На правах рукописи

Костин Андрей Михайлович

МОДЕЛИ И МЕТОДЫ ОЦЕНКИ ТРУДОЗАТРАТ НА ВСКРЫТИЕ ЗАЩИТЫ ОТ КОПИРОВАНИЯ РЫНОЧНЫХ ЭКОНОМИЧЕСКИХ ИНФОРМАЦИОННЫХ СИСТЕМ

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 ГОУВПО «Ростовский государственный экономический университет (РИНХ)».

Научный руководитель:	доктор экономических наук, профессор **Хубаев Георгий Николаевич**
Официальные оппоненты:	доктор экономических наук, профессор **Тяглов Сергей Гаврилович**
	кандидат экономических наук, доцент **Широбокова Светлана Николаевна**
Ведущая организация:	Донской государственный технический университет (ДГТУ)

Защита состоится 23 декабря 2009 года в 13 часов 30 мин. на заседании диссертационного совета ДМ 212.209.03 в Ростовском государственном экономическом университете (РИНХ) по адресу: 344002, г. Ростов-на-Дону, ул. Б. Садовая, 69, ауд. 231.

С диссертацией можно ознакомиться в научной библиотеке Ростовского государственного экономического университета (РИНХ).

Автореферат разослан 20 ноября 2009 г.

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

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. Известно, что организация-разработчик не гарантирует полноценной надежности создаваемого программного продукта. Помимо надежности существует понятие защищенности программного продукта[1], способности защищать информацию и данные таким образом, чтобы неавторизованные субъекты или процессы не смогли читать или модифицировать (удалять) их, а авторизованным пользователям и процессам не было отказано в доступе к ним. В случае нарушения этого требования возможно нанесение существенного урона производителю программных продуктов (ПП) посредством несанкционированного доступа, копирования, модификации программ, их незаконного распространения и использования. Борьба с несанкционированным использованием программ включает множество средств, методов и технологий защиты программных продуктов. Однако с расширением сферы применения программных продуктов растут и модификации программных защит и, соответственно, масштабы вложения ресурсов в их развитие и эксплуатацию. Задача выбора наиболее эффективной в конкретных условиях применения системы защиты (СЗ) имеет четко выраженную экономическую значимость.

Это дает основание считать вопросы моделирования и разработки методики оценки и сравнения трудозатрат на вскрытие защиты рыночных экономических информационных систем (ЭИС) достаточно актуальными для экономики в целом.

Степень изученности исследуемой проблемы. В настоящее время большое внимание уделяется проблемам безопасности информационных систем. Эта предметная область рассматривается в работах ученых, специалистов-практиков: О. Казарина, Ю. Спаффорда, Л. Фисенко, И. Голдовского, С. Полаженко, В. Митина, Д. Стенга, С. Муна, и др.

[1] Международный стандарт ISO/IEC 9126 «Software engineering – Product quality»

Вопросам взлома различных систем защиты в целом, их отдельных компонентов, как программных, так и аппаратных, описанию способов и технологий исследования алгоритмов и устройств защиты, моделированию процессов вскрытия защиты посвящены работы Г.Н. Хубаева, С.М. Щербакова, Р.Д. Андерсона (R.J. Anderson), М.Г. Куна (M.G. Kuhn), Р.А. ДеМило (R.A. DeMillo), Р.Д. Липтона (R.J. Lipton), Д. Бонеха (D. Boneh), О. Коммерлинга (O. Kommerling), Э. Бихама (E. Biham), А. Шамира (A. Shamir), М. Ломаса (M. Lomas), П. Кочера (P. Kocher), Д. Джаффи (J. Jaffe), Б. Джуна (B. Jun), К. Касперски, П. Семьянова, и др.

Однако в опубликованных работах практически не рассматриваются проблемы моделирования и оценки трудозатрат на реализацию процессов вскрытия защиты от копирования экономических информационных систем. Этот факт обусловил выбор темы диссертационного исследования.

Объектом исследования являются экономические информационные системы различного назначения и различных производителей, включая предприятия всех форм собственности.

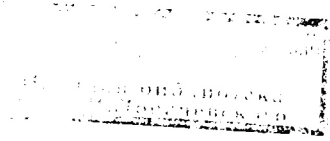
Предметом исследования являются процессы, связанные с оценкой трудозатрат на вскрытие защиты от копирования рыночных экономических информационных систем.

