.

В четвертой главе рассматриваются практические вопросы функционирования и технического обслуживания информационной банковской сети и системы ее защиты. Показывается, что средства и методы защиты информации представляют собой систему мер, предназначенную для предотвращения возможности перехвата и искажения информации посредством совокупности известных и потенциально возможных каналов несанкционированного доступа. Анализируются требования стандарта банка России по обеспечению информационной безопасности и методы их реализации. Рассматривается мониторинг и расследование инцидентов информационной безопасности локальной вычислительной сети банка на основе системы CS MARS, предназначенной для управления угрозами информационной безопасности. В качестве источников информации могут выступать сетевое оборудование (маршрутизаторы и коммутаторы), средства защиты (межсетевые экраны, антивирусы, системы обнаружения атак и сканеры безопасности), журналы регистрации ОС (Solaris, Windows NT, 2000 2003, Linux) и приложений (СУБД, Web), а также сетевой трафик инцидентов информационной безопасности, регистрируемых сенсорами CS MARS.

Проведен анализ распределения инцидентов, зарегистрированных сенсорами IDS CS MARS по различным временным интервалам: в течение года, месяца и дня. Показано, что основными зарегистрированными атаками были:

1. Парольные атаки. Тип – попытка. К данной категории инцидентов относятся попытки извлечения системных паролей, массовые ошибки при попытках подключится к системе через сервис «telnet», SSH, в терминальном режиме. Случай, когда пользователь забыл/утерял свои идентификационные данные/пароль и пытался методом подбора войти в систему, расцениваются, как инцидент.
2. Направленное сканирование. К данной категории инцидентов относятся попытки целевого сканирования хостов, идентификации текущих сессий пользователей, попытки идентифицировать сервисы, открытые порты и т.д.

3. Атаки, направленные на RPC. Переполнение буфера, превышение полномочий, удаленное выполнение команд, организация атак на сервис типа «отказ в обслуживании».
4. Парольные атаки. Тип – подозрение на успешную реализацию. Успешное получение прав системного/доменного администратора с последующим извлечением/изменением паролей более низкого уровня.
5. Атаки категории «Отказ в обслуживании».
6. Атаки на почтовые сервисы.
7. Распространение червей через сервисы SMTP, TFTP.

Эффективное решение задач мониторинга событий в системе CS MARS в условиях большого количества регистрируемых инцидентов, а также способность агрегировать информацию систем обнаружения вторжений позволяет собрать необходимый статистический материал для реализации оптимальных стратегий технического обслуживания систем защиты информации и разработки методик определения показателей качества данных систем.

В заключение главы приведены методики определения показателей качества технического обслуживания систем защиты информации, эксплуатируемых по стратегиям, исследованным в предыдущей главе.

## ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

1) Предложены математические модели надежности невосстанавливаемых и восстанавливаемых систем в контексте технического обслуживания, контроля и диагностики информационных систем.
2) Определены основные вероятностные показатели надежности, позволяющие анализировать эксплуатационные характеристики систем обеспечения информационной безопасности.
3) Разработаны модель и алгоритм оптимального управления системой защиты информации, подверженной атакам и обеспечивающей минимальный риск информационной безопасности.
4) Разработаны математические модели оптимальных стратегий технического обслуживания и контроля систем защиты информации, в которых предусматривается проведение плановых предупредительных профилактик и внеплановых восстановительных работ при появлении каналов несанкционированного доступа к информации.
5) Проанализирована стратегия оптимального управления рисками информационной безопасности на основе данных о состоянии системы защиты информации в моменты контроля.
6) Разработаны методики определения показателей качества технического обслуживания систем защиты информации, эксплуатируемых в соответствии с оптимальными стратегиями.

## ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

1. *Глова В.И., Насыров Р.И.* Показатели качества функционирования и стратегии обслуживания систем защиты информации // Вестник КГТУ им. А.Н. Туполева, №4, 2006. – С. 39-43.

2. *Насыров Р.И., Глова В.И.* Стратегии управления рисками на основе информации о состоянии системы защиты с избыточностью // Вестник КГТУ им. А.Н. Туполева, №2, 2007. – С. 59-64.
3. *Насыров Р.И.* Моделирование потока отказов и восстановлений системы защиты информации при обнаружении каналов несанкционированного доступа к информации // Инфокоммуникационные технологии глобального информационного общества: Сб. трудов 4-й ежегодной междунар. научно-практ. конференции. Казань, 2006. – С. 225-238.
4. *Насыров Р.И., Глова В.И.* Управление рисками информационной безопасности на основе оптимальных стратегий технического обслуживания системы защиты информации // Инфокоммуникационные технологии глобального информационного общества: тезисы докладов 4-й ежегодной междунар. научно-практ. конференции, Казань, 2006. – С. 240-243.
5. *Насыров Р.И., Глова В.И.* Контроль и диагностика системы защиты информации на основе эволюции вектора состояния в фазовом пространстве // Инфокоммуникационные технологии глобального информационного общества: тезисы докладов 4-й ежегодной междунар. научно-практ. конференции, Казань, 2006. – С. 243-246.
6. *Насыров Р.И., Глова В.И.* Определение вероятности реализации угрозы информационной безопасности при наличии потока угроз // Инфокоммуникационные технологии глобального информационного общества: тезисы докладов 5-й ежегодной междунар. научно-практ. конференции. Казань, 2007. – С. 53-55.
7. *Насыров Р.И.* Оптимальное управление рисками информационной безопасности // Инфокоммуникационные технологии глобального информационного общества: Сб. трудов 5-й ежегодной междунар. научно-практ. конференции. Казань, 2007. – С. 181-187.
8. *Насыров Р.И.* Активный аудит безопасности восстанавливаемых информационных систем с использованием методов и моделей надежности // XI Туполевские чтения: тезисы докладов всероссийской (с междунар. участием) молодежной научной конференции. Казань, 2003. – С. 78-79.
9. *Насыров Р.И.* Оценка комплексных показателей надежности систем защиты информации // Туполевские чтения: Международная молодежная научная конференция, посвященная 1000-летию города Казани: Материалы конференции. Казань, 2005. – С. 91-93.
10. *Насыров Р.И.* Контроль и диагностика состояния системы защиты информации на основе фрактальной размерности и корреляционного интеграла // XIV Туполевские чтения: международная молодежная научная конференция: Материалы конференции. Казань, 2006. – С. 86-87.
11. *Насыров Р.И.* Диагностика состояния системы защиты информации на основе энтропии Колмогорова // XIV Туполевские чтения: международная молодежная научная конференция: Материалы конференции. Казань, 2006. – С. 83-85.

12. *Насыров Р.И.* Определение параметров функций распределения длительностей наработки на отказ и восстановление // XV Туполевские чтения: международная молодежная научная конференция: Материалы конференции. Казань, 2007. – С. 95-96.
13. *Насыров Р.И.* Оптимальное управление системой защиты информации без восстановления (модель I) // Информационные технологии в науке, образовании и производстве: Матер. Всеросс. научной конф. Казань, 2007. – С. 509-511.
14. *Насыров Р.И.* Оптимальное управление системой защиты информации с восстановлением (модель II) // Информационные технологии в науке, образовании и производстве: Матер. Всеросс. научной конф. Казань, 2007. – С. 490-492.

Формат 60×84 1/16. Бумага офсетная. Печать офсетная.
Печ. л. 1,0. Усл. печ. л. 0,93. Усл. кр.-отт. 0,98. Уч. изд. л. 1,0.
Тираж 100. Заказ Л123.

Типография Издательства Казанского государственного
технического университета
420111, Казань, К. Маркса, 10