На правах рукописи

Сильнов Дмитрий Сергеевич

РАЗРАБОТКА И ИССЛЕДОВАНИЕ ПРОГРАММНЫХ МЕТОДОВ И СРЕДСТВ ЗАЩИТЫ СИСТЕМ УДАЛЕННОГО МОНИТОРИНГА

05.13.11 – математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей

05.13.19 – методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Автор: 

Москва – 2011

Работа выполнена в Национальном исследовательском ядерном университете «МИФИ»

Научный руководитель: кандидат технических наук, доцент ВАСИЛЬЕВ Николай Петрович

Официальные оппоненты: доктор технических наук, профессор МИНАЕВ Владимир Александрович, НОУ ВПО Российский новый университет

кандидат технических наук КОСЫХ Петр Александрович, ООО «Фактор-ТС»

Ведущая организация: ФАУ «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю» (ГНИИИ ПТЗИ ФСТЭК России)

Защита диссертации состоится 21 марта 2012 г. в 15^{00} на заседании диссертационного совета Д 212.130.03 при Национальном исследовательском ядерном университете «МИФИ» по адресу: 115409, г. Москва, Каширское шоссе, 31.

С диссертацией можно ознакомиться в библиотеке НИЯУ МИФИ.

Отзывы на автореферат в двух экземплярах, заверенные печатью, просьба направлять по адресу: 115409, г. Москва, Каширское шоссе, 31, диссертационные советы НИЯУ МИФИ (тел. +7 (495) 323-95-26).

Автореферат разослан ____ февраля 2012 г.

Ученый секретарь
диссертационного совета  Леонова Н.М.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследований. В настоящее время происходит бурный рост сетевых технологий: развиваются технологии передачи данных (как проводные, так и беспроводные), совершенствуются как аппаратные, так и программные средства. Во всем мире возрастает роль глобальной сети Интернет как при решении производственных задач, так и в повседневной деятельности. Как следствие происходящих процессов, вычислительные системы становятся более сложными, что увеличивает количество возможных точек отказа аппаратуры и программного обеспечения. Системы удаленного мониторинга (СУМ) в современных вычислительных системах становятся неотъемлемым атрибутом: они выполняют ответственные задачи контроля работоспособности отдельных элементов вычислительных систем, контроля целостности данных и мониторинга событий (отказ оборудования, срабатывание датчиков и др.). К СУМ также можно отнести системы контроля доступа, видеонаблюдения, системы пожаротушения, контроля деятельности сотрудников и др. Также следует обозначить обособленную область применения СУМ – неявный мониторинг, например, в рамках системы технических средств для обеспечения функций оперативно-розыскных мероприятий (СОРМ) в интересах правоохранительных органов. С повышением востребованности и увеличением областей применимости СУМ задача защиты этих систем от различных внешних воздействий становится все более актуальной. Внешние воздействия на СУМ могут иметь различную природу: отказ оборудования, программный сбой, человеческий фактор; при этом воздействия также могут иметь умышленный характер. Например, сотрудники могут быть лично заинтересованными в создании помех в работе систем, которые контролируют их деятельность.

Системы удаленного мониторинга, как любое программное обеспечение (ПО), подвержено воздействию вредоносного ПО (вирусы, черви, троянские программы). Проблема защиты ПО от подобного воздействия является достаточно проработанной: антивирусы, межсетевые экраны и прочие подобные системы (которые можно назвать системами контроля поведения вычислительных процессов (СКП)), в целом, успешно справляются с такими угрозами. Современные СКП, несомненно, осуществляют важную функ-

цию защиты данных пользователей от вредоносного ПО, от внешних атак и других нежелательных воздействий. Вместе с тем, СУМ зачастую имеют схожий функционал с вредоносным ПО, хотя назначение у этих двух классов ПО совершенно разное. По этой причине, СКП, либо же сами пользователи, могут ошибочно классифицировать легальное ПО систем удаленного мониторинга как вредоносное. Как следствие, СУМ оказываются уязвимыми вдвойне: от воздействий вредоносного ПО, а также от СКП. Кроме того, блокировка СУМ может быть произведена пользователями сознательно с целью достижения собственных интересов.

Существующие на данный момент методики не гарантируют защиты СУМ от СКП. Фактически современные технологии защиты СУМ сводятся к использованию недоработок в системах контроля поведения.

Таким образом, разработка методов и средств защиты систем удаленного мониторинга, является *актуальной научной и инженерной задачей*.

Объектом исследования являются системы удаленного мониторинга, работающие в условиях многозадачной среды, в том числе под влиянием систем контроля поведения (антивирусов, брандмауэров и пр.), а **предметом исследования** - методика снижения влияния систем контроля поведения на системы удаленного мониторинга.

Целью диссертационной работы является недопущение снижения эффективности работы систем мониторинга вычислительных ресурсов, посредством их защиты от внешних воздействий со стороны систем контроля поведения.

Методы исследования. В диссертационной работе используются методы теории множеств, теории вероятности и математической статистики, теории массового обслуживания, методы проектирования структурных и функциональных моделей систем (стандарты IDEF), метод экспертных оценок, метод анализа иерархий.

Научная новизна.

1. Впервые построена классификация методов защиты программных систем удаленного мониторинга от СКП. На основании классификаций показано, какие недостатки имеют современные системы защиты СУМ.