Цель и задачи диссертационного исследования. Основной целью диссертационного исследования является разработка визуальных и имитационных моделей для оценки трудозатрат на реализацию процессов вскрытия защиты от копирования рыночных экономических информационных систем.

Для достижения поставленной цели потребовалось решить следующие задачи:

– провести анализ предметной области и выявить основные технологии защиты программных продуктов;

– провести анализ методик и способов снятия защитных функций программных продуктов;



– провести анализ выбранного подмножества защищенных рыночных экономических информационных систем для оценки степени их защищенности;

– разработать классификацию систем защиты ЭИС по признакам, соответствующим специфике диссертационного исследования, и позволяющую выделять классы СЗ ЭИС для их сравнения и выбора;

– провести пооперационное сравнение процессов вскрытия защиты от копирования рыночных ЭИС, сформировать перечень операций процесса вскрытия защиты от копирования, получить количественные оценки взаимосвязи по операциям (пересечение, объединение, разность), сформировать группу систем, взаимосвязанных по операциям вскрытия;

– разработать UML-модели процесса вскрытия защиты экономических информационных систем;

– построить имитационные модели и выполнить имитационное моделирование процессов вскрытия защиты от копирования;

– выполнить сравнительную оценку стойкости используемых систем защиты.

Теоретическая база исследования. Теоретической и методологической базой исследования являются работы отечественных и зарубежных ученых в области теории экономических информационных систем, информационной безопасности, теории и практики вскрытия систем защиты программных продуктов, моделирования деловых процессов, материалы научных конференций, публикации в периодической печати.

Работа выполнена в рамках пунктов Паспорта специальности 08.00.13 – математические и инструментальные методы экономики: 2.2. «Конструирование имитационных моделей как основы экспериментальных машинных комплексов и разработка моделей экспериментальной экономики для анализа деятельности сложных социально-экономических систем и определения эффективных направлений развития социально-экономической и финансовой сфер»; 2.7. «Проблемы

стандартизации и сертификации информационных услуг и продуктов для экономических приложений».

Эмпирической базой исследования явились данные, характеризующие выбранное подмножество защищенных экономических информационных систем, данные о рыночной стоимости исследуемых ЭИС, данные, полученные в результате экспериментов по снятию систем защиты ЭИС, результаты экспериментальных исследований автора.

Инструментально-методический аппарат исследования. В процессе исследования использовались различные методы научного познания: системный анализ, формализованный анализ информационных характеристик ЭИС, унифицированный язык моделирования UML, методы имитационного моделирования, непараметрические методы математической статистики, общесистемное и специализированное программное обеспечение: Microsoft Windows XP Professional, Microsoft Office 2003 Standard, Конструктор имитационных моделей деловых процессов («Hoblin»).

Положения, выносимые на защиту

1. Классификация систем защиты ЭИС, позволяющая определять число защитных функций, реализованных в системах защиты ЭИС, оценивать эффективность реализации защитных функций по каждой классификационной группе и осуществлять обоснованный выбор системы защиты из конкретного класса.

2. Количественные оценки взаимосвязи по операциям процессов вскрытия защиты семи рыночных экономических информационных систем, при построении защиты от копирования которых применялись разные методы.

3. Методика оценки трудозатрат на вскрытие защиты экономических информационных систем, позволяющая охарактеризовать степень эффективности той или иной системы защиты различных ЭИС, осуществлять оптимальный выбор систем защиты и их компонентов для рыночных ЭИС.

4. Визуальные модели процессов снятия защиты от копирования экономических информационных систем. Разработанные диаграммы позволяют визуализировать рассматриваемый процесс, определить состав функций и поведение системы в различных условиях деятельности.

5. Имитационные модели процессов снятия защиты экономических информационных систем. Использование полученных имитационных моделей позволяет определить трудозатраты на выполнение всего набора и отдельных подмножеств элементарных операций.

6. Экспериментальное доказательство того, что процессы вскрытия защиты рыночных ЭИС можно разделить на отдельные элементарные операции со случайным временем реализации, а закон распределения времени вскрытия ЭИС имеет существенную положительную асимметрию.

Научная новизна. Элементы научной новизны содержат следующие основные результаты.

