На правах рукописи

Кравченко Алексей Алексеевич

ИНСТРУМЕНТАЛЬНЫЕ МЕТОДЫ АНАЛИЗА ЗАЩИЩЕННОСТИ ЭКОНОМИЧЕСКИХ ИНФОРМАЦИОННЫХ СИСТЕМ ТЕРРИТОРИАЛЬНЫХ ОРГАНОВ УПРАВЛЕНИЯ

Специальность 08.00.13 – математические и инструментальные методы экономики

Автореферат

диссертации на соискание ученой степени
кандидата экономических наук

Ростов-на-Дону – 2009

Работа выполнена в ГОУ ВПО «Ростовский государственный экономический университет (РИНХ)».

Научный руководитель:	доктор экономических наук, доцент, **Тищенко Евгений Николаевич.**
Официальные оппоненты:	доктор экономических наук, профессор, **Крюков Сергей Владимирович.**
	кандидат экономических наук, доцент, **Щербаков Сергей Михайлович.**
Ведущая организация:	**Ростовский государственный университет путей сообщения.**

Защита диссертации состоится 21 декабря 2009 года в 14^{30} часов, на заседании диссертационного совета ДМ 212.209.03 в ГОУ ВПО «Ростовский государственный экономический университет (РИНХ)» по адресу: 344002, г. Ростов-на-Дону, ул. Б. Садовая 69, ауд. 231

С диссертацией можно ознакомиться в научной библиотеке и на сайте www.rsue.ru ГОУ ВПО «Ростовский государственный экономический университет (РИНХ)».

Автореферат разослан 20 ноября 2009 года.

Ученый секретарь
диссертационного совета **И.Ю. Шполянская**

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. По мере развития и усложнения средств, методов и форм защиты все более обостряется проблема оценки их качества, выработки критериев, которым должен соответствовать тот или иной тип систем защиты. Это особенно актуально в контексте создания, внедрения и эксплуатации защищенных сред функционирования распределенных информационных систем и, следовательно, как их вариант, экономических информационных систем территориальных органов управления (ЭИС ТОУ), в связи с тем, что именно защищенность, как показатель потребительского качества ЭИС ТОУ, в современных условиях является наиболее важным.

Известно, что при организации тех или иных сетевых и телекоммуникационных топологий потенциальная уязвимость обрабатываемой в среде ЭИС ТОУ информации резко возрастает. Это объясняется возникновением многовариантности возможных каналов доступа к процессорным узлам сети, массивам хранимой информации и сегментам сетевых топологий. В связи с этим оценка качества реализации механизмов защиты от несанкционированного доступа (НСД) является одной из основных задач при анализе защищенности ЭИС ТОУ.

Степень разработанности проблемы. Попытки разработки методологических подходов и инструментальных средств, обеспечивающих анализ потребительского качества систем защиты информации (СЗИ) и защищенности информационных систем, предпринимались многими отечественными и зарубежными авторами: В. Герасимовым, Д. Гроувером, Д. П. Зегенда, С. Мафтиком, Д. Сяо, Л. Дж. Хоффманом, В. В. Мельниковым, А.Г. Мамиконовым А. Астаховым, Г. Н. Хубаевым, Е. Н. Тищенко и многими другими. Ими были проанализированы отдельные методы и средства защиты, рассмотрены некоторые существующие системы защиты. Однако нам неизвестны в достаточной мере серьезные попытки ранжирования

выделенных критериев качества систем защиты, привязки их к конкретным условиям функционирования ЭИС ТОУ. Не проводилась сравнительная экономическая оценка потребительского качества систем защиты ЭИС ТОУ в связи с трудностями оценки затрат живого труда и машинного времени на их эксплуатацию и вскрытие.

Анализ показывает, что задача создания эффективной защищенной среды функционирования ЭИС ТОУ состоит из таких подзадач, как: качественная сегментация топологии ЭИС ТОУ; адекватный выбор базовых составляющих защищенной среды ЭИС ТОУ на основе перечня функциональных характеристик и потенциальных угроз, а также на основе экспертной оценки специалистов в области информационной безопасности. По утверждениям отечественных и зарубежных специалистов, решение этих задач наталкивается на большие трудности, что обуславливается нечеткостью и большой неопределенностью исследуемых процессов.

Перечисленные задачи и определили содержание настоящего исследования. Несмотря на большое количество публикаций, ни одна из этих задач не изучена в степени, достаточной для анализа защищенности, как одного из важнейших показателей потребительского качества ЭИС ТОУ.