2. Разработана математическая модель системы защиты СУМ, позволяющая обеспечить каналы взаимодействия СУМ, минуя СКП.
3. На базе разработанной математической модели, впервые разработаны структурные и функциональные модели системы защиты СУМ, позволяющие создавать методы защиты.
4. Разработаны методы защиты файлового и сетевого взаимодействий элементов СУМ, а также защиты процессов и потоков СУМ от воздействий СКП. Методы позволяют разрабатывать реальные программные средства защиты СУМ.
5. Проведено исследование эффективности работы созданной системы защиты СУМ, которое показало целесообразность предложенного решения проблемы защиты СУМ.

Обоснованность и достоверность результатов работы обеспечивается корректностью применения математического аппарата, доказанностью выводов, разработкой и успешной реализацией результатов в виде прототипа системы, публикацией результатов в печати, апробацией на научно-технических конференциях и семинарах, а также внедрением результатов в практическую деятельность ряда организаций.

Практическая значимость работы заключается в следующем:

1. Разработанные классификации СУМ, СКП и методов защиты СУМ, а также структурные и функциональные модели подсистем защиты СУМ имеют стандартные нотации (IDEF1x, IDEF0), что позволяет их использовать при построении информационных систем практического и учебного назначения.
2. Созданы программные средства защиты СУМ, реализующие разработанные методы.
3. На базе разработанного программного интерфейса доступа к методам защиты СУМ могут создаваться более сложные системы защиты СУМ конкретного назначения.
4. Разработанная методика оценки эффективности системы защиты может использоваться в смежных областях для оценки качества подобных систем.

Реализация результатов исследования. Результаты исследования использовались при выполнении НИР по направлению «Обработка, хранение, передача и защита информации» по проблеме

«Обеспечение безопасности критически важных информационных систем» в рамках Федеральной целевой программы «Научные и научно-педагогические кадры инновационной России». Отдельные результаты использовались при разработке систем удаленного мониторинга сотрудников в организациях Некоммерческое Партнерство «Интернет Сервис +» и ООО «Симдо».

Апробация. Основные результаты диссертационной работы докладывались на следующих конференциях: Научной сессии МИФИ-2009 (г. Москва), Третьей всероссийской конференции «Информационные бизнес системы» (г. Москва, 2011г.), IV Всероссийской научно-практической конференции «Актуальные вопросы развития современной науки, техники и технологий» (г. Москва, 2011г.), Международной научно-практической конференции «Применение инновационных технологий в научных исследованиях» (г. Курск, 2011г.).

Публикация результатов. По теме диссертации опубликовано 10 печатных работ, в том числе 6 статей в ведущих научных журналах из перечня ВАК.

Основными положениями работы, выносимыми на защиту, являются:

1. Три классификации: систем удаленного мониторинга вычислительных ресурсов, систем контроля поведения, методов защиты программных систем удаленного мониторинга.
2. Математическая модель системы защиты СУМ.
3. Структурные и функциональные модели системы защиты СУМ.
4. Методы защиты файлового и сетевого взаимодействий элементов СУМ, а также защиты процессов и потоков СУМ от воздействий СКП.
5. Исследование эффективности разработанной системы защиты СУМ.

Структура и объем диссертационной работы. Диссертационная работа включает введение, четыре главы, заключение, список литературы и два приложения. Общий объем работы 177 страниц (без учета приложений). Работа содержит 57 рисунков, 29 таблиц и 142 наименования библиографии.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность проблемы, определены цели, задачи и методы исследования, представлены основные положения диссертационной работы, выносимые на защиту.

В первой главе проведен анализ современных методов и средств защиты систем удаленного мониторинга (СУМ) вычислительных ресурсов. Проведена классификация СУМ (см. Рис. 1), систем контроля поведения вычислительных процессов (СКП) (см. Рис. 2), а также существующих методов защиты СУМ.

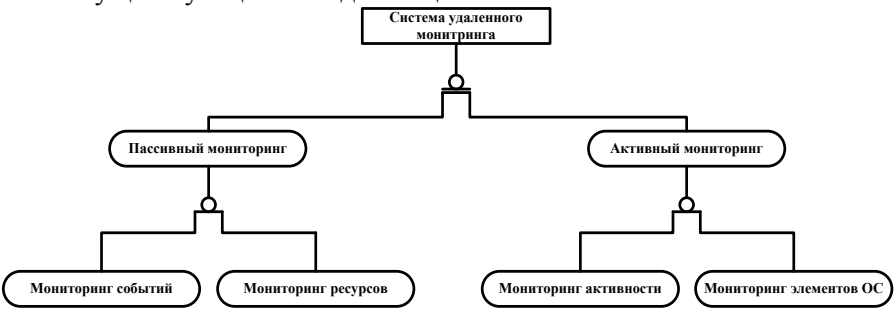

Рис. 1. Классификация систем удаленного мониторинга

При построении классификаций использовался стандарт IDEF1x. Методы защиты СУМ классифицировались по двум основным направлениям (см. Рис. 3) – по защищаемым областям (что именно подлежит защите) и по расположению элементов защиты (где их место в ОС.