1. Предложена классификация систем защиты ЭИС, ***отличающаяся*** использованием в качестве классификационных признаков способа вскрытия защиты, класса и подкласса метода защиты и ***позволившая*** *определить* число защитных функций (подклассов), реализованных в системах защиты ЭИС, *оценить* эффективность реализации защитных функций по каждой классификационной группе, *осуществлять* обоснованный выбор системы защиты из конкретного класса.

2. Осуществлено (на основе сформированного перечня элементарных операций) вскрытие защиты семи рыночных экономических информационных систем, при построении защиты от копирования которых применялись разные методы. Получены количественные оценки взаимосвязи по операциям (пересечение, объединение, разность) процессов вскрытия защиты экономических информационных систем, ***позволившие*** *систематизировать* сведения о составе операций процесса вскрытия защиты рыночных ЭИС, *определить* полный перечень операций процесса вскрытия защиты семи рыночных ЭИС (113 операций), *сформировать* группы систем,

взаимосвязанных по операциям вскрытия, *расширить* для разработчиков и владельцев ЭИС возможности для выбора лучшей для конкретных условий СЗ ЭИС.

3. Разработана методика оценки трудозатрат на вскрытие защиты от копирования экономических информационных систем, ***отличающаяся*** составом и содержанием реализуемых действий и предусматривающая *формирование* перечня операций, выполняемых в процессе вскрытия защиты, *получение* данных о статистических характеристиках времени выполнения каждой операции, визуальное и имитационное *моделирование* процесса вскрытия защиты ЭИС. Методика ***позволяет*** *выявлять* наиболее и наименее стойкие системы защиты, *количественно оценивать* степень соответствия СЗ ЭИС требованиям рынка, обоснованно *формировать* состав мероприятий по обеспечению защищенности рыночных ЭИС.

4. Разработаны UML-модели процесса вскрытия защиты экономических информационных систем, ***отличающиеся*** построением диаграмм прецедентов и деятельности, ***позволившие*** *визуализировать* анализируемые процессы, *представить* их в обозримом, структурированном виде, с минимальными трудозатратами *построить* всю совокупность имитационных моделей.

5. Построены имитационные модели (путем автоматизированного синтеза на основе UML-диаграмм), ***отличающиеся*** составом переменных (более 100 переменных), и выполнено имитационное моделирование процессов вскрытия защиты семи разных по назначению рыночных экономических информационных систем. В результате моделирования получены статистические характеристики (математическое ожидание, дисперсия, среднеквадратическое отклонение, коэффициент вариации, асимметрия, эксцесс) и законы распределения (гистограммы) времени выполнения всех операций процессов вскрытия защиты экономических информационных систем, ***позволившие*** *оценивать* вероятности вскрытия

защиты за определенное время или, наоборот, *определять* время вскрытия при заданной вероятности.

6. Экспериментально *установлено*, что процессы вскрытия защиты рыночных экономических информационных систем можно представить состоящими из отдельных элементарных операций, время реализации каждой из которых является случайной величиной, а закон распределения времени вскрытия защиты ЭИС имеет существенную положительную асимметрию (порядка 0,5), при этом коэффициент вариации времени вскрытия превышает в среднем 0,4.

Теоретическая значимость исследования состоит в развитии и обосновании методов анализа рыночных ЭИС на предмет их защищенности от несанкционированного копирования, моделирования и оценки трудозатрат на реализацию процессов вскрытия защиты рыночных экономических информационных систем.

Практическая апробация и внедрение результатов исследования. Основные положения диссертационного исследования докладывались и обсуждались на научно-практических конференциях:

– Шестой всероссийской олимпиаде развития народного хозяйства России (Москва: Молодежный союз экономистов и финансистов, 2005);

– Всероссийском смотре-конкурсе научно-технического творчества студентов высших учебных заведений «ЭВРИКА-2005» (Новочеркасск: Южно-Российский государственный технический университет (НПИ), 5–6 декабря 2005).

Результаты диссертационного исследования внедрены и используются в ООО «Регион-Сервис» и в отделе Автоматизации управления ГОУВПО «РГЭУ (РИНХ)» для анализа защищенности разрабатываемых автоматизированных систем управления.

Публикации. По результатам диссертационного исследования опубликовано 5 печатных работ объемом 2,03 п.л., в том числе 2 работы в изданиях, рекомендованных ВАК РФ. Результаты экспериментальных

исследований содержатся в научном отчете РГЭУ «РИНХ» по теме «Исследование защищенности от копирования экономических информационных систем» (с грифом «ДСП»).

