На правах рукописи

СТЮГИН Михаил Андреевич

МЕТОДЫ И МОДЕЛИ ЗАЩИТЫ ОТ ИССЛЕДОВАНИЯ ПРИ УПРАВЛЕНИИ КОНФЛИКТОМ В АКТИВНЫХ СИСТЕМАХ

05.13.17 – Теоретические основы информатики

АВТОРЕФЕРАТ

диссертации на соискание ученой степени
кандидата технических наук

Красноярск 2010

Работа выполнена в Сибирском государственном аэрокосмическом университете имени академика М.Ф. Решетнева

Научный руководитель: доктор технических наук, профессор
Семенкин Евгений Станиславович

Официальные оппоненты: доктор технических наук, профессор
Глухова Елена Владимировна

доктор технических наук, профессор
Кашкин Валентин Борисович

Ведущая организация: Томский государственный университет

Защита диссертации состоится «3» июня 2010 г. в 14.00 часов на заседании диссертационного совета Д 212.099.11 при Сибирском федеральном университете по адресу 660074 , г. Красноярск, ул. Киренского, 26, ауд. УЛК 115.

С диссертацией можно ознакомиться в библиотеке Сибирского федерального университета по адресу: г. Красноярск, ул. Киренского, 26, ауд. Г 2-74.

Автореферат разослан «30» апреля 2010 г.

Ученый секретарь
диссертационного совета,
кандидат технических наук,
доцент Покидышева Л.И.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность.

С развитием информационных технологий все более актуальной становится задача разработки методов и моделей обеспечения безопасности информационных систем. Однако крайне редко данные исследования отражают тот факт, что злоумышленник, атакующий систему, имеет необъективные представления о самой системе, с которой он находится в состоянии конфликта, и получает новые знания в процессе исследования или на основании ранее построенных стереотипных решений, которые могут быть неадекватны текущей ситуации.

Когда речь идет о конфликте двух или более субъектов активной системы, необходимо учитывать имеющуюся у них информацию об объекте конфликта (объект, который отражает различие интересов участников конфликта), его структуре (сколько участников конфликта и каковы их цели), а также возможные сценарии развития конфликта (множество действий, которые может совершить каждый из участников конфликта и выигрыш или потери, который при этом понесет каждый из них). Чем более объективна эта информация у субъекта, тем более адекватные действия относительно своей цели он совершает. Информация эта может априорно присутствовать в представлениях субъекта или формируется им в результате процесса *исследования* системы. Если удастся понять принципы получения этой априорной информации и механизм исследования, то станет возможным эффективно управлять информацией в конфликте, и, тем самым, управлять конфликтом в своих целях.

Исходя из такой постановки задачи, в данной работе каждый *участник* конфликта в активной системе отождествлен с *исследователем*, поскольку перед ним всегда стоит задача получения объективной информации о состоянии конфликта, даже если процесс исследования не проводится им осознанно, а осуществляется на основе ассоциативных схем (априорной информации). Осуществляя информационное управление таким исследователем, т.е. используя модели защиты от исследования, можно расширить круг методов управления конфликтом. Так как теоретические основы для получения более выигрышных стратегий в конфликтах за счет технологии защиты от исследования еще не получили достаточного развития, то для создания моделей и методов защиты от исследования в конфликтных системах требуется разработка теоретико-методологической базы, что и предопределяет актуальность данной научной проблемы в области теории и практики управления конфликтом.

Целью работы является повышение уровня безопасности использования информационных технологий за счет применения моделей и методов защиты от исследования систем при управлении конфликтом.

Для достижения указанной цели необходимо решить следующие **задачи**:

1. Провести анализ моделей конфликтов в активных системах с точки зрения зависимости выигрыша участников от их информированности и определить проблему получения информации участником конфликта – исследователем.

2. Построить модель исследователя, отражающую информационные ограничения, с которыми он сталкивается при определении функциональной структуры исследуемого объекта.
3. Разработать модель конфликта, позволяющую учитывать влияние информированности агента на принятие решений в конфликте и достижимость цели.
4. Построить модель конфликта, позволяющую анализировать принятие решений агентами в зависимости от состояния рефлексивной структуры конфликта и отражать процесс исследования на рефлексивной структуре.
5. Разработать методы защиты систем от исследования относительно информационных ограничений, определяемых моделью исследователя и моделями конфликта, учитывающими его функциональную и рефлексивную составляющую.
6. Разработать технологию защиты от исследования и провести ее экспериментальную апробацию.

Методы исследования основаны на использовании методологии системного анализа, теории активных систем, теории алгоритмов и кибернетических моделей исследователя.

Основные результаты, выносимые на защиту:

1. Модель исследователя и три класса информационных ограничений в конфликте.
2. Метод защиты от исследования систем на основе добавления нефункционального преобразования по дополнительным параметрам.
3. Метод защиты от исследования систем на основе увода процесса за пределы области параметрической и функциональной видимости.
4. Функциональная модель структуры информированности в конфликте, алгоритм определения достижимости цели субъектом в рамках функциональной модели структуры информированности и методика достижения информационного превосходства в конфликте.
5. Сигнатурная модель субъекта в конфликте и схемы расчета готовности субъекта совершить действие в зависимости от ранга рефлексии.

Научная новизна работы заключается в следующем:

1. Разработана модель исследователя, позволяющая выделить три класса информационных ограничений, которые затрудняют получение исследователем точной информации о функциональной структуре исследуемого объекта: параметрическая невидимость, функциональная невидимость, существующее множество гипотез по структуре исследуемого объекта.
2. Впервые разработаны три метода защиты от исследования систем: добавление нефункционального преобразования по дополнительным параметрам и увод процесса за пределы области параметрической и функциональной видимости.
3. Впервые разработана модель конфликта, позволяющая определять достижимость агентом цели относительно формулируемого им множества гипотез о структуре объекта конфликта, а также определять

методы достижения функциональной невидимости, если в качестве объекта исследования выбран сам конфликт.

4. Разработана новая модель конфликта, отражающая качественные характеристики рефлексивной структуры информированности и позволяющая прогнозировать готовность агента к совершению активных действий в зависимости от выбранного им ранга рефлексии.
5. Впервые разработаны теоретические основы и алгоритм модификации функциональной структуры систем с точки зрения защиты их от исследования злоумышленником, учитывающие информационные ограничения исследователя (злоумышленника), множества гипотез злоумышленника относительно структуры конфликта и рефлексивную структуру конфликта.

Практическая ценность работы.

Практическая значимость результатов диссертации заключается в том, что разработанные модели и методы защиты систем от исследования контрагентом позволяют:

1. Снижать риски преднамеренных атак или сокращать издержки на систему безопасности.
2. Получать более эффективные конкурентные стратегии за счет анализа функциональной структуры информированности в конфликте.
3. Обеспечивать безопасность веб-ресурсов путем защиты их от исследования.