Цель и задачи диссертационного исследования. Основной целью диссертации является развитие инструментария оценки потребительского качества защищенной среды функционирования ЭИС ТОУ на основе анализа ее параметров и разработки экономико-математических моделей для принятия решений при создании, эксплуатации и развитии средств и методов построения защищенной среды ЭИС ТОУ.

Поставленная в работе цель обусловила решение следующих научных проблем и практических задач:

- анализ отечественных и зарубежных исследований, посвященных определению содержательной сути построения защищенной среды функционирования ЭИС ТОУ и экономико-математическим моделям, разработанным для оценки ее качества;

- разработка и развитие подходов к качественной сег ментации ЭИС ТОУ для возможности осуществления оценки эффективности и построения адекватной защищенной среды ЭИС ТОУ;

- разработка методологии сравнительного экономического анализа эффективности защищенной среды ЭИС ТОУ;

- разработка и реализация программного инструментария для анализа потребительского качества защищенной среды ЭИС ТОУ.

Объект исследования. Объектом исследования являются экономические информационные системы территориальных органов управления субъектов РФ.

Предмет исследования. Предметом исследования являются процессы обеспечения защищенности ЭИС ТОУ.

Теоретическая база исследования. Теоретическую и методологическую базу исследования составляют научные труды российских и зарубежных ученых по теории выбора и принятия решений, экономико-математическому моделированию, а также теоретические и методологические вопросы оценки защищенности ЭИС ТОУ. В проведенном исследовании использовались элементы теории информационных систем и статистического анализа, а также экспертные методы.

Работа проведена в рамках пункта Паспорта специальности 08.00.13 – математические и инструментальные методы экономики: 2.6 «Развитие теоретических основ, методологии и инструментария проектирования, разработки и сопровождения информационных систем субъектов экономической деятельности: методы формализованного представления предметной области, программные средства, базы данных, корпоративные хранилища данных, базы знаний, коммуникационные технологии».

Эмпирическая база исследования. Эмпирической базой исследования явились экспериментальные и статистические данные, собранные в процессе эксплуатации ЭИС ТОУ Ростовской области. Основные выдвигаемые

научные положения и рекомендации экспериментально подтверждены. Поставленные эксперименты с ЭИС ТОУ и их компонентами составляют основу предлагаемого инструментария исследования защищенности ЭИС ТОУ.

Положения, выносимые на защиту. На защиту выносятся следующие положения:

1. Методика определения параметров сегментирования ЭИС ТОУ на базе модели защиты с полным перекрытием для обеспечения максимально возможного контроля трафика между сегментами.

2. Алгоритм сравнительного анализа программных систем защиты ЭИС ТОУ по функциональной полноте и закрываемым угрозам при проектировании и использовании защищенной среды функционирования ЭИС ТОУ.

3. Методика определения вероятности вскрытия базовых элементов защищенной среды функционирования ЭИС ТОУ на основе экспертных методов.

4. Методика определения потребительского качества распределенной системы защиты ЭИС ТОУ с единым центром управления.

Научная новизна. Научная новизна работы заключается в решении проблемы создания целостного инструментального обеспечения для оценки потребительского качества и моделирования характеристик функционирования защищенной среды ЭИС ТОУ. Научную новизну содержат следующие положения:

1. Разработана модель определения параметров сегментирования ЭИС ТОУ, отличающаяся учетом таких характеристик, как размер сегмента, состав информационных элементов и узлов сегмента. Модель позволяет формулировать требования к проектируемой или модифицируемой ЭИС ТОУ при решении задачи обеспечения ее защищенности, как показателя потребительского качества.

2. Определен перечень характеристик элементов защищенной среды ЭИС ТОУ (более 130), отличающийся структурированием данных элементов в соответствии с функциональным назначением. Перечень позволяет на базе формализованных процедур провести сравнительный анализ программных систем защиты ЭИС ТОУ.

3. Определен перечень угроз информационным объектам ЭИС ТОУ, отличающийся более полным, по сравнению с содержанием баз данных коммерческих средств анализа защищенности экономических информационных систем, составом угроз и позволяющий на базе формализованных процедур провести сравнительный анализ элементов защищенной среды.

4. С использованием экспертных методов проранжирован перечень характеристик базовых элементов защищенной среды ЭИС ТОУ, отличающийся наличием рассчитанных вероятностных значений каждой из характеристик и позволяющий определять общую вероятность вскрытия конкретного базового элемента.

5. Предложен метод анализа защищенности ЭИС ТОУ, отличающийся учетом наличия в структуре распределенной системы защиты единого центра управления. Данный метод позволяет определять потребительское качество распределенной системы защиты ЭИС ТОУ.