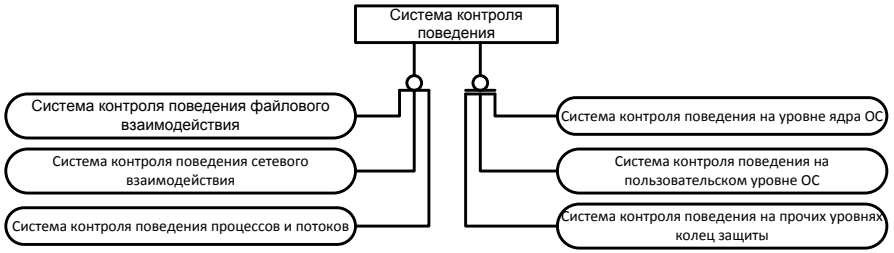

Рис. 2. Классификация систем контроля поведения вычислительных процессов

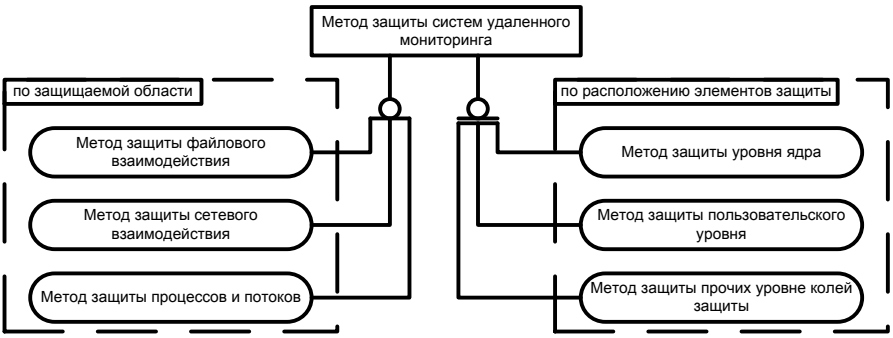

Рис. 3. Классификация методов защиты СУМ

В результате проведенных исследований выявлен основной недостаток современных методов защиты систем удаленного мониторинга - существующие методы не носят технологический характер (т.е. не предоставляют единого механизма защиты), а базируются на недостатках отдельных СКП. На основании проведенных исследований заключено, что разрабатываемые методы и средства защиты СУМ от СКП должны обеспечивать защиту в трех направлениях: сетевое взаимодействие, файловая активность, процессы и потоки. Кроме того необходимы единая модель функционирования системы защиты и предоставление системам удаленного мониторинга единого и законченного функционала защиты.

Вторая глава посвящена разработке методов защиты систем удаленного мониторинга. Прежде всего, разработана математическая модель системы защиты СУМ. Современные операционные системы являются многозадачными. В свою очередь задача (task, process) состоит из множества потоков (thread). Совокупность потоков определяется как множество T^t. В операционной системе могут функционировать различные СКП; обозначим множество работающих в момент времени t СКП как M^t, а $M_i^t \in M^t$ – некоторая СКП. Обозначим как $S_{M_i^t}^t \subset T^t$ – множество штатных потоков, т.е. любой поток, принадлежащий данному множеству, определяется СКП M_i^t как штатный. Множество $X_{M_i^t}^t \subset T^t$ образуют потоки, не обнаруженные системой контроля поведения M_i^t. P(a, $S_{M_i^t}^t$) - вероятность того, что в момент времени t для системы контроля поведения M_i^t некоторый поток

$a \in S^t_{M_i^t}$; $P(a, X^t_{M_i^t})$ - вероятность того, что в момент времени t для системы контроля поведения M_i^t некоторый поток $a \in X^t_{M_i^t}$. Обозначим как $P_a^{\text{раб}}(t)$ вероятность безотказной работы потока a в момент времени t, $P_r^{\text{раб}}(t)$ – вероятность безотказного функционирования ресурса r момент времени t и $P_{M_k^t}^{\text{раб}}(\text{t})$ вероятность безотказной работы СКП M_k^t в момент времени t. Запросы от потока a к ресурсу r в операционной системе проходят через промежуточные программные элементы, в том числе это могут быть СКП, то есть логически они находятся между a и r. Для каждой пары (a, r) определим множество M'^t, где элемент множества – система контроля поведения, находящаяся логически между потоком a и ресурсом r, а m – мощность этого множества.

$P'_{M_i^t}(a, r, t)$ – вероятность того, что доступ потоку a к ресурсу r в момент времени t разрешен СКП M_i^t.

Вероятность доступа потока a к ресурсу r в момент времени t определяется следующим образом:

$$\rho(a,r,t) = P_a^{\text{раб}}(t) P_r^{\text{раб}}(t) \prod_{k=1}^{m} [\left[P\left(a, X^t_{M'^t_k}\right) + P\left(a, S^t_{M'^t_k}\right) P'_{M'^t_k}(a,r,t)\right] P^{\text{раб}}_{M'^t_k}(t)] \quad (1)$$

В том случае, если доступ запрещен всеми СКП, формула имеет вид:

$$\rho = P_a^{\text{раб}}(t) P_r^{\text{раб}}(t) \prod_{k=1}^{m} P\left(a, X^t_{M'^t_k}\right) \quad (2)$$

Далее построим сеть массового обслуживания, отражающую функционирование вычислительной системы в условиях совместной работы системы контроля поведения и системы защиты СУМ (см. Рис. 4).