Использование результатов. На основе разработанных в ходе выполнения диссертации моделей и технологий подана заявка на патент RU2009124336 "Способ построения системы информационной безопасности компьютерной системы", получены два свидетельства о регистрации программных систем №2009615408 "PRIS Trap" и №2009615409 "PRIS Mirror" в Роспатенте. Работа выполнялась в рамках проекта № 02.442.11.7337 ФЦНТП «Исследования и разработки по приоритетным направлениям развития науки и техники», НИР НК-136П/3 ФЦП «Научные и научно-педагогические кадры инновационной России» и проекта № Б1.7.08 темплана ЕЗН СибГАУ. Исследования по теме диссертации были поддержаны четырьмя грантами Красноярского краевого фонда науки и грантом Фонда Михаила Прохорова, а также грантом Фонда содействия развитию малых форм предприятий в научно-технической сфере (программа У.М.Н.И.К.) по контракту 6371р/8857. Работа удостоена Государственной премии Красноярского края за высокие результаты в научных разработках, направленных на социально-экономическое развитие края, достигнутые в 2009 году (распоряжение Губернатора Красноярского края от 10 августа 2009 г. №314-рг). Работа удостоена высоких оценок на конкурсах инновационных проектов – Конкурс Русских Инноваций 2009, БИТ-Сибирь 2010.

Научные результаты данной диссертационной работы заложены в основу деятельности созданного диссертантом малого инновационного предприятия ООО «Инновационные технологии безопасности», являющегося резидентом Красноярского городского инновационно-технологического бизнес-инкубатора. Технология защиты от исследования систем была использована консалтинговой

компанией ООО «Практика» для расширения функционала существующих систем информационной безопасности, а так же применена для поисковой оптимизации сайтов «Информационные войны» (http://infwar.ru) и «Инновационные технологии безопасности» (http://infosafety.ru).

Достоверность полученных результатов подтверждается корректностью теоретического обоснования, применением современного аппарата системного анализа, широкой апробацией и результатами практического использования разработанных в диссертации моделей и алгоритмов.

Апробация работы. Основные результаты, полученные в ходе работы над диссертацией, были представлены на Международных научно-практический междисциплинарных симпозиумах «Рефлексивные процессы и управление», Москва (2007, 2009); Международных конференциях «Проблемы управления безопасностью сложных систем», Москва (2007, 2008, 2009); Четвертой международной конференции по проблемам управления, Москва (2009); Международных конференциях «Проблемы регионального и муниципального управления», Москва (2008, 2009); Международных научных конференциях «Решетневские чтения», Красноярск (2007, 2008, 2009); Международных научно-практических конференциях «Инновационные недра Кузбасса. IT-технологии», Кемерово (2007, 2008); а также ряде других научных конференций и семинаров.

Публикации. По теме диссертации опубликовано более 20 научных трудов, из них три статьи опубликованы в центральном рецензируемом журнале «Информационные войны» (Москва) за 2009 г., а также две статьи в журналах «Вестник Сибирского государственного аэрокосмического университета» и «Программные продукты и системы», которые входят в перечень изданий, рекомендованных ВАК РФ для публикации результатов диссертационных работ.

Объем и структура диссертации. Диссертация состоит из введения, четырех глав, заключения, списка литературы, включающего 70 наименований. Основной текст диссертации изложен на 129 страницах, включая 7 рисунков и 13 таблиц.

СОДЕРЖАНИЕ РАБОТЫ

Во введении кратко рассматривается актуальность работы, цели и основные задачи, научная новизна и практическая ценность работы, приводится карта всей работы.

В первой главе определяются основные понятия, относящиеся к теме работы, рассматриваются кибернетические модели процесса «исследования» в кибернетике, а также информационные ограничения, априорно предшествующие данному процессу. Приводится модель черного ящика, введенная У.Р. Эшби, и определяемые ею свойства изоморфизма и гомоморфизма исследуемого объекта. Рассмотрена кибернетическая модель познания по Л.А. Растригину, где помимо исследователя и объекта присутствует фильтр, определяемый моделью вводимой самим исследователем. Данная модель наглядно показывает неотделимость от процесса исследования информации, заранее имеющейся у исследователя об исследуемом объекте. Рассматривается проблема исследования активных

систем, когда цели исследуемой системы могут противоречить цели исследователя, формулируется классическая парадигма решения задач в области активных систем.

Анализ научной литературы показывает, что в области существующих подходов к защите систем от исследования, мы не можем обнаружить единой методологии, формулирующей общезначимые методы и технологии решения прикладных задач. На данный момент можно выделить лишь несколько теоретических работ в этом направлении, относящихся к области информационной безопасности: это система HoneyPot и защита целостности программного кода. Поэтому становится очевидной актуальность выбранной темы исследования.

Во второй главе строится модель исследователя с учетом существующих у него информационных ограничений. За основу берется модель черного ящика представляющего собой функцию некоторого множества параметров **par**.

В реальных системах мы, как правило, не можем знать, что является для черного ящика входом и выходом, поэтому исследователю приходится строить *гипотезы* относительно функциональной структуры ящика. Такая гипотеза по существу есть предположение относительно множества параметров (**par'**), от которого зависит целевая функция системы – f (рис.1).

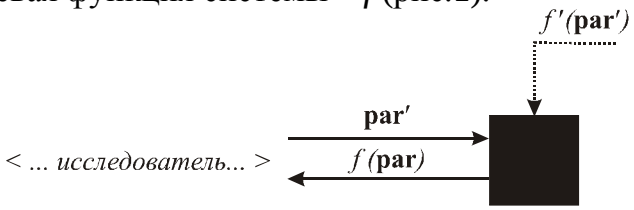


Рисунок 1 – Модель исследователя

Имея некую гипотезу относительно функциональной структуры черного ящика – $f'(\mathbf{par'})$ и перебирая множество входных параметров **par'**, исследователь наблюдает значение функции – $f(\mathbf{par})$. Гипотезу исследователя будем называть *стереотипной схемой*.

Несмотря на различие функций, множество их значений определено на одном множестве, т.к. исследователь контролирует значение одного выхода:

$$f:\mathbf{par}\to\mathbf{y};\quad f':\mathbf{par}'\to\mathbf{y};\quad f'':\mathbf{par}''\to\mathbf{y};\quad \ldots$$

У исследователя может присутствовать любая из гипотез $f^x:\mathbf{par}^x\to\mathbf{y}$, но такой функции может не существовать в действительности. То есть в рамках выбранного множества параметров $\mathbf{par}^x$ невозможно найти функциональное отображение на множество $\mathbf{y}$. Может быть ситуация когда функциональная зависимость есть, но не равна реальной функции черного ящика $f^x\neq f$.