Практическая значимость исследования. Практическая значимость исследования определяется тем, что основные положения, выводы, рекомендации, модели, методы и алгоритмы ориентированы на широкое использование экономико-математического, алгоритмического обеспечения и инструментальных средств и могут быть использованы территориальными органами управления субъектов РФ для принятия решения в области обеспечения защищенности ЭИС ТОУ.

Апробация и внедрение результатов исследования. Основные результаты докладывались и обсуждались на международных и всероссийских симпозиумах и конференциях, в том числе: Всероссийская

научно-практическая конференция «Проблемы информационной безопасности» (Ростов-на-Дону, 2008, 2009 г.г.); Международная научно-практическая конференция «Информационная безопасность» (Таганрог, 2007); Научно-практическая конференция «Статистика в современном мире: методы, модели, инструменты» (Ростов-на-Дону, 2008, 2009 г.г.) и другие.

Основные положения, полученные в результате проведенного исследования используются при чтении курсов специальностей «Прикладная информатика» («Информационная безопасность») и «Организация и технология защиты информации» («Введение в специальность», «Теория информационной безопасности и методология защиты информации», «Защита информационных процессов в компьютерных системах») в Ростовском государственном экономическом университете (РИНХ).

Отдельные результаты диссертационной работы использованы при анализе защищенности ЭИС ТОУ в образовательной деятельности (Ростовский государственный экономический университет (РИНХ)), в деятельности администраций субъектов РФ (администрация г. Ростова-на-Дону), а также в деятельности коммерческих организаций (ООО «Ростовский-на-Дону центр «Акра»».

Результаты исследования использованы в типовом прикладном программном обеспечении: «Service Providing Cost» (Свидетельство о государственной регистрации программы для ЭВМ в Федеральной службе по интеллектуальной собственности, патентам и товарным знакам №2009615770).

Публикации. Основные результаты диссертации изложены в 6 научных работах, в том числе в сборниках, рекомендованных ВАК РФ. Общий объем авторских публикаций по теме 1,05 печатных листа.

Структура и объем работы. Диссертационная работа состоит из введения, 3 глав, заключения, библиографического списка и приложений. Работа содержит 119 страниц текста, 19 таблиц, 10 рисунков и графиков. Библиографический список содержит 214 литературных источников.

ОСНОВНЫЕ ПОЛОЖЕНИЯ ДИССЕРТАЦИИ

Во введении обосновывается актуальность проблемы, формулируются цель и задачи исследования, определяются предмет и объект исследования, рассматриваются теоретические и методологические основы исследования, научная новизна, практическая значимость работы, положения, выносимые на защиту, оценка внедрения и апробации исследования, публикации, структура диссертационной работы.

В главе 1 «Общие вопросы анализа защищенности ЭИС ТОУ» выполнен анализ структуры и особенностей ЭИС ТОУ, основных принципов организации защищенных ЭИС ТОУ, а также сформулированы и систематизированы критерии качества сегментации ЭИС ТОУ.

Структура и особенности ЭИС ТОУ. ЭИС ТОУ предназначена для автоматизации административных функций территориальных органов управления. ЭИС ТОУ состоит из ряда функциональных ЭИС, территориально разнесенных и связанных единой средой передачи данных. Отдельная ЭИС, установленная в каком-либо органе власти и управления, является узлом ЭИС ТОУ. Каждый узел ЭИС ТОУ физически является локальной вычислительной сетью или отдельным компьютером и представляет собой одно или несколько автоматизированных рабочих мест сотрудников соответствующих подразделений территориальных органов управления. Все информационные узлы могут быть связаны между собой через различные коммуникации. В результате информационные узлы образуют интегрированную распределенную территориальную экономическую информационную систему.

ЭИС ТОУ представляет собой унифицированную программную среду, в результате внедрения которой по определенной методике предлагается создавать интегрированную информационную систему, автоматизирующую работу территориальных органов управления, содержащую сеть узлов с

распределенным хранением данных и с возможностью корпоративного использования данных всеми узлами сети.

ЭИС ТОУ решают две основные группы задач:

Первая - автоматизация первичных административных операций при работе с населением или юридическими лицами - регистрация, лицензирование, начисление, оформление, прием заявлений, контроль исполнения поручений и т.д. В результате повышается производительность работы низовых органов власти и управления, повышается корректность и достоверность вносимых данных. При этом параллельно с автоматизацией работы сотрудников аппарата управления, осуществляющих первичные операции, формируются компьютерные базы данных по всем информационным ресурсам территории.