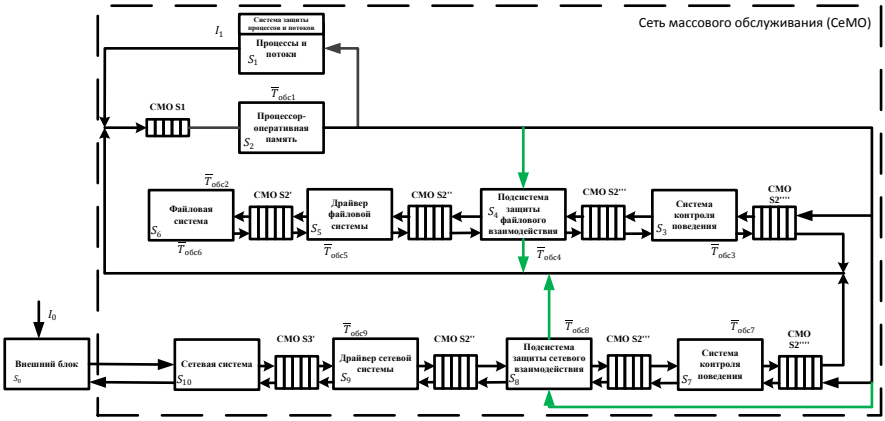

Рис. 4. Сеть массового обслуживания ИС

Разработанная сеть массового обслуживания показывает путь запросов (заявок) минуя системы контроля поведения. В тексте диссертации приведена матрица вероятности передач для полученной СеМО. Так, вероятности передачи от блока S_2 к блокам S_4 и S_8 равны P_{2-4} и P_{2-8} соответственно. Блоки S_4 и S_8 являются элементами системы защиты СУМ, а обозначенные вероятности (которые являются вероятностями обхода определенной СКП и имеют вид $P^{\text{пер}}_{M\prime^t_k}$) соответствуют вероятности $P\left(a, X^t_{M\prime^t_k}\right)$ в формуле (2). Таким образом, формула (2) принимает более конкретный вид (3).

$$\rho = P_a^{\text{раб}}(\text{t}) P_r^{\text{раб}}(\text{t}) \prod_{k=1}^{m} \text{P}^{\text{пер}}_{M\prime^t_k} \qquad (3)$$

Основываясь на полученных формулах, а также построенной СеМО и с учетом материалов первой главы, построим структурные и функциональные модели системы защиты СУМ.

Структурная модель системы защиты состоит из следующих областей: область системы защиты СУМ, область операционной системы и область аппаратной части ЭВМ, показано взаимодействие всех областей между собой. Система защиты СУМ посредством свое-

го API взаимодействует с системой удаленного мониторинга. Структурная и функциональная модель построена в виде ER-моделей.

При создании функциональной модели целевую аудиторию формируют лица, – специалисты в IT-области, разрабатывающие средства защиты СУМ, заинтересованные в изучении и модернизации этой системы с целью проектирования конкретных программных средств защиты СУМ. Точка зрения – взгляд специалиста на систему защиты в целом. Ширина охвата установлена таким образом, чтобы все, что имеет отношение к системе защиты СУМ, вошло в функциональную модель. Глубина детализации функциональной модели такова, чтобы ее можно было положить в основу алгоритмов работы системы защиты СУМ.

Контекстный блок функциональной модели (Лист А-0) (см. Рис. 5) показывает, что на вход системы защиты СУМ поступают запросы от систем мониторинга. Запрос СУМ в файловую подсистему поступает в систему защиты СУМ, которая должна обеспечить взаимодействие с файловыми элементами: файлами и директориями (каталогами, папками). Сетевые запросы СУМ анализируется и обрабатывается сетевой подсистемой системы защиты СУМ. Запросы СУМ связанные с защитой процессов и потоков обрабатываются соответствующей подсистемой системы защиты. Выходами системы защиты СУМ являются результаты обработки соответствующих входящих запросов. Формат ответа зависит от запроса и представляется в виде данных или кодов возврата. Управляющий механизм определяет правила работы системы защиты СУМ, а также задает требования к форматам данных и заголовкам функций программного интерфейс (API). К механизмам управления относятся: подсистема ввода-вывода ОС, механизм работы планировщика процессов ОС, сетевой стек ОС, API системы защиты СУМ, структура сетевого пакета. Подсистема ввода-вывода ОС устанавливает правила, по которым будет функционировать подсистема защиты файлового взаимодействия. Механизм работы планировщика процессов ОС определяет порядок функционирования подсистемы защиты процессов и потоков. Функционирование подсистемы защиты сетевого взаимодействия должно полностью соответствовать сетевому стеку ОС.

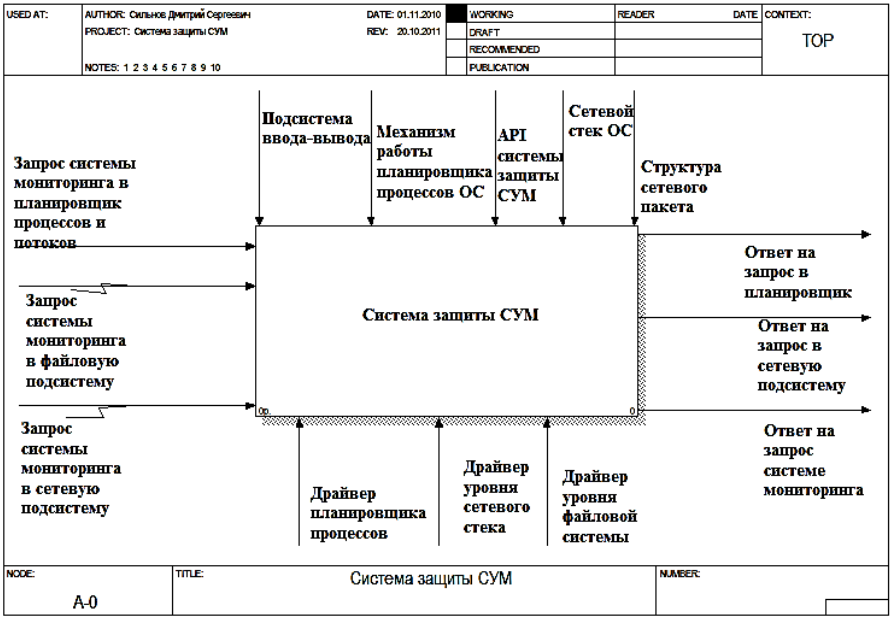

Рис. 5. Функциональная модель системы защиты СУМ. IDEF0-диаграмма A-0

API системы защиты СУМ имеет стандартный формат, подобный формату WinAPI, что определяет требования к оформлению заголовков процедур и функций, которые будут предоставляться СУМ. Исполнительными механизмами системы защиты СУМ, являются: драйвер уровня сетевого стека, драйвер уровня файловой системы и драйвер планировщика процессов.