Множество всех возможных множеств параметров функции черного ящика составляет множество $\mathbf{S}_{\mathbf{par}}$, т.е.

$$\mathbf{par}',\mathbf{par}'',\mathbf{par}''',\ldots\in\mathbf{S}_{\mathbf{par}}\ .$$

Множество все возможных функций черного ящика по гипотезам исследователя

$$\mathbf{F}_{\mathbf{par}}=\{\,f^x(\mathbf{par}^x):\mathbf{par}^x\in\mathbf{S}_{\mathbf{par}}\,\}.$$

Дополнительным ограничением процесса исследования являются функциональная и параметрическая невидимость. Для каждого исследователя можно определить множество параметров, изменение значений которых он может наблюдать во всем диапазоне – $\mathbf{S_v} \subseteq \mathbf{S_{par}}$. Это – *область параметрической видимости*. Аналогично определяется множество *функциональной видимости* $\mathbf{F_v} \subseteq \mathbf{F_{par}}$:

$$\mathbf{F_v} = \{ f^x(\mathbf{par}^x) : \mathbf{par}^x \in \mathbf{S_v} \}.$$

Описанная модель исследователя может принадлежать одному из четырех классов.

Класс 1. $\mathbf{par'} = \mathbf{par},\ \mathbf{par} \in \mathbf{S_v},\ \{f(\mathbf{par})\} \in \mathbf{F_v}$

Эта классическая модель исследования черного ящика. Для определения функциональной структуры черного ящика достаточно перебрать входные значения и сопоставить со значением функции выхода. Здесь стереотипная схема (гипотеза) исследователя соответствует действительности.

Класс 2. $\mathbf{par'} \neq \mathbf{par},\ \mathbf{par} \in \mathbf{S_v},\ \{f(\mathbf{par})\} \in \mathbf{F_v}$

Неинформативная обратная связь. В силу неверной гипотезы относительно функциональной структуры системы исследователь не может найти функцию черного ящика. Здесь стереотипная схема (гипотеза) уже не соответствует действительности. Задача исследователя при данных условиях путем перебора гипотез добиться информативной обратной связи и свести тем самым систему к первому классу.

Класс 3. $\mathbf{par'} \neq \mathbf{par},\ \mathbf{par} \notin \mathbf{S_v},\ \{f(\mathbf{par})\} \in \mathbf{F_v}$

Невозможно добиться информативной обратной связи от исследуемой системы. Параметры целевой функции черного ящика не входят в область параметрической видимости исследователя. Исследование в таких условиях бессмысленно. Необходимо расширить область параметрической видимости и привести тем самым модель ко второму классу.

Класс 4. $\mathbf{par'} \neq \mathbf{par},\ \mathbf{par'} \notin \mathbf{S_v},\ \{f'(\mathbf{par'})\} \notin \mathbf{F_v}$

Невозможность постановки задачи исследования. Здесь исследователь сталкивается уже с проблемой функциональной невидимости, для которой можно сформулировать следующее утверждение: *функции, выходящей за область функциональной видимости, всегда можно сопоставить функцию с меньшим числом параметров, находящейся в области функциональной видимости*:

$$\forall \{f'(\mathbf{par}, \mathbf{par'})\} \notin \mathbf{F_s}\ \exists \{f(\mathbf{par})\} \in \mathbf{F_s} : \quad f'(\mathbf{par}, \mathbf{par'}) \equiv f(\mathbf{par}). \tag{1}$$

Т.е. в данном случае значение функции $f'(\mathbf{par}, \mathbf{par'})$ и $f(\mathbf{par})$ при одних и тех же значениях параметров **par** тождественны. В такой ситуации исследователь может сопоставить с моделью черного ящика более простую функциональную структуру. Поскольку нет какого-либо диссонанса в рамках наблюдаемых величин, то и невозможна постановка задачи исследования. Перевести модель к третьему или второму классу можно только путем расширения области функциональной видимости.

Информационное управление конфликтом теперь можно осуществлять путем перевода реальной ситуации к четвертому классу, по возможности оставляя контрагента в заблуждении, что ситуация относится к первому классу.

Чтобы рассмотреть данную модель в контексте реального конфликта необходимо выделить структуру информированности каждого агента, признаки по которым он определяет достижимость своей цели и формулирует задачу исследования, а также выделить методы увода объекта в область функциональной невидимости. Для решения этих задач была построена *функциональная модель структуры информированности в конфликте*. Она представляет собой направленный граф, ставящий в соотношения цели и параметры их достижения, и характеризует действие в конфликте как процесс.

Обозначим через $\boldsymbol{A}$ действие одного субъекта конфликта x. Если при этом ничего больше не уточняется, то можно говорить о том, что действие происходит в некотором роде стереотипно. В этом случае образ в структуре информированности субъекта состоит из единственного параметра, который обозначает также и цель:

$$\mathbf{I}_x = \{ A \}.$$

Далее структуру можно расширить. Например, действие можно производить двумя принципиально различными способами, а, следовательно, по двум независимым параметрам - P_1 или P_2.

$$\mathbf{I}_x = \left\{ A \begin{array}{l} \diagup P_1 \\ \diagdown P_2 \end{array} \right\}.$$

Оба этих параметра уточняют действие A, определенного как конечная цель. Теперь субъект действует либо по параметру P_1, либо по параметру P_2 (вводятся со знаком «или»). Если для достижения $\boldsymbol{A}$ необходимо совершить действие по обоим параметрам (со знаком «и»), то они обводятся пунктирной линией:

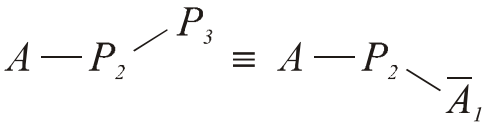
$$\mathbf{I}_x = \left\{ A \begin{array}{l} \diagup P_1 \\ \\ \diagdown P_2 \end{array} \right\}.$$

Построение таких функциональных структур в представлениях каждого из субъектов позволяет выделить информационные ограничения при принятии решений, например, неразличимость относительно параметров процесса.