Вторая - информационная поддержка принятия решений руководителем и обеспечение всех аспектов социально-экономического управления и устойчивого развития территории на основе анализа и обработки всех первичных информационных ресурсов.

Для решения второй группы задач важно, чтобы ЭИС ТОУ административного управления предоставляла бы возможность использования всех компонентов информационных ресурсов вне зависимости от ведомственной подчиненности органов, производящих их первичное накопление. В этом случае информационные ресурсы территории являются основой поддержки принятия и контроля исполнения решений по управлению территорией, включая формирование достоверной налогооблагаемой базы и реально сбалансированных бюджетов, планирование и контроль за расходами, реализация обоснованной адресной социальной помощи и т.д. Интегрированные информационные ресурсы территории могут быть основой для разработки программ социально-экономического развития территории, для формирования инвестиционных проектов или для создания верифицированной государственными органами электронной биржи недвижимости, товаров, услуг, инвестиций и проектов.

При этом обеспечение информационной безопасности инфраструктуры ЭИС ТОУ на сегодняшний день является одной из основных.

Основные принципы организации защищенных ЭИС ТОУ. Учитывая возможную пространственную и организационную удаленность элементов ЭИС ТОУ как друг от друга, так и от управляющего единого центра, система безопасности должна предусматривать реализацию хотя бы одного из своих механизмов на каждом возможном пути проникновения в ЭИС ТОУ. Такая структура определяет модель системы безопасности с полным перекрытием[1].

В модели с полным перекрытием множество отношений объект-угроза образуют граф, в котором ребро $<t_i,o_i>$ определяет угрозу получения доступа к объекту o_i методом t_i. В случае ЭИС ТОУ каждая осуществленная угроза потенциально преобразует объект o_i в новую угрозу t'_i для достижимых новых объектов o'_i. Это приводит к тому, что практически каждый элемент ЭИС ТОУ становится источником угрозы. Данному распространению угроз способствует архитектура ЭИС ТОУ, в которой каждый элемент имеет каналы связи с определенным количеством других элементов.

При этом набор механизмов обеспечения безопасности и разделения (сегментации) $m_1,m_2,...,m_n$ преобразует граф, существенно уменьшая количество ребер объект - угроза. Причем, чем сильнее уровень сегментации, тем меньшее количество угроз реализуется с порождением новых угроз. В идеальном варианте в системе с полным перекрытием для ЭИС ТОУ каждое $<t_i,o_i>$ предусматривает $<t_i,o_i,m_i>$, доводя степень сегментации до уровня конечных узлов.

Критерии сегментации ЭИС ТОУ. Как отмечалось выше, степень сегментации при повышении требований к безопасности ЭИС ТОУ стремится к уровню конечных узлов ЭИС ТОУ. Однако при этом необходимо

[1] Хоффман Л. Дж. Современные методы защиты информации: Пер. с англ./ Под ред. В.А. Герасименко. - М.: Сов. радио, 1980.

учитывать целый ряд ограничений, накладываемых на глубину сегментации. Ограничения определяются, исходя из:

- топологии ЭИС ТОУ;
- решаемых задач;
- конфиденциальности обрабатываемой информации;
- политики безопасности;
- финансовых и организационных возможностей администрации сегментов ЭИС ТОУ;
- операционных сред узлов ЭИС ТОУ и других условий.

Определение правильного сценария сегментации на этапе проектирования ЭИС ТОУ, а также при последующей модификации ее структуры является одним из главных условий дальнейшего адекватного функционирования ЭИС ТОУ. Это условие в значительной степени влияет на экономическую эффективность ЭИС ТОУ, зависящую, во-первых, от качества системы защиты конфиденциальной информации, а во-вторых, от количества используемых средств защиты. При этом следует принимать во внимание их высокую рыночную стоимость.

Рассмотрим пример сегментации ЭИС ТОУ.

Пусть задана система конечных узлов сегмента ЭИС ТОУ, программных элементов и массивов информации и их характеристики. Необходимо определить параметры сегментации и процедуры защиты от НСД к информации, которые обеспечивают минимальное приращение вероятности главного события НСД при ограничении на размер сегмента сети, на стоимостные и временные затраты, вызванные применением методов сегментации и защиты от НСД: $\Delta Y(P) \rightarrow min$, где $\Delta Y(P)$ - вероятность главного события НСД; $P = (p_1, p_2, ..., p_n)$ - вектор вероятностей базисных событий НСД.

Решение этой задачи обеспечивает определение такого размера сегмента, состава информационных элементов и узлов сегмента, а также

состава методов защиты, при которых приращение $\Delta Y(P)$ оказывается минимальным.