На основании разработанной математической модели, структурной и функциональной модели, разработаны алгоритмы работы драйвера защиты сетевого взаимодействия (см. Рис. 6) и драйвера защиты файлового взаимодействия (см. Рис. 7). Драйвер защиты сетевого взаимодействия в процессе своей работы обменивается данными с сетевой подсистемой ОС (NDIS).

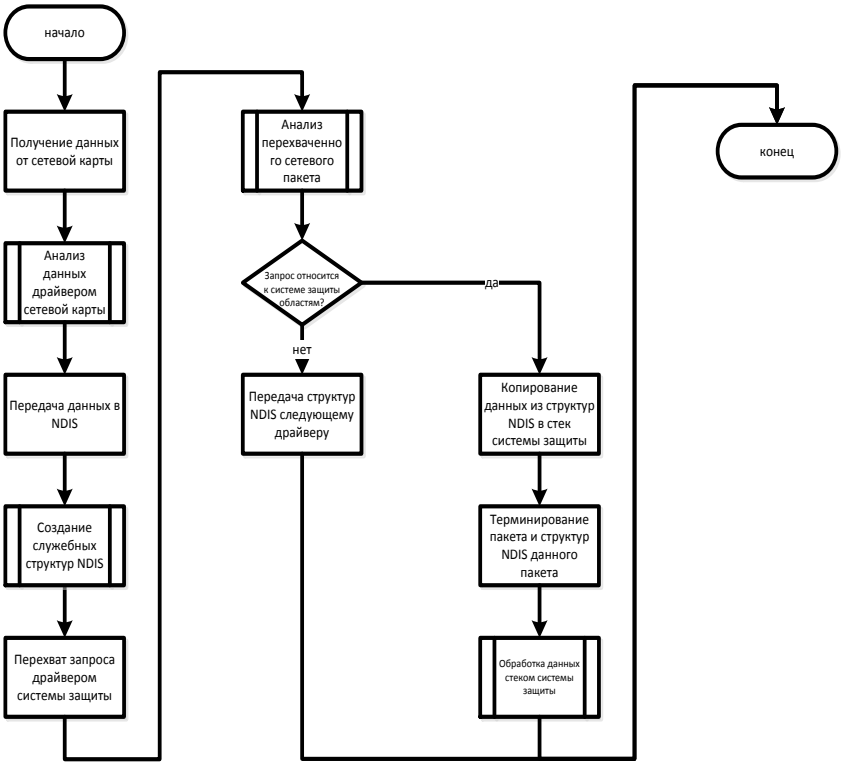

Рис. 6. Схема алгоритма работы драйвера защиты сетевого взаимодействия, входящий пакет

При взаимодействии системы защиты СУМ с NDIS происходит отбор сетевых пакетов, предназначенных для СУМ. Данная операция происходит таким образом, что средствами ОС будет невозможно получить доступ к этим пакетам, поэтому необходимо иметь собственную реализацию стека протоколов TCP/IP, в частности протокола ARP. Драйвер защиты файлового взаимодействия анализирует и перенаправляет запросы от СУМ менеджеру ввода-вывода ОС (I/O Manager). Запросы преобразовываются во внутреннюю структуру менеджера ввода-вывода, называемую IRP-пакетом.