Например, субъект y пытается не допустить достижения цели $\boldsymbol{A}$. Он может ввести дополнительный параметр ($\bar{A}_1$ и P_3) в структуру действия и снова отойти от стереотипной схемы. То есть его образ в структуре информированности расширяется:

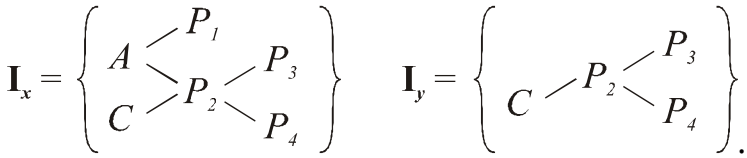
$$\mathbf{I}_x = \left\{ A \begin{array}{l} \diagup P_1 \\ \diagdown P_2 \end{array} \right\} \qquad \mathbf{I}_y = \left\{ A \begin{array}{l} \diagup P_1 \\ \diagdown P_2 \begin{array}{l} \diagup P_3 \\ \diagdown \bar{A}_1 \end{array} \end{array} \right\}.$$

Если у субъекта x структура остается прежней, то это означает неспособность субъекта x различить действия по параметрам P_3 и $\bar{A}_1$. Действия конкурента в этом случае для него невидимы. То есть на множестве всех структур вводится *отношение эквивалентности* для x:

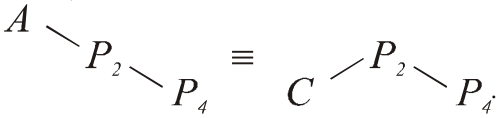


Это отношение эквивалентности вводит стереотипную схему и сужает множество параметров, вводимых гипотезой исследователя в исходной модели (рис. 1). Такое равенство будем называть *стереотипной схемой первого рода*. Она связана с движением по функциональной структуре слева направо, т.е. поиск параметров действий под конкретные цели. Т.к. добавлять параметры и тем самым увеличивать структуру вправо можно бесконечно, то соответственно в любой структуре присутствует бесконечное количество стереотипных схем, но увидеть их можно только если ввести эти параметры. Это одно из существенных информационных ограничений в конфликте.

Однако расширять функциональную структуру можно и влево. Движение по графу справа налево связанно с процессом смыслообразования, т.е. смысл тех или иных действий рассматривается с точки зрения некоторой более общей цели, как, например, для следующей функциональной структуры субъектов *x* и *y*:

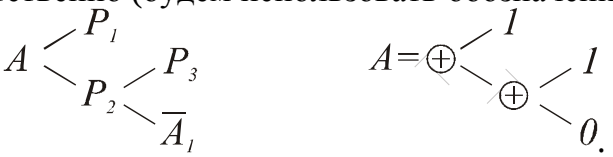


Здесь у субъекта *y* присутствует стереотипная схема, в результате чего он становится неразличимым по целям ***A*** и ***C***.



Это – *стереотипные схемы второго рода*. Они связаны с поиском смысла действий по конкретным параметрам.

В рамках образов каждого из субъектов можно говорить о достижимости той или иной цели. Целями, как уже говорилось, являются крайние левые элементы в структуре. Их оставляют без изменений, а крайние правые элементы заменяются на *1*, если это обычные параметры и *0*, если это – параметры, способствующие *не* достижению данной цели. Остальные элементы заменяются на «и» и «или» соответственно (будем использовать обозначения · и +):



В результате получаем: $A = 1 \oplus (1 \oplus 0) = 1$, т.е. в рамках данной функциональной структуры цель ***A*** достижима. Данный математический аппарат дает возможность рефлексивного управления субъектом в конфликте и манипулирования его выбором (отказ от активных действий).

По данным функциональным структурам вводятся три способа отхода от стереотипных схем:

1. Поиск дополнительных параметров. Этот способ связан со стереотипными схемами первого рода, т.е. поиск дополнительных крайних правых элементов в графе. Этот способ переводит систему ко 2-

му классу или 3-му, если вводимые параметры являются для исследователя ненаблюдаемыми.

2. Введение дополнительной «цели-субъекта». Характеризует возможность цели в функциональных структурах быть никак не привязанной к конкретным субъектам. Тем самым расширяется множество значений функции, и система уводится в область функциональной невидимости (4 класс).
3. Функциональный шум. Этот метод подразумевает совершения действий по параметрам, не имеющим смысла в рамках ключевой цели. Он также не дает возможность постановки задачи исследования и относится к 4-му классу.

Функциональная структура информированности дает возможность манипулирования выбором действий субъекта по конкретным параметрам, что позволяет сформулировать методику корректировки функциональных структур с целью получения выигрыша в конфликте. Данная методика выражается в последовательности действий: расширить дерево параметров как можно больше вправо, завершить ветки нулевыми параметрами по цели противника, по параметрам, где есть контратаки, - применить обратное дезинформирование, по параметрам, где нет контратак, - применить прямое дезинформирование, применить функциональный шум относительно реальной цели.

Только для модели исследователя первого класса, можно строго сформулировать принцип получения новых знаний, для всех остальных классов это невозможно. Защищая систему от исследования, нам необходимо перевести ее в один из классов 2-4. Каждому из этих классов можно сопоставить метод защиты от исследования систем. Для моделей первого класса, единственным затруднением может являться лишь очень большое число входов или неприемлемо большой диапазон входных значений, необходимых для исследования системы. Нельзя рассматривать это как самостоятельный метод защиты от исследования систем. Методы защиты от исследования классифицируются по классам 2-4, т.е. всего получается 3 основных метода защиты от исследования систем.

1. Добавление нефункционального преобразования системы по дополнительным параметрам. Суть этого метода в переводе исследователя к модели второго класса, то есть к кортежу:

$$\mathbf{par}' \neq \mathbf{par},\ \mathbf{par} \in \mathbf{S}_v,\ \{f(\mathbf{par})\} \in \mathbf{F}_v.$$

В данном случае необходимо привести систему в состояние $\mathbf{par}' \neq \mathbf{par}$. В реальных ситуациях просто изменить процесс и сделать его принципиально другим невозможно, поэтому чтобы добиться неравенства (несоответствия исходной стереотипной схемы) вводятся дополнительные параметры, бессмысленные с точки зрения целевой функции системы. При этом необходимо, чтобы целевая функция системы оставалась неизменной.

$$f : \mathbf{par} \to \{f(\mathbf{par})\}.$$

Поскольку исследователю необходимо будет добиться равенства $\mathbf{par}' = \mathbf{par}$ простым перебором гипотез, то, следовательно, и сложность исследования можно ввести как разность мощности этих множеств

$$m = |\mathbf{par}| - |\mathbf{par}'|.$$

Усложняя процесс, его представляют как композицию двух функций

$$f = f_1 \circ f_2,$$

$$f_1 : \mathbf{par} \times \mathbf{par\_d} \to \{ f_1(\mathbf{par}, \mathbf{par\_d}) \},$$

$$f_2 : \{ f_1(\mathbf{par}, \mathbf{par\_d}) \} \times \mathbf{par\_d} \to \{ f(\mathbf{par}) \}.$$

В результате, сложность исследования характеризуется количеством введенных в процесс дополнительных параметров $m = |\mathbf{par\_d}|$. Совокупность этих параметров и функций отклонения по ним определяют *концепцию уникальности системы*.

Каждую из функций f_1 и f_2 можно представить в виде функциональной декомпозиции, и далее каждую из полученных функций можно снова представить в виде функциональной декомпозиции и т.д.