Логическая структура и объем работы. Диссертационная работа состоит из введения, трех глав, заключения, библиографического списка и приложений. Работа содержит 16 рисунков, 15 таблиц, 8 приложений. Библиографический список включает 84 наименования.

СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность темы диссертационного исследования, определены цель, задачи, объект, предмет, методы и инструментарий исследования. Представлены основные научные положения и результаты, выносимые на защиту.

В первой главе «Рыночные экономические информационные системы и их защита от копирования» отмечено, что основной проблемой отношений производителей и покупателей ЭИС является их несанкционированное копирование, распространение, использование и реализация пиратских копий ЭИС, слабость организационно-правовых, юридических, технических и программно-аппаратных мер для защиты от распространения пиратского программного обеспечения.

В последнее время четко прослеживается тенденция роста мирового уровня пиратства в области программного обеспечения. Как отмечается в литературе, во всем мире средняя доля «пиратского» программного обеспечения составила почти четверть копий, которые, по сути, *являются украденными у производителей, лишенных законной прибыли*. В России в 2008 году доля «пиратского» программного обеспечения составила 68%[2] (!).

Одним из эффективных методов борьбы с пиратством является

[2] Sixth annual BSA – IDC global software piracy study 2008. May 2009. http://global.bsa.org/globalpiracy2008/studies/globalpiracy2008.pdf

экономический. Этот вариант предполагает установление настолько низкой цены ЭИС, которая могла бы сравниться с ценой взломанного продукта, продаваемого пиратами. В большинстве случаев, если цена будет приблизительно одинаковой, покупатель, очевидно, предпочтёт лицензионный продукт «пиратскому». Однако большинство производителей обращаются к защите программного обеспечения от взлома и нелегального копирования. Хорошая защита доставляет множество трудностей пиратам и в итоге приводит производителей программного обеспечения к требуемой цели – получению прибыли.

Защита от несанкционированного копирования предотвращает использование ворованных копий программного обеспечения и является в настоящее время единственно надежным средством, как защищающим авторские права программистов-разработчиков, так и стимулирующим развитие рынка. Под системой защиты от копирования обычно понимают систему, которая обеспечивает выполнение программой своих функций только при опознании некоторого уникального, некопируемого элемента. Таким элементом (называемым ключевым) может быть носитель информации, определенная часть компьютера или специальное устройство, подключаемое к нему.

В дальнейшем изложении используется термин «система защиты от копирования».

При использовании системы защиты должна учитываться её комплексность, разносторонность, многофункциональность и систематизация. Любая система должна обеспечивать ряд основных функций, являющихся общими для всех систем защиты: идентификация среды, из которой будет запускаться программа; аутентификация среды, из которой программа запущена; реакция на запуск из несанкционированной среды; регистрация санкционированного копирования; противодействие

изучению алгоритмов работы системы.

В диссертации приведено подробное описание технологий, применяемых в современных системах защиты ЭИС.

Во второй главе «Способы обхода защитных функций и визуальное моделирование трудозатрат на вскрытие систем защиты экономических информационных систем» детально рассмотрены способы вскрытия систем защиты ЭИС, каждый из которых направлен на соответствующий метод защиты: уязвимость криптографических систем защиты, вскрытие ключа шифрования методом атаки полного перебора, взлом защиты, основанный на ключевом сравнении, мониторинг файлов и реестра, отладка, дизассемблирование, дампинг, использование программ «распаковщиков (депротекторов)», побитовое копирование компакт-дисков, эмулирование компакт-дисков, эмулирование электронных ключей (HASP) и др.

Для моделирования процессов вскрытия защиты от копирования рыночных ЭИС и оценки трудозатрат на вскрытие системы защиты отобрано подмножество рыночных ЭИС (таблица 1).

Таблица 1 – Анализируемые ЭИС и их средняя рыночная цена

Наименование рыночной ЭИС	Цена (руб.)
Office 2003 Standard	9734
Offline Explorer Enterprise 2.9	10850
Circuit Magic 1.02	2170
Decompiler.NET 2.0	17050
Соло на клавиатуре 8.1	450
Offline Explorer Enterprise 4.9	15469
Базис Конструктор Мебельщик 5.0	41850

В таблице 2 представлена предложенная автором классификация систем защиты рассматриваемых ЭИС.