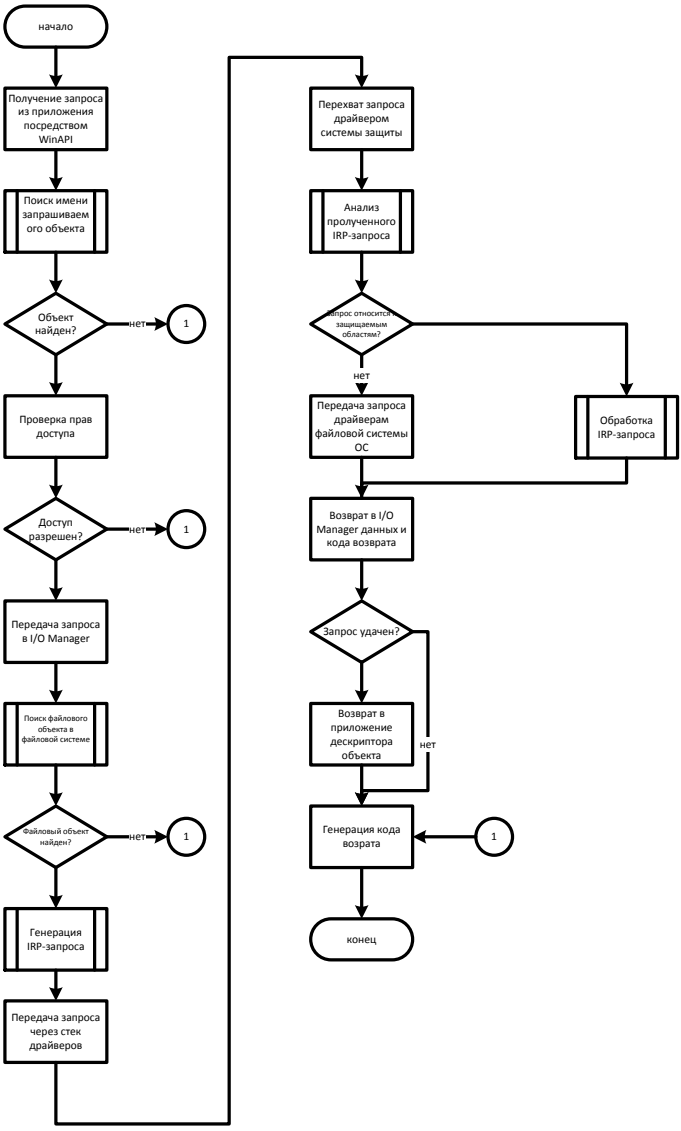

Рис. 7. Схема алгоритма работы драйвера защиты файлового взаимодействия

Третья глава посвящена реализации разработанных методов в виде прототипа системы защиты СУМ для последующих исследований ее эффективности. Описаны структура и архитектура прототипа, разработаны и описаны структуры данных системы, интерфейсы прикладного программирования (API). Показаны ключевые моменты при реализации функционала системы. Проведено тестирование и отладка программного обеспечения прототипа.

Прототип состоит из трех частей. Каждая из частей является автономной подсистемой и реализует свою часть в общем функционале, предоставляемом системам мониторинга. Элементы представлены в виде программных драйверов - файлов с расширением .sys, функционирующих в рамках ядра ОС семейства Windows. Прототип состоит из трех драйверов (см. Рис. 8): драйвер защиты файлового взаимодействия, драйвер защиты сетевого взаимодействия и драйвер защиты процессов и потоков.

Драйвер защиты файлового взаимодействия представлен в виде фильтра файловой системы. Экспортируемые функции являются частью, отвечающей за файловые операции, в программном интерфейсе ZlwAPI [9]. Для реализации заложенных функций, драйвер использует интерфейс фильтров файловых запросов, который предоставляется менеджером ввода\вывода ОС Windows. Драйвер работает в режиме ядра и функционирует автономно, независимо от других частей прототипа.

Драйвер защиты сетевого взаимодействия реализован в виде фильтра сетевой системы. Экспортируемые функции являются частью, отвечающей за сетевые операции, в программном интерфейсе ZlwAPI. Для реализации функционала драйвер использует интерфейс фильтров сетевых запросов, который предоставляется драйвером NDIS (сетевой подсистемы ОС Windows). Драйвер работает в режиме ядра и напрямую не взаимодействует с другими драйверами прототипа.

Драйвер защиты процессов и потоков реализован в виде драйвера общего назначения. Экспортируемые функции являются частью, отвечающей за защиту процессов и потоков, в программном интерфейсе ZlwAPI. Для реализации необходимых функциональных возможностей, требуемых от данного драйвера, он использует адресные

данные из планировщика процессов и потоков ОС Windows, который осуществляет распределение процессорного времени между потоками.

Рис. 8. Структура прототипа системы защиты СУМ

Основной задачей данного драйвера является получение процессорного времени, которое далее посредством внутреннего механизма драйвера, распределяется соответствующим потокам (например, потокам СУМ). Драйвер также работает в режиме ядра и непосредственно не взаимодействует с другими драйверами прототипа.

Несмотря на то, что драйверы-элементы прототипа не взаимодействуют друг с другом напрямую, общая координация и экспорт элементов ZlwAPI осуществляется посредством взаимодействия через системный реестр ОС, разделы которого могут быть также включены в области файловой защиты для предотвращения несанкционированных изменений.

В четвертой главе проведено исследование методов и средств защиты систем удаленного мониторинга вычислительных ресурсов. Для определения эффективности разработанной системы защиты, введены критерии эффективности системы защиты (см. Табл. 1). На основании анализа данных критериев, используя метод расчетов, предложенный Т.Саати [1] в методе анализа иерархий, были выделены три наиболее значимых критерия эффективности, на базе которых построен единый синтетический критерий (4).

Таблица 1. Критерии эффективности системы защиты

№	Наименование критерия	Приоритет
К1	Вероятность успешной защиты	0.418
К2	Версия операционной системы	0.043
К3	Значение параметра altitude *	0.119
К4	Разница во времени запуска	0.296
К5	Производительность элементов системы защиты	0.029
К6	Процент загрузки процессоров ЭВМ	0.029
К7	Количество систем контроля	0.065

* данный параметр определяет взаимное логическое местоположение драйверов относительно аппаратного обеспечения

$$K' = f(K1, K4, K3) = (max\, P'', min\, \Delta t, altitude \leq min(a_i)) \qquad (4)$$

где P''- вероятность успешной защиты, Δt – разница во времени, описанная в критерии эффективности К4. a_i – altitude i-ой системы контроля поведения.

Параметр altitude необходимо выбирать таким образом, чтобы значение данного параметра у элементов (драйверов) системы защиты было меньше, чем у систем контроля поведения, установленных в рамках ОС. Учитывая эти ограничения, необходимо определить вероятность успешной защиты, во взаимосвязи с разницей во времени запуска. Данная вероятность обозначается через $P''(t)$. Обозначим через t_1 – момент времени в который происходит запуск СКП, t_2 – момент времени в который происходит запуск системы защиты СУМ, N – общее количество защищаемых элементов.