2. Увод процесса в область параметрической невидимости

В соответствии с этим методом система приводится к третьему классу, представленную кортежем:

$$\mathbf{par}' \neq \mathbf{par}, \ \mathbf{par} \notin \mathbf{S}_v, \ \{ f(\mathbf{par}) \} \in \mathbf{F}_v.$$

То есть система приводится к параметрической невидимости для злоумышленника, где $\mathbf{par} \notin \mathbf{S}_v$. Примером может служить изменение бизнес-процессов организации в соответствии с ноу-хау, сохраняемом как коммерческая тайна, шифрование информации о системе безопасности, закрытие внутренней сети организации файрволом для невозможности сканирования.

Все это относится к области *защиты информации* и не составляет определенную область исследования: «информационные ограничения, которые формирует исследователь при построении объектов идеального мира». Данный метод приведен для того, чтобы не терять системность изложения материала. Однако именно такого рода защита информации воспринимается сегодня всеми как единственный метод защиты от исследования систем.

3. Увод процесса в область функциональной невидимости

Суть данного метода в приведении системы к четвертому классу, представленного кортежем:

$$\mathbf{par}' \neq \mathbf{par}, \ \mathbf{par} \notin \mathbf{S}_v, \ \{ f(\mathbf{par}) \} \notin \mathbf{F}_v.$$

Для этого необходимо в исходную функцию ввести дополнительные параметры, но при этом преобразование не является обратимым, а расширяет множество значений целевой функции

$$f' : \mathbf{par} \times \mathbf{par\_d} \to \{ f'(\mathbf{par}, \mathbf{par\_d}) \}.$$

Новые значения функции выходят за область функциональной видимости исследователя, вследствие чего он наблюдает исходную функцию черного ящика. Это определяет отношение эквивалентности между исходной и полученной функциями системы.

$$\forall\, p' \in \mathbf{par}, p \in \mathbf{par\_d} : f(p') \equiv f'(p', p).$$

В результате получается отношение эквивалентности (неразличимости) по значениям функции *f'*:

$$\equiv : \{ f'(\mathbf{par}, \mathbf{par\_d}) \} \to \{ f'(\mathbf{par}, \mathbf{par\_d}) \}$$

$$\forall\ p' \in \mathbf{par},\ p_1 \in \mathbf{par\_d},\ p_2 \in \mathbf{par\_d}:$$
$$f'(p', p_1)(\equiv) f'(p', p_2).$$

В соответствии с выражением (1) исследователь всегда может сопоставить функции $f'(\mathbf{par}, \mathbf{par\_d})$ более простую функцию $f(\mathbf{par})$. Это делает невозможным постановку задачи исследования по подбору гипотез относительно вида функции $f'(\mathbf{par}, \mathbf{par\_d})$. Можно рассматривать этот метод как некий «абсолютный» вид защиты, т.к. скрытой становится сама проблема исследования. Однако он имеет очень ограниченную область применения для случаев, когда возможно расширить функционал системы.

Такое расширение очень удобно для технических систем, когда легко может быть расширен ее функционал в пределах «невидимости» пользователя. По такому принципу строится система HoneyPot. Она представляет собой «приманку» для исследователя (злоумышленника), пытающегося совершить атаку в компьютерной сети. Аналог данной системы можно рассматривать для любых систем безопасности. В частности, это система защиты web-ресурсов от sql-инъекций, позволяющая настраивать концепцию уникальности (параметры **par_d**) в области функциональной невидимости злоумышленника. Это не дает ему возможности исследовать реальные уязвимости сайта.

Для конфликтов в активных системах такая функциональная невидимость в подавляющем большинстве случаев строится на основе стереотипных схем, а не реальной неспособности увидеть целевую функцию конкурента. Например, конкурент может добавить в реальную функцию ценообразования на свои услуги дополнительные параметры, учитывающие специфику бренда. При этом его целью является не увеличение продаж, а охват нового сегмента рынка, т.е. борьба за «завтрашних» покупателей. Реальные истории успеха, как правило, часто придерживаются такой схемы, поскольку расширить область своей функциональной видимости конкурентам удается уже слишком поздно. Такая «невидимость» основана на стереотипных схемах второго рода определяемых функциональной моделью конфликта.

В **третьей главе** приводится модель конфликта позволяющая моделировать логику принятия решений контрагентом, а также моделировать процесс исследования в активных системах. В таких системах объект исследования (черный ящик) может сам прогнозировать действия исследователя и корректировать выходную последовательность в рамках своей цели. Классические теоретико-игровые модели (включая теорию рефлексивных игр Д.А. Новикова и А.Г. Чхартишвили) слишком сложны для моделирования динамики реальных систем, в том числе и процесса защиты систем от исследования. В связи с этим была разработана сигнатурная модель субъекта в конфликте, которая дает возможность моделировать механизмы защиты от исследования для организационных систем. Данная модель строится на теоретико-игровой парадигме, но заменяет количественные характеристики функции полезности их качественными показателями – сигнатурой.

Такую модель целесообразно строить для игровых ситуаций, не имеющих решения в чистых стратегиях. Как, например, для следующей матрицы ценности:

$x_+ =$

$\_^+$	0	1
0	0	+1
1	0	-1

$y_- =$

$\_^+$	0	1
0	0	-2
1	-1	-1

.

Данная игра не имеет решения в чистых стратегиях, а поэтому агенты вынуждены руководствоваться гарантирующими стратегиями. Гарантирующие стратегии основаны в данном случае на ранге рефлексии. Решение каждого агента предпринимать или не предпринимать действие основывается на длине цепочке «я думаю, что он думает о том, что думаю я …».

Здесь унифицируется запись таких стратегий с построением более наглядных принципов умозаключений агентов. Для этого возьмем как 0 и 1 в рассмотренном примере – готовность совершить агентом конкретное действие (противодействие). Обозначим исходное состояние объекта конфликта как O и предположим, что в результате активных действий субъекта(ов) объект может быть переведен в состояние O'. Данный переход возможен в результате активных действий субъектов, для которых состояние O' более выгодно, чем O. Для обозначения качественной характеристики (интенции) субъекта будем использовать следующие символы: $(+)$ – субъект готов осуществить переход $O \to O'$ (положительная интенция); $(-)$ – субъект сопротивляется переходу $O \to O'$ (отрицательная интенция); $(\pm)$ – субъект безразлично относится к переходу $O \to O'$ (нулевая интенция).