Таблица 2 – Классификация систем защиты рассматриваемых ЭИС

Методы защиты ЭИС				Способы вскрытия СЗ
Класс	Наименование	Подкласс	Наименование	Наименование
1	2	3	4	5
А	Криптографические	А1	Шифрование данных	Вскрытие ключа шифрования методом атаки полного перебора
				Отладка
				Дизассемблирование
				Дампинг
		А2	Шифрование кода	Вскрытие ключа шифрования методом атаки полного перебора
				Отладка
				Дизассемблирование
				Дампинг
		А3	Динамическое шифрование кода	Вскрытие ключа шифрования методом атаки полного перебора
				Отладка
				Дизассемблирование
				Дампинг
		А4	Технология виртуальных машин	Отладка
				Дизассемблирование
Б	Привязка к идентификатору	Б1	Файл	Файловый мониторинг
				Отладка
				Дизассемблирование
		Б2	Элемент реестра	Мониторинг реестра
				Отладка
				Дизассемблирование
		Б3	Область жесткого диска	Файловый мониторинг
				Отладка
				Дизассемблирование
		Б4	Аппаратная конфигурация ПК	Мониторинг реестра
				Отладка
				Дизассемблирование
В	Работа с переходами и стеком	В1	Самогенерирующиеся команды (при сложении и вычитании)	Отладка
		В2	Использование команды RET вместо команды JMP	Отладка
				Дизассемблирование
		В3	Определение стека в области исполняемых команд	Отладка
				Дизассемблирование

1	2	3	4	5
Г	Манипуляции с кодом программы	Г1	Включение в тело программы «пустых» модулей	Отладка
				Дизассемблирование
		Г2	Перемешивание кода	Отладка
				Дизассемблирование
		Г3	«Упаковка» программы	Использование программ «распаковщиков (депротекторов)»
				Отладка
				Дампинг
		Г4	Использование программ «протекторов»	Использование программ «распаковщиков (депротекторов)»
				Отладка
				Дампинг
Д	Обфускация программ	Д1	Применение алгоритмов обфускации программного кода	Отладка
				Дизассемблирование
Е	Противодействие динамическим способам снятия защиты	Е1	Периодический подсчет контрольной суммы	Отладка
		Е2	Проверка количества свободной памяти	Отладка
		Е3	Проверка содержимого незадействованных программой областей памяти	Отладка
		Е4	Подавление изменения операционной среды	Отладка
		Е5	Контроль времени выполнения отдельных фрагментов программы	Отладка
		Е6	Использование многопоточности	Отладка
Ж	Использование онлайн сервера лицензирования	Ж1	Интеграция онлайн технологий идентификации	Отладка
				Дизассемблирование
З	Методы защиты на основе взаимодействия с пользователем	З1	Использование серийного номера	Отладка
				Дизассемблирование
				Файловый мониторинг
				Мониторинг реестра
		З2	Использование технологии активации	Отладка
				Дизассемблирование
				Файловый мониторинг
				Мониторинг реестра
		З3	Использование ограничения по времени	Отладка
				Дизассемблирование
				Файловый мониторинг
				Мониторинг реестра
		З4	Использование ограничения по функциональности	Отладка
				Дизассемблирование

1	2	3	4	5
И	Аппаратные	**И1**	Использование лазерных компакт-дисков	Побитовое копирование компакт-дисков
				Эмулирование компакт-дисков
				Отладка
				Дизассемблирование
		И2	Использование аппаратных ключей	Эмулирование электронных ключей
				Отладка
				Дизассемблирование
		И3	Использование биометрических характеристик человека	Отладка
				Дизассемблирование

Практически все рассмотренные системы защиты используют комбинированные методы и относятся к нескольким классам и подклассам.

Из-за чрезвычайно широкого набора средств, методов и способов защиты ЭИС выбор оптимального их состава для применения в конкретных условиях становится трудноразрешимой проблемой. Причем сведения о характеристиках существующих средств защиты и передовых технологиях обеспечения информационной безопасности не систематизированы, нет данных и о сравнительной количественной оценке функциональной полноты рыночных программно-аппаратных систем защиты информации.

В этих условиях производителям программного обеспечения практически невозможно ни количественно оценить степень соответствия той или иной системы защиты требованиям защищаемого объекта, ни осуществить оптимальный выбор конкретного набора средств защиты из множества сопоставимых.