В таблице 1 выделены выбранные методы защиты для конкретного конечного узла. Далее узлы группируются в соответствии с набором необходимых методов защиты и образуют сегменты. Результатом анализа также является перечень методов защиты, которые должны быть реализованы в структуре определенного сегмента.

Таблица 1

Значение коэффициентов целевой функции

Конечный узел	Методы защиты					
	1	2	3	4	5	...
1	$0.85x10^{-6}$	$\mathbf{0.7x10^{-6}}$	$1.03x10^{-6}$	$0.63x10^{-6}$	$0.87x10^{-6}$	...
2	$\mathbf{1.17x10^{-6}}$	$0.52x10^{-6}$	$1.05x10^{-6}$	$0.75x10^{-6}$	$1.21x10^{-6}$	...
3	$0.92x10^{-6}$	$1.05x10^{-6}$	$1.24x10^{-6}$	$\mathbf{0.3x10^{-6}}$	$0.47x10^{-6}$	...
4	$0.43x10^{-6}$	$0.18x10^{-6}$	$\mathbf{0.09x10^{-6}}$	$0.52x10^{-6}$	$0.3x10^{-6}$	...
5	$0.27x10^{-6}$	$\mathbf{0.19x10^{-6}}$	$1.35x10^{-6}$	$0.87x10^{-6}$	$0.51x10^{-6}$	...
6	$0.38x10^{-6}$	$1.1x10^{-6}$	$1.59x10^{-6}$	$\mathbf{1.24x10^{-6}}$	$0.97x10^{-6}$	...
7	$\mathbf{1.43x10^{-6}}$	$1.21x10^{-6}$	$0.65x10^{-6}$	$1.13x10^{-6}$	$1.7x10^{-6}$	...
8	$1.03x10^{-6}$	$1.4x10^{-6}$	$1.18x10^{-6}$	$0.97x10^{-6}$	$\mathbf{0.21x10^{-6}}$	...
...	...	...	...	...	...	...

В главе 2 «Методы сравнительного анализа систем защиты ЭИС ТОУ» предложен алгоритм сравнительного анализа систем защиты ЭИС ТОУ, состоящий из таких этапов, как сравнительный анализ по функциональной полноте, сравнительный анализ по закрываемым каналам утечки информации, сравнительный анализ методом экспертных оценок.

Сравнительный анализ по функциональной полноте. Основные трудности, с которыми приходится сталкиваться при сравнительной оценке систем защиты, - это неопределенность и сложность продуктов данного класса. При этом на сегодняшний день недостаточно статистических данных (а по некоторым позициям они вообще отсутствуют) для характеристики систем защиты конкретного типа. Следует также отметить, что эксплуатационные параметры существующих систем защиты практически не систематизированы, отсутствуют серьезные исследования в области

сравнительных количественных оценок функциональной полноты коммерческих систем.

В данной ситуации специалистам в области информационной безопасности невозможно в полной мере оценить адекватность реальной системы защиты требованиям объекта защиты. Это, в свою очередь приводит к проблеме оптимального выбора среди однородных продуктов.

Вполне обоснованным, на наш взгляд, является применение формальных процедур сравнения ряда систем защиты по выделенным ранее характеристикам [2]. Данные характеристики могут описывать как функциональные особенности систем защиты, так и такие, как развитость пользовательского интерфейса, количество поддерживаемых платформ и интерфейсов.

Анализ коммерческих программных систем защиты, реализующих функции СЗИ, позволил выделить перечень их характеристик, фрагмент которого приведен в таблице 2.

Таблица 2

Характеристики СЗИ

№	*Характеристики*
1	**2**
Реализуемая функция	
Резервирование/восстановление конфигурации	
1	*резервирование: носитель, комментарий, имя файла;*
2	*восстановление: носитель, имя файла.*
Мониторинг	
3	*протокол событий: сервер, событие, дата и время возникновения, описание;*
4	*состояние сервисов: сервер, сервис, статус, количество сессий, время активизации. Возможные сервисы: Web proxy, Firewall, задания;*
5	*активные сессии: сервер, тип сессии, имя пользователя, имя/IP-адрес компьютера пользователя, IP-адрес интерфейса, дата и время активации;*
6	*отчеты: суммарный, Web-отчет, отчет по приложениям, детальный отчет по трафику, отчет по попыткам нарушения политики безопасности.*
Определение политики доступа	
7	*контентные правила: имя правила, описание, статус (активно/неактивно), объект правила, время действия правила, действие (разрешить/запретить), субъекты правила, контент;*

[2] Хубаев Г.Н. Сравнение сложных программных систем по критерию функциональной полноты//ПРОГРАММНЫЕ ПРОДУКТЫ И СИСТЕМЫ (SOFTWARE&SYSTEMS). – 1998. – №2. – с.6-9.