Теоретическая оценка, $P''(t')$ определяется следующим образом:

$$\begin{aligned} &P''^{(t')} \to 1, \quad \forall\, t', \text{если } t_2 < t_1 \\ &P''^{(t')} = 1 - \frac{i}{N}, \end{aligned} \qquad (5)$$

$$t' > t_1 + \sum_{k=1}^{i+1} t_{D_k}^{\text{обн}}, \text{если } t_1 + \sum_{k=1}^{i+1} t_{D_k}^{\text{обн}} > t_2 > t_1 + \sum_{k=1}^{i} t_{D_k}^{\text{обн}}$$

$$P''(t') \to 0, \qquad \forall\, t', \text{если } t_2 > t_1 + \sum_{k=1}^{N} t_{D_k}^{\text{обн}}$$

где i – порядковый номер последнего обнаруженного защищаемого элемента.

Графически данная оценка выглядит как показано на рисунке ниже (см. Рис. 9):

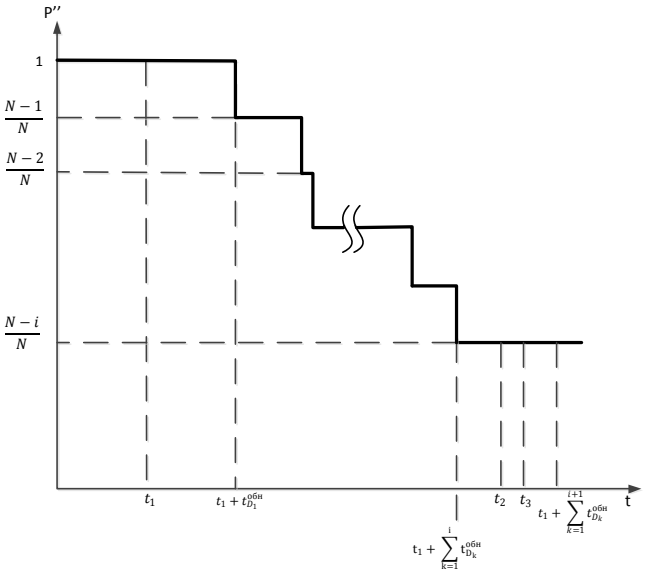

Рис. 9. Теоретическая оценка зависимости вероятноятности защиты от времени

Разработана методика оценки результатов, проведены экспериментальные исследования и проведен анализ полученных результатов. Точками на графике (см. Рис. 10) обозначены тестовые элементы, обнаруженные системой контроля поведения. По мере их обнаружения, снижается общая вероятность успешной защиты.

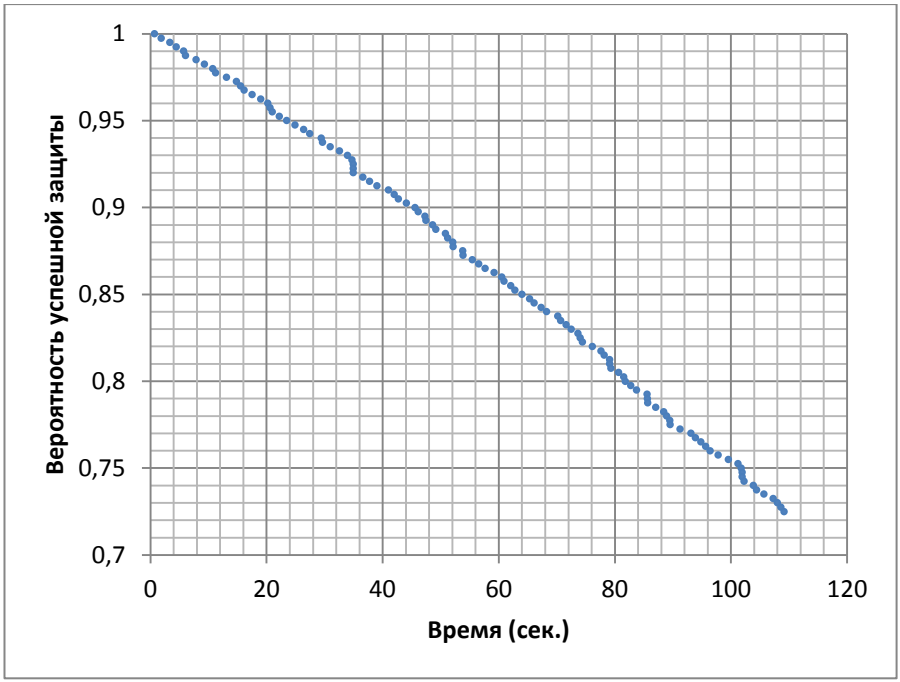

Рис. 10. График зависимости вероятности защиты от времени

С доверительной вероятностью 0.95 полученная экспериментальным путем вероятность защиты СУМ от СКП соответствует параметрической модели (5).

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

В диссертации решена важная научная задача недопущения снижения эффективности работы систем мониторинга вычислительных ресурсов, посредством их защиты от внешних воздействий со стороны систем контроля поведения.

Основными результатами данной работы являются:

1. Проведены анализ и классификации современных систем контроля поведения, систем удаленного мониторинга и систем защиты СУМ. Обозначены основные элементы операционной системы, в которых работают системы контроля поведения и в которых

следует разрабатывать системы защиты СУМ: файловая подсистема, сетевая подсистема, процессы и потоки. Сделан вывод, что существующие методы защиты не носят технологический характер (т.е. не предоставляют единообразного механизма защиты), а базируются на недостатках отдельных СКП.