Описана последовательность проведения экспериментальных исследований системы защиты от копирования выбранных ЭИС.

Общая процедура снятия системы защиты предполагает выполнение определенных действий в соответствии со следующим алгоритмом:

- инсталляция (установка) ЭИС;
- детальное изучение работы взламываемой ЭИС;

– определение способов защиты ЭИС, взаимодействующих с пользователем;

– выбор инструментальных средств для исследования системы защиты ЭИС;

– исследование системы защиты ЭИС;

– снятие системы защиты ЭИС;

– формирование пооперационного отчета;

– классификация исследуемой ЭИС.

На рисунке 1 приведена общая процедура вскрытия системы защиты экономических информационных систем.

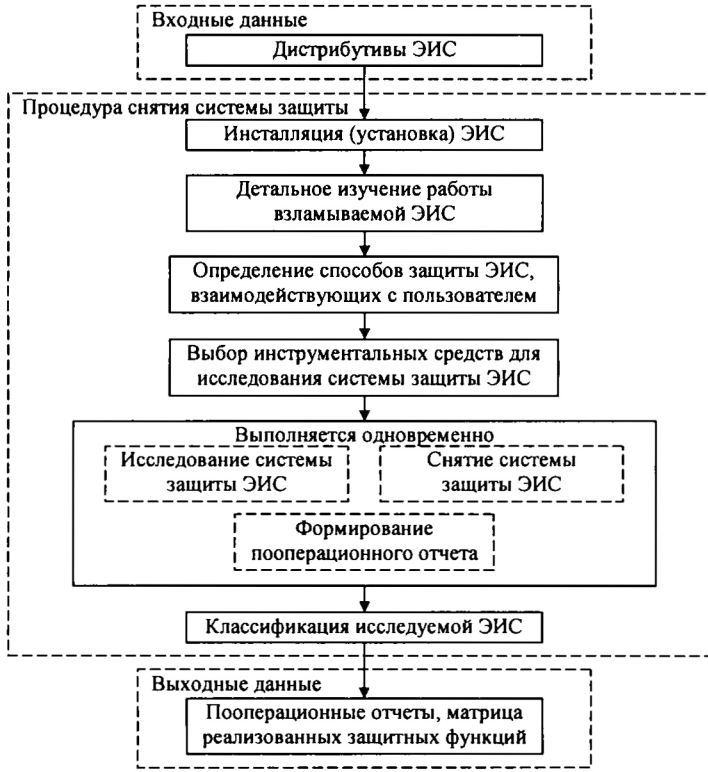


Рисунок 1 – Последовательность действий, реализуемых в процессе вскрытия защиты ЭИС

В диссертации приведены результаты экспериментов по вскрытию защиты от копирования семи рыночных ЭИС.

В таблице 3 представлен фрагмент пооперационного отчета, содержащий перечень действий, реализуемых в процессе вскрытия защиты от копирования одной из семи ЭИС – программной системы Microsoft Office 2003 Standard.

Таблица 3 – Фрагмент пооперационного отчета по результатам вскрытия защиты Microsoft Office 2003 Standard

Описание операций	**Время (мин.)**
…	
Анализ программы-установщика на предмет использования методов защиты на основе взаимодействия с пользователем	
2. Анализ всплывающих окон	
3. Анализ поведения программы-установщика	
…	
Поиск в коде программы алгоритма защиты при помощи отладчика	
20. Переход к началу программного модуля	
…	
23. Поиск по маске определенных сигнатур исполняемых команд	
…	
Исследование работы защитного алгоритма в отладчике	
…	
28. Установка «точек останова» на события чтения/записи определенных	
…	
30. Изучение вызываемых функций и процедур	
…	
32. Просмотр содержимого соответствующих регистров процессора	
…	
Проверка результатов исследования	
…	

Защитные функции Microsoft Office 2003 Standard в соответствии с классификацией систем защиты включают использование многопоточности (E6), использование серийного номера (31), шифрование данных (A1).

В таблице 4 систематизированы защитные функции, реализованные в рассматриваемых рыночных ЭИС.