8	*правила уровня протоколов: имя правила, описание, статус (активно/неактивно), действие (разрешить/запретить), протокол, время действия правила, субъекты правила;*
9	*правила уровня пакетов: имя правила, описание, статус (активно/неактивно), стандартный протокол/создаваемый протокол (IP-протокл, номер протокола, направление), IP-адрес интерфейса протокола, удаленный IP-адрес. Фильтрация на основании IP-адресов отправителя и получателя, фреймов инкапсулированных в IP протоколов, времени и даты передачи пакета, разрешённых портов абонентов (для TCP/UDP-пакетов), а также пар адресов абонентов, для которых разрешено соединение.*
Маршрутизация	
10	*переадресация: имя правила, описание, статус (активно/неактивно), правила переадресации (внутренний IP-адрес, внешний IP-адрес, протокол), субъект правила;*
11	*маршрутизация: имя правила, описание, статус (активно/неактивно), объект правила, действие (перенаправление на локальный адрес, перенаправление на upstream сервер (имя сервера, порт), перенаправление на удаленный компьютер (имя, порт);*
12	*создание таблицы внутренних IP-адресов: диапазон IP-адресов, описание;*
…	…

Для оценки степени поглощения тем или иным СЗИ выделенных функций были рассчитаны значения функционального веса: СЗ1-*5;* СЗ2-*4;* СЗ3-*5;* СЗ4-*0;* СЗ5-*10;* СЗ6-*5;* СЗ7-*5;* СЗ8-*15;* СЗ9-*77.* Наибольшую функциональную полноту (процент характеристик, которым соответствует СЗИ), имеет СЗ9 – СЗИ, разработанная фирмой IS Friendsheep (рисунок 1).

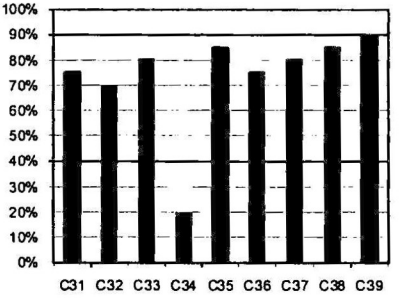

Рис. 1. Значения функциональной полноты СЗИ[3]

[3] Здесь и в дальнейшем обозначения СЗ1, СЗ2, … соответствуют конкретным системам защиты.

Сравнительный анализ по закрываемым уязвимостям. Однако на практике наиболее важно учитывать не только характеристики самой системы защиты, но особенности объекта защиты, который может иметь очень сложный и неоднородный характер. В первую очередь это касается ЭИС ТОУ, построенных на базе современных телекоммуникаций и каналов связи. Такими особенностями могут являться, например, топология вычислительной сети и информационных потоков, а также состав потенциально уязвимых мест и возможных вариантов НСД к информации. Следовательно, и системы защиты необходимо уже оценивать не с точки зрения набора выполняемых функций и качества функциональных характеристик, а с точки зрения совокупности закрываемых уязвимостей и вариантов НСД.

Представляется, что алгоритм реализации формализованных процедур анализа предметной области позволяет строить системы поддержки принятия решений, обеспечивающие информацией для оптимального выбора средств защиты, исходя из структурно-функционального состава компьютерной сети, и с учетом ограничений на создание и функционирование системы безопасности. Список уязвимостей приведен в таблице 3.

Таблица 3

Список известных уязвимостей ЭИС ТОУ

№	*Уязвимость*	Уровень опасности
1	2	3
Backdoor		
1	Getadmin Present	Высокий
2	Fsp	Низкий
3	PortdCheck	Высокий
4	PC Anywhere Detect	Низкий
5	BackOrifice	Высокий
6	NetBus	Высокий
7	Active Modem	Средний
8	BackdoorPbbser	Высокий
…	…	…
376	guestblankpw	Средний
377	adminblankpw	Высокий
378	accountblankpw	Высокий

379	adminuserpw	Высокий
380	guestuserpw	Средний
…	…	…
663	HttpIndexserverDirtrans	Средний
664	HttpIndexserverPath	Низкий
665	TivoliLcfFileRead	Высокий
…	…	…

Для оценки степени поглощения тем или иным СЗИ соответствующих угроз были рассчитаны значения функционального веса: СЗ1-*42;* СЗ2-*18;* СЗ3-*48;* СЗ4-*6;* СЗ5-*127;* СЗ6-*18;* СЗ7-*48;* СЗ8-*48;* СЗ9-*127.* Наибольшую степень поглощения (процент поглощенных уязвимостей) имеют СЗИ СЗ5 – Амикон и СЗ9 – IS Friendsheep (рисунок 2).