2. Разработана математическая модель комплексной системы защиты СУМ. В виде сети массового обслуживания построена модель ЭВМ в условиях совместной работы СУМ и систем контроля поведения. Данная модель в формализованном виде отражает особенности взаимодействия и местоположения данных элементов защиты СУМ относительно аппаратного обеспечения и ОС.
3. Разработаны методы защиты файлового взаимодействия, сетевого взаимодействия и методы защиты процессов и потоков. Предлагаемые методы позволяют осуществлять создание защищенных областей в файловой системе, системном реестре и каналов связи не контролируемых СКП. Данные методы предоставляют интерфейс для программных СУМ для доступа к защищаемым областям. Методы защиты процессов и потоков позволяют распределять процессорное время элементам СУМ, которые необходимо исполнять в формате защиты от СКП.
4. Разработаны обобщенные структурные и функциональные модели подсистем защиты СУМ на базе стандартных нотаций IDEF1x и IDEF0, что позволяет использовать их при построении информационных систем как прикладного, так и учебного назначения.
5. Разработана структура и архитектура, структуры данных и программный интерфейс (API) прототипа системы защиты СУМ. Структура и архитектура разработаны таким образом, чтобы предоставлять программный интерфейс системам удаленного мониторинга и взаимодействовать с операционной системой на уровне ядра ОС.
6. Реализован прототип системы защиты СУМ в виде набора драйверов уровня ядра ОС Windows, проведено тестирование и отладка прототипа. Созданный прототип системы защиты используется для исследования эффективности предложенного подхода.
7. Выделено семь критериев эффективности системы защиты СУМ. Среди данных критериев методом расчетов, предложенным Т.Саати [1], выделено три наиболее значимых критерия (разница

во времени запуска системы защиты и системы контроля поведения, близость драйверов системы защиты к аппаратному обеспечению в иерархии драйверов в ОС, вероятность успешной защиты элементов, которые используются системой удаленного мониторинга), чей суммарный приоритет более 0.83. На их базе построен синтетический критерий эффективности защиты СУМ, для которого определена теоретическая оценка.

8. Проведены экспериментальные исследования, получены и проанализированы результаты, которые подтверждают теоретические оценки эффективности системы с доверительной вероятностью 0.95. В отдельных сериях экспериментов полученные результаты улучшают теоретическую оценку, что связано с недоработками современных СКП.

Исходя из теоретических оценок, подкрепленных экспериментальными исследованиями, разработанные методы и средства защиты решают поставленную в данной работе задачу.

Основные результаты диссертационной работы изложены в 10 печатных трудах:

1. Сильнов Д.С. Методика многокритериальной оценки эффективности средств защиты систем удаленного мониторинга // Глобальный научный потенциал, №8 - СПб: Изд-во ТМБпринт, 2011, с. 111-115. (**журнал из перечня ВАК**)
2. Сильнов Д.С. Классификация средств защиты систем удаленного мониторинга вычислительных ресурсов // Прикладная информатика, №3(33), 2011, с. 79-82. (**журнал из перечня ВАК**)
3. Сильнов Д.С. Оценка эффективности средств защиты систем удаленного мониторинга // Прикладная информатика, №4(34), 2011, с. 111-115. (**журнал из перечня ВАК**)
4. Сильнов Д.С. Актуальность современных систем удаленного мониторинга вычислительных ресурсов // Известия Российского государственного педагогического университета им. А.И.Герцена. Научный журнал. Естественные и точные науки. № 141, СПб: Издательство РГПУ им. А.И.Герцена, 2011, с. 55-59. (**журнал из перечня ВАК**)
5. Сильнов Д.С. Современные системы удаленного мониторинга вычислительных ресурсов: состояние, проблемы, перспективы. //

Безопасность информационных технологий 2011. №3, с. 57-60. (**журнал из перечня ВАК**)

6. Сильнов Д.С., Васильев Н.П. Программные средства защиты систем удаленного мониторинга вычислительных ресурсов. // Безопасность информационных технологий 2011. №3, с. 140-142. (**журнал из перечня ВАК**)
7. Сильнов Д.С. Передача информации в средствах удаленного мониторинга вычислительных ресурсов // Актуальные вопросы развития современной науки, техники и технологий. Материалы IV Всероссийской научно-практической (заочной) конференции.- М.:НИИРРР, 2011., с. 137-139.
8. Сильнов Д.С., Васильев Н.П. Методы передачи информации в программных средствах удаленного мониторинга вычислительных ресурсов // Научная сессия МИФИ-2009. Аннотация докладов. – М:НИЯУ МИФИ, 2009. – Т.3 – С.167.
9. Сильнов Д.С. Вопросы передачи информации в программных средствах удаленного мониторинга вычислительных ресурсов // Применение инновационных технологий в научных исследованиях. Сборник научных статей по материалам II Международной научно-практической конференции, 2011., С.194-197.
10. Сильнов Д.С., Васильев Н.П. Программные средства защиты систем удаленного мониторинга вычислительных ресурсов. // Информационные бизнес системы. Третья Всероссийская ежегодная научно-практическая конференция. 23 апреля 2011 г.: материалы конференции / Под научной редакцией, д.э.н. профессора М.И. Лугачева. – М.: Гелиос АРВ, 2011. – с. 327 – 329.