Интенцию субъекта $x \in N$ будем обозначать как $(\cdot)_x$, представление субъекта x об интенции субъекта y - $(\cdot)_{xy}$, и т.д. Последовательную запись ячеек дерева вида $(+)_x$, $(-)_{xy}$, $(\pm)_{xyx}$ будем называть сигнатурой. Поскольку до каждой ячейки дерева есть только один путь, будем сокращенно записывать сигнатуры по идентификатору последней ячейки, т.е. $(+-\pm)_{xyx}$. Если мы исследуем общие свойства сигнатур вне конкретных субъектов, то идентификаторы у сигнатур будем опускать. Выразим готовность субъекта к активным действиям поставив в соответствие сигнатурной модели субъекта булеву функцию готовности $f:(\cdot)_{x\ldots} \to \{0,1\}$. В качестве *аксиом* введем $f(-)=1$, $f(+)=1$, $f(\pm)=0$. Готовность для других сигнатур выражается путем введения правил (гипотез) «рациональных умозаключений», которые используют субъекты (агенты), принимая решения о возможности совершить действия. Эти правила можно ввести на матрице функций полезности агента:

$x_+ =$

$\_^+$	0	1
0	0 →	+1
1	0 ←	-1

$y_- =$

$\_^+$	0	1
0	0 ↑	-2 ↓
1	-1	-1

$f(+(-\lambda)) = \neg f(-\lambda)$ $\qquad$ $f(-(+\lambda)) = f(+\lambda)$.

Определяя правила принятия решений, можно вводить теоремы, характеризующие функцию готовности агента по всем рангам рефлексии (полному множеству структур информированности в конфликте).

Например,

Теорема 1. $f\left(\{_1\ \{_2\ \ldots\ \{_n\ s\right) = \begin{cases} 1, \text{если n - четное,} \\ 0, \text{если n - нечетное,} \end{cases}$

где σ равен либо $(+)$, либо пустому множеству.

Рассматривая конфликтную ситуацию сразу по всем рангам рефлексии, можно упростить задачу исследования одних агентов другими. Для этого немного расширим нашу модель и представим теперь, что игра разыгрывается множество раз. Наблюдая действия других участников, агенты могут совершать операции осознания и увеличивать свою сигнатуру слева (по аналогии с операторами осознания в теории рефлексивного анализа В.А. Лефевра, здесь оператором осознания будет сигнатура, добавляемая в начало последовательности).

Если поставить агента *x* в позицию исследователя и предположить, что в его интересах прогнозировать функцию готовности агента *y* на каждом следующем шаге, то его задача – понять принцип, по которому агент *y* совершает операцию осознания, т.е. найти функциональную зависимость

$$s_y^i = p_y\left(s_y^{i-1}, \text{par}\right),$$

где **par** – это множество неизвестных параметров, относительно которых агент *y* получает новую сигнатуру s_y^i. Задача *x* теперь сводится к поиску функции p_y. Для этого он, перебирая гипотезы относительно множества **par**, исследует систему как черный ящик. Для данной задачи крайне затруднительно определить отношение эквивалентности, определяемое множеством функциональной невидимости агента, поэтому механизм защиты от исследования – это увеличение размерности множества **par** и затруднение тем самым подбора гипотез относительно структуры осознания агентом *y*.

Однако защита от исследования для *y* не является самоцелью, его задача – получить выигрыш, а для этого необходимо прогнозировать действия *x* – знать его функцию p_x, то есть здесь стоит задача *исследования исследователя*. Если два таких исследователя исследуют друг друга, то может ли в результате один из исследователей получить объективную информацию о контрагенте? Если они оба действуют по принципу исследователя *x* в предыдущем примере, то процесс будет бесконечным, поскольку любая гипотеза, положенная в основу исследования, будет неверной (т.к. у контрагента ее в принципе нет, он сам является исследователем). Такого рода исследователей назовем *исследователями первого рода***.** В.А. Лефевром был предложен особый способ получения информации в рефлексивных системах, который порождает *исследователей второго рода*. Они получают информацию о контрагенте, т.к. сами ее в него закладывает (рефлексивное управление).

Рассмотрим теперь функцию p_y, параметром которой является шаг игры – *i*:

$$s_y^i = p_y\left(s_y^{i-1}, f\left(s_x^{i-1}\right), i\right) = \begin{cases} p\left(s_y^{i-1}, f\left(s_x^{i-1}\right)\right), \text{если } i < n \\ \left(- + p\left(s_y^{i-1}, f\left(s_x^{i-1}\right)\right)\right), \text{если } i > n \end{cases}.$$

Здесь *x*, являясь исследователем первого рода, очень быстро может убедиться в истинности гипотезы

$$s_y^i = p_y\left(s_y^{i-1}, f\left(s_x^{i-1}\right)\right).$$

Таким образом, во второй главе формализован процесс исследования систем, а так же построена функциональная модель структуры информированности в конфликте, определяющая информационные ограничения исследователя в конфликте, и построена сигнатурная модель субъекта, позволяющая моделировать процесс защиты от исследования для организационных систем, в которых присутствуют активные элементы, имеющие собственные цели и способные рационализировать свои действия для их достижения.

В **четвертой главе** для метода дополнения нефункционального преобразования по функциям системы разрабатывается технология защиты технических систем от исследования с введением «концепции уникальности», и рассматриваются примеры ее реализации.

Алгоритм преобразования системы с целью защиты ее от исследования представлен на рис. 2.

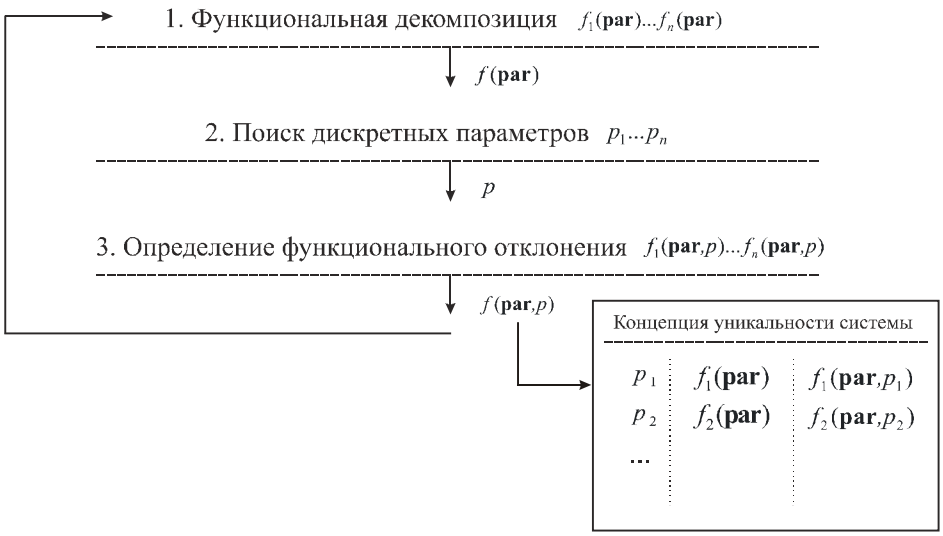


Рисунок 2 – Алгоритм построения «уникальной» системы.