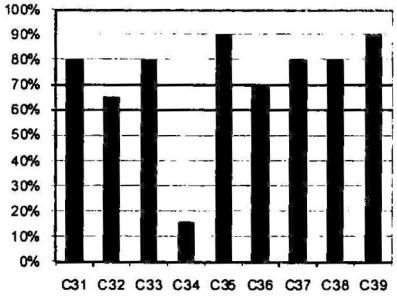

Рис. 2. Степень поглощения СЗИ угроз

Сравнительный анализ с использованием метода экспертных оценок. Каждая анализируемая система защиты представляет собой совокупность реализуемых функций и других характеристик. На практике набор характеристик представляет собой пересекающийся набор средств, которые в случае совместного использования увеличивают степень обеспечения безопасности ЭИС ТОУ.

Учитывая вышесказанное, можно сделать вывод, что при сравнительном анализе систем защиты, как совокупности выделенных характеристик, оправданно применение экспертных методов.

При ранжировании характеристик вполне обоснованным является также проведение экспертного опроса. Для этого используем следующие показатели, характеризующие:

- обобщенное мнение группы экспертов об относительной важности характеристик;

- степень согласованности мнений экспертов.

Показателем обобщенного мнения может служить среднее статистическое значение величины оценки определенной характеристики.

Далее проводится оценка согласованности мнений экспертов. Цель проведения данной процедуры будет заключаться в выявлении экспертов, чье мнение особенно сильно разошлось с остальными, а также характеристик, по которым это расхождение наблюдается. В дальнейшем предполагается уточнение позиций этих экспертов. Для оценки степени сходимости мнений экспертов используют коэффициент парной корреляции Спирмена, а также медиану (расстояние) Кемени.

На основании ранжирования характеристик экспертами определялись их весовые коэффициенты. В дальнейшем были привлечены несколько ведущих в области информационной безопасности организаций для проведения экспертной оценки конкретных систем защиты (указывалась степень реализации характеристик в структуре реальных систем защиты), на основании которой была рассчитана степень обеспечения защиты от НСД к информации в сегменте, защищенном СЗИ (таблица 4).

В главе 3 «Анализ и совершенствование структуры распределенных систем защиты ЭИС ТОУ» предложены экономическо-статистическая оценка при сравнении СЗИ, методы определения вероятности блокировки НСД при наличии центра управления распределенной системой защиты и рентабельности СЗИ.

Таблица 4

Степень защищенности

№	СЗИ	Значение
1	С31	0,261
2	С32	0,315
3	С33	0,217
4	С34	0,634
5	С35	0,092
6	С36	0,303
7	С37	0,262
8	С38	0,381
9	С39	0,412

Экономико-статистическая оценка. Данная методика позволяет достаточно эффективно сравнивать ограниченное количество распределенных систем защиты, например, при окончательном уточнении выбора[4]. Она включает в себя следующие возможные этапы:

1. Сравнительная оценка по альтернативному признаку (парные сравнения с одной выборкой).

2. Сравнительная оценка средств защиты данных с использованием методов анализа таблиц сопряженности признаков.

3. Аппроксимация биномиального критерия.

Вероятность блокировки НСД при наличии центра управления распределенной системой защиты. Учитывая специфические особенности функционирования СЗИ с центром управления, процесс НСД к информации может развиваться по следующему сценарию. Злоумышленник осуществляет НСД к информации в защищенном сегменте ЭИС ТОУ. Сообщение от СЗИ того или иного уровня о попытке НСД в реальном масштабе времени поступает в центр управления. Центр управления автоматически или по командам администратора безопасности реагирует тем или иным способом на попытку НСД. При этом возможна реализация двух альтернативных ситуаций: НСД осуществлен; попытка НСД блокирована.

[4] Данная методика была описана в диссертационной работе научного руководителя Тищенко Евгения Николаевича «Инструментальные методы анализа защищенности распределенных экономических информационных систем».

Обозначим вероятность второго события, как вероятность пресечения $P_{пр}$. Тогда задача определения вероятности $P_{пр}$ может быть сформулирована следующим образом.