На первом шаге производится функциональная декомпозиция системы, целью которой является выделение подпроцессов для конкретной цели ($f_1(\mathbf{par})...f_n(\mathbf{par})$), где **par** - любые параметры процесса. Например, доступ к базе данных – это последовательная аутентификация, соединение с базой данных и формирование запроса. Аутентификацию, в свою очередь, можно разбить на ввод идентификатора и пароля и т.д.

Второй шаг – для конкретных процессов, полученных в ходе функциональной декомпозиции, ищутся возможные дополнительные параметры, имеющие дискретный характер ($p_1...p_n$). Например, время в минутах, позиция символов, номер сессии и т.д.

После определения дискретных параметров вводится бессмысленное отклонение исходного процесса по его значению ($f_1(\mathbf{par},p)...f_n(\mathbf{par},p)$).

Например, для ввода пароля – это смещение символов на клавиатуре в зависимости от их позиции в строке, для коммутации – это перераспределение портов и адресов компьютеров в сети в зависимости от номера сессии и пр. Функция отклонения должна быть отражена в концепции уникальности системы. Зная ее, можно восстановить исходную функциональную структуру.

В области безопасности рациональнее закрывать от исследования самые популярные уязвимости, совершая атаку, по которым нарушитель не получал бы информативной обратной связи. Сценарий такого подхода достаточно прост – пытаясь реализовать простые уязвимости, злоумышленник не наблюдает «сопротивления» системы, а следовательно – тратит много времени на «распутывание» логики ее работы. Можно сказать, что он «вязнет» в системе, т.к. будучи не в состоянии правильно интерпретировать обратную связь, он не совершает действий в рамках поставленной им цели. В это время сама система легко протоколирует несанкционированную активность, т.к. обнаруживает действия по стереотипным схемам.

Принцип действия системы защиты от исследования основан на неразличимости для контрагента реакции информационной системы. Например, по формируемому им запросу к базе данных, т.е. функциональной невидимости за счет невидимости параметров, используемых сервером при формировании соединения с базой данных.

Например, обозначим через p запрос к базе данных сайта, формируемый системой на основании информации передаваемой через массивы *$GET* и *$POST*. Система управления базой данных (MySQL) обрабатывает запрос и выдает ответную реакцию – $query(p)$.

Введем в этот процесс дополнительный параметр – p_1. Он может принимать всего два значение – 0 и 1. Значение единицы он принимает в том случае, если регулярные выражения, проверяющие массивы *$GET* и *$POST*, обнаружили характерные символы для атак ISS и SQL-инъекций.

Формирование запроса к базе данных показано на рис.3.

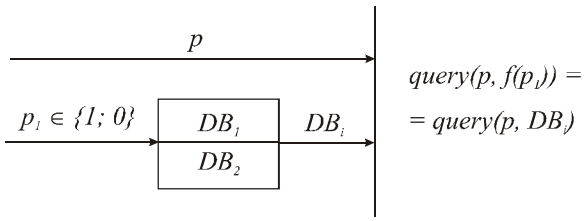


Рисунок 3 – Формирование запроса к базе данных

DB_1 – исходная (оригинальная) база данных сайта. На ее основе создается копия – DB_2, из которой можно убрать (подменить) нужную информацию.

Разработанный в ходе диссертационного исследования модуль работы с базой данных (PRIS Mirror) включает настройку концепции уникальности системы, увеличивая тем самым многообразие структуры и содержания базы данных. Технология защиты от исследования требует введения множества дискретных параметров $p_1, \ldots, p_n$, относительно которых можно ввести функцию отклонения системы $f(p_1, \ldots, p_n)$. Поскольку результатом должен быть запрос

$$query(p, f(p_1, \ldots, p_n)) = query(p, DB_i),$$

то функция f есть отображение на множество баз данных:

$$f(p_1,...,p_n) \in \left\{DB_1, DB_2, DB_2^{\ 1}, DB_2^{\ 2},..., DB_2^{\ m}\right\}.$$

Принцип формирования запроса для такой функции показан на рис.4.

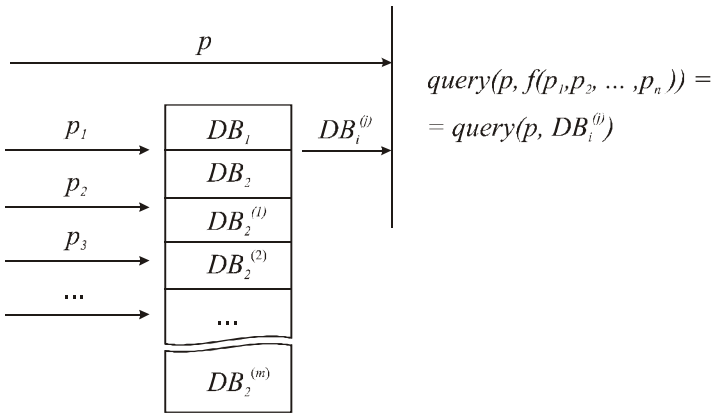


Рисунок 4 – Формирование запроса к базе данных для модуля PRIS Mirror

Запись баз данных с двумя индексами отражает принцип их формирования. DB_1 – исходная (оригинальная) база данных сайта. DB_2 – как и в предыдущем примере – копия ее структуры с пустыми таблицами. Если в концепции уникальности прописаны правила модификации структуры в зависимости от найденных параметров, то структура DB_2 меняется и формируется новое состояние $DB_2^{(j)}$.

Такой подход позволяет администратору добавлять в работу сайта (запрос к базе данных) любые дополнительные параметры и строить, таким образом, уникальную с точки зрения защиты от исследования систему.

Механизмы защиты от исследования не подразумевают блокирование уязвимостей (хотя и не исключают их применение). Здесь используется принципиально иной ресурс защиты от преднамеренных атак – информационное управление нарушителем, а, следовательно, технология защиты от исследования позволяет дополнительно снижать риск систем информационной безопасности. Рассмотренные механизмы являются примером технической реализации данной технологии.

В заключении диссертации приводятся основные результаты работы, полученные в ходе исследований и делаются общие выводы.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ И ВЫВОДЫ

При решении поставленных в диссертационной работе задач получены следующие научные результаты.

1. Построена модель исследователя, на основе которой введено три класса информационных ограничений в конфликте. Введен показатель глубины отклонения функционального состояния структуры, характеризующий сложность подбора гипотез в процессе исследования системы.
2. Разработаны методы функционального преобразования структуры систем с целью защиты их от исследования: добавление нефункционального преобразования по дополнительным параметрам и увод процесса за пределы области параметрической и функциональной видимости.

3. Построена функциональная модель структуры информированности в конфликте, позволяющая рассматривать действие как процесс и ставящая в соответствие цели и параметры их достижения. Введен метод представления достижимости цели в рамках информационных ограничений субъекта конфликта. Найдены три способа отклонения функциональной структуры от стереотипных схем, а также методика достижения информационного превосходства в конфликте.
4. Построена сигнатурная модель субъекта в конфликте, представляющая собой упрощенную теоретико-игровую модель конфликта с заменой количественных показателей функции полезности качественными переменными – сигнатурой, на которой вводится функция готовности агентов к совершению активных действий. Для данной модели сформулировано и доказано семь теорем.
5. На основе разработанных методов и моделей предложена технология повышения безопасности информационных систем за счет защиты их от исследования злоумышленником. Данная технология апробирована на примере защиты веб-сервера, где ранее атаки имели успех в 7 случаях из 100, при этом среднее время успешной атаки составляло 10-15 минут. За время тестирования установленной системы было предпринято более 150 преднамеренных атак, из которых ни одна не завершилась успешно, при этом среднее время атаки составило 1,5-2 часа.

Таким образом, в диссертации разработаны методы, модели и алгоритмы защиты от исследования систем, а также модели их функционального представления, что имеет существенное значение для теории и практики повышения уровня безопасности использования информационных технологий.

Основные публикации по теме диссертации:

1. Семенкин, Е.С. Защита от исследования и ее применение в системах безопасности / Е.С. Семенкин, М.А. Стюгин // Вестник Сибирского государственного аэрокосмического университета имени академика М.Ф. Решетнева. – Вып. 2 (23). – 2009. – С. 66-70.
2. Семенкин, Е.С. Повышение информационной безопасности веб-сервера методом защиты от исследования / Е.С. Семенкин, М.А. Стюгин // Программные продукты и системы. – № 3. – 2009. – С. 29-32
3. Стюгин, М.А. Планирование действий в конфликте на уровне функциональных структур / М.А. Стюгин // Информационные войны. – №2. – 2009. – С. 18-24.
4. Стюгин, М.А. Анализ сигнатурной модели субъекта в конфликте / М.А. Стюгин // Информационные войны. – № 3. – 2009. – С. 12-23.
5. Стюгин, М.А. Методы защиты от исследования систем / М.А. Стюгин // Информационные войны. – № 4. – 2009. – С. 23-29.
6. Стюгин, М.А. Технологии информационного противоборства в системах информационной безопасности / М.А. Стюгин // Ползуновский альманах №4. – 2008. – С. 220-222.
7. Стюгин, М.А. Планирование оптимальных параметров подсистемы защиты информации с использованием рефлексивных игр / М.А. Стюгин // Инновационные недра Кузбасса. IT-технологии: сборник научных трудов. - Кемерово: ИНТ, 2007. – С. 404-408.
8. Стюгин, М.А. Рефлексивное управление в системах безопасности / М.А. Стюгин // Проблемы безопасности современного мира и управления рисками. Материалы XII Всероссийской научно-практической конференции с международным участием. - Иркутск, 2007. – С. 314-317.

9. Стюгин, М.А. Рефлексивное планирование в системах информационной безопасности / М.А. Стюгин // Актуальные проблемы безопасности информационных технологий: Материалы I Международной заочной научно-технической конференции – Красноярск, 2007. - С. 103-111.
10. Стюгин, М.А. Информационная безопасность «по существу» / М.А. Стюгин // Актуальные проблемы безопасности информационных технологий: Сб. научн. трудов / Под общей ред. О.Н. Жданова, В. В. Золотарева; Красноярск: СибГАУ, 2007. – С. 102-123.
11. Стюгин, М.А. Рефлексивный аспект информационной безопасности / М.А. Стюгин // VI Международный научно-практический междисциплинарный симпозиум «Рефлексивные процессы и управление». - Москва, 2007. - С. 110-112.
12. Стюгин, М.А. Сигнатурная модель субъекта в конфликте и ее исследование / М.А. Стюгин // Решетневские чтения: материалы XI Международной научной конференции посвященной памяти академика М.Ф.Решетнева – Красноярск, СибГАУ, 2007. - С. 257-258.
13. Стюгин, М.А. Информационное превосходство в контексте безопасности / М.А. Стюгин // Проблемы управления безопасностью сложных систем. Труды XV международной конференции. – Москва: ИПУ РАН, 2007. – С. 273-276.
14. Стюгин, М.А. Специфический метод защиты от информационных атак / М.А. Стюгин // Проблемы управления безопасностью сложных систем. Труды XV международной конференции. – Москва: ИПУ РАН, 2007. – С. 259-262.
15. Стюгин, М.А. Технологии информационной борьбы в конфликте / М.А. Стюгин // Инновационные недра Кузбасса. IT-технологии: сборник научных трудов. - Кемерово: ИНТ, 2008. – С. 267-271
16. Стюгин, М.А. Информационное противоборство на уровне функциональных структур / М.А. Стюгин // Проблемы регионального и муниципального управления. Труды IX международной конференции. - Москва. РГГУ, 2008 – С. 121-125
17. Стюгин, М.А. Защита от исследования в системах информационной безопасности / М.А. Стюгин // Решетневские чтения: материалы XII Международной научной конференции посвященной памяти академика М.Ф.Решетнева – Красноярск, СибГАУ, 2008. – С. 67-69.
18. Стюгин, М.А. Информационные операции в антагонистических конфликтах / М.А. Стюгин // Проблемы управления безопасностью сложных систем. Труды XVI международной конференции. – Москва: ИПУ РАН, 2008. – С. 199-202.
19. Стюгин, М.А. Создание «хаоса» с целью защиты от исследования / М.А. Стюгин // Проблемы управления безопасностью сложных систем. Труды XVI международной конференции. – Москва: ИПУ РАН, 2008. – С. 378-381.
20. Стюгин, М.А. Иммунная система информационной безопасности / М.А. Стюгин // Проблемы регионального и муниципального управления. Труды IX международной конференции. - Москва. РГГУ, 2009. – С. 217-219.
21. Стюгин, М. А. Информационная безопасность и проблемы исследователя в конфликте / М.А. Стюгин // Рефлексивные процессы и управление. Сборник материалов VII Международного симпозиума. – Москва.: Когито-Центр, 2009. – С. 254-257.
22. Стюгин, М.А. Методы защиты систем от исследования / М.А. Стюгин // Проблемы управления управления безопасностью сложных систем. Труды VII международной конференции. – Москва. ИПУ РАН, 2009. – С 235-239.

Формат 60x84 1/16 Бумага офсетная.
Печать офсетная. Усл.п.л. - 1
Заказ № Тираж 100 экз.

Сибирский государственный аэрокосмический университет им. академика М.Ф. Решетнева
660014, г.Красноярск, пр.газ.Красноярский рабочий, 31