Пусть имеется сегмент ЭИС ТОУ, защищенный СЗИ. Сегмент содержит определенное количество информационных объектов (процессорных узлов, массивов хранимой информации и т.д.). Необходимо найти вероятность блокирования НСД к информации одного из объектов.

Введем следующие ограничения:

- злоумышленник знает место расположения атакуемого информационного объекта и выбирает наиболее эффективный метод атаки;

- сигнал от СЗИ в реальном масштабе времени поступает в центр управления;

- система СЗИ периодически поверяется и диагностируется:

- контроль и блокировка НСД осуществляются только в пределах защищенного сегмента ЭИС ТОУ.

Блокировка НСД будет возможна только при выполнении двух независимых условий:

- факт НСД будет зафиксирован СЗИ определенного уровня;

- центр управления в автоматическом или управляемом администратором безопасности режиме будет иметь соответствующие алгоритмы блокировки и успеет осуществить данную блокировку НСД.

Таким образом, получим

$$P_{пр} = P_{обн} P_k ,$$

где $P_{обн}$ – вероятность обнаружения НСД, $P_к$ - вероятность срабатывания механизма блокировки НСД вовремя.

В свою очередь вероятность обнаружения складывается из двух составляющих:

$$P_{обн} = P_{мэ} P_{оз} ,$$

где $P_{мз}$ – вероятность обнаружения НСД конкретным СЗИ, зависящая от количества контролируемых методов НСД; $P_{оз}$ – вероятность обхода механизмов защиты СЗИ алгоритмом НСД.

Расчеты по приведенной выше методике позволили получить следующее значение вероятности блокировки попытки НСД к информации, защищенной СЗИ: $P_{пр} = 0.771$.

В заключении сформулированы выводы, основные положения и обобщения по результатам диссертационного исследования.

ПО ТЕМЕ ДИССЕРТАЦИИ ОПУБЛИКОВАНЫ РАБОТЫ

Статьи в изданиях из перечня ВАК РФ

1 Деревяшко В.В., Кравченко А.А. Анализ защищенности информационной системы предприятия//Вестник ростовского государственного экономического университета «РИНХ». – 2009. – № 1 (27). – С. 234-239. – 0,3 п.л. (авт. 0,25 п.л.)

2 Кравченко А.А. Оценка качества распределенной защищенной среды функционирования экономических информационных систем территориальных органов управления//Вестник ростовского государственного экономического университета (РИНХ) – 2009. – № 3 (29). – С. 250-254. – 0,2 п.л.

Статьи в сборниках научных трудов вуза

3 Тищенко Е.Н., Строкачева О.А., Кравченко А.А. Комплексная оценка защищенности систем электронной коммерции//Информационные системы, экономика, управление трудом и производством: уч. зап./ Рост. гос. эконом. ун-т «РИНХ». – Ростов н/Д., 2007. – Вып. 11. – С. 160-163. – 0,2 п.л. (авт. 0,1 п.л.).

4 Тищенко Е.Н., Деревяшко В.В., Кравченко А.А. Анализ подходов к аттестации автоматизированных систем обработки и хранения

данных//Информационные системы, экономика, управление трудом и производством: уч. зап. / Рост. гос. эконом. ун-т «РИНХ». – Ростов н/Д, 2008. – Вып. 12. – С. 126-131. – 0,3 п.л. (авт. 0,2 п.л.)

Материалы конференций

5 Тищенко Е.Н., Кравченко А.А. Определение требований к структуре системы информационной безопасности с единым центром управления//Статистика в современном мире: методы, модели, инструменты: материалы II межвузовской научно-практической конференции/Рост. гос. эконом. ун-т «РИНХ» – Ростов н/Д., 2008. – С. 161-165. – 0,25 п.л. (авт. 0,2 п.л.).

6 Кравченко А.А. Средства защиты информации экономических информационных систем территориальных органов управления//Статистика в современном мире: методы, модели, инструменты: материалы региональной научно-практической конференции/Ростовский государственный экономический университет «РИНХ». – Ростов н/Д., 2009. – С. 151-153. – 0,15 п.л.

7 Кравченко А.А. Основные принципы организации защищенных экономических информационных систем территориальных органов управления//Проблемы информационной безопасности: материалы четвертой всероссийской научно-практической конференции/Ростовский государственный экономический университет «РИНХ» – Ростов н/Д., 2008. – С. 39-41. – 0,1 п.л.

Свидетельство об официальной регистрации

8 Service Providing Cost/*Свидетельство о государственной регистрации программ для ЭВМ №2009615770* (авторы: К.С. Морозов, Е.Н. Тищенко, А.А. Кравченко). – М., 2009.