Таблица 4 – Функции систем защиты от копирования рыночных ЭИС

Наименование рыночной ЭИС	Класс защиты																												
	А			Б				В			Г				Д	Е						Ж	З					И		
	Подкласс																												
	1	2	3	1	2	3	4	1	2	3	1	2	3	4	1	1	2	3	4	5	6	1	1	2	3	4	1	2	3
Microsoft Office 2003 Standard	**1**	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**1**	0	**1**	0	0	0	0	0	0
Metaproducts Offline Explorer Enterprise 2.9	**1**	0	0	0	0	0	0	0	0	0	0	0	**1**	0	0	0	0	0	0	0	0	0	1	0	**1**	**1**	0	0	0
Circuit Magic 1.02	**1**	0	**1**	0	0	0	**1**	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**1**	0	**1**	0	0	0
Decompiler.NET 2.0	**1**	**1**	0	0	0	0	0	0	0	0	**1**	0	0	0	**1**	0	0	0	0	0	0	0	0	0	0	0	1	0	0
Соло на клавиатуре 8.1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**1**	0	0	1	0	0	0
Metaproducts Offline Explorer Enterprise 4.9	**1**	0	0	0	0	0	0	0	0	0	0	0	**1**	0	0	0	0	0	0	0	0	0	**1**	0	**1**	1	0	0	0
Базис Конструктор Мебельщик 5.0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**1**	0

В диссертации представлены результаты хронометражных наблюдений за процессом вскрытия защиты от копирования семи рыночных ЭИС. В таблице 5 представлены результаты пооперационных замеров времени вскрытия защиты одной из ЭИС – системы Microsoft Office 2003 Standard.

Таблица 5 – Результаты пооперационных замеров времени вскрытия защиты ЭИС Microsoft Office 2003 Standard

№ опер.	Специалисты										Аргументы		
	I	II	III	IV	V	VI	VII	VIII	IX	X	min	moda	max
1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	1	3	3	1	3	1	2	2	2	1	**1**	**1**	**3**
2	3	4	6	2	5	6	3	3	6	4	**2**	**3**	**6**
3	5	10	7	9	8	6	11	7	8	12	**5**	**7**	**12**
4	3	5	6	3	4	2	5	3	4	6	**2**	**3**	**6**
5	40	61	30	44	38	40	48	39	60	76	**30**	**40**	**76**
6	51	80	58	63	57	58	67	58	79	95	**51**	**58**	**95**
7	22	37	16	24	20	48	24	19	34	22	**16**	**22**	**48**
8	165	226	181	194	180	224	253	176	180	200	**165**	**180**	**253**
9	153	208	160	176	182	163	160	158	228	206	**153**	**160**	**228**

1	2	3	4	5	6	7	8	9	10	11	12	13	14
10	233	312	243	261	248	233	236	217	291	228	**217**	**233**	**312**
11	194	138	148	162	149	201	141	148	192	144	**138**	**148**	**201**
12	36	49	39	45	32	29	36	31	46	60	**29**	**36**	**60**
13	91	76	59	58	53	58	63	54	75	48	**48**	**58**	**91**
14	25	35	21	16	18	22	21	17	46	32	**16**	**21**	**46**
15	456	397	410	424	411	410	483	406	454	430	**397**	**410**	**483**
16	305	351	294	319	306	372	325	301	349	305	**294**	**305**	**372**
17	93	115	87	99	92	98	130	99	114	102	**87**	**99**	**130**
18	60	89	72	110	66	73	76	67	88	73	**60**	**73**	**110**
19	82	67	49	50	44	45	54	41	49	66	**41**	**49**	**82**
20	49	72	50	55	54	87	59	54	71	42	**42**	**54**	**87**
21	176	188	233	201	187	260	187	183	231	207	**176**	**187**	**260**
22	231	272	299	240	227	213	246	222	231	270	**213**	**231**	**299**
23	37	60	43	39	31	39	47	75	59	38	**31**	**39**	**75**
24	414	397	349	365	352	347	371	349	395	336	**336**	**349**	**414**
25	312	268	258	280	267	319	268	262	310	286	**258**	**268**	**319**
26	370	354	299	322	309	311	328	311	352	304	**299**	**311**	**370**
27	23	38	17	23	21	49	25	20	35	25	**17**	**23**	**49**
28	43	60	38	30	37	36	47	75	38	59	**30**	**38**	**75**
29	97	77	101	83	82	112	83	80	96	84	**77**	**83**	**112**
30	528	477	417	445	432	439	451	427	475	439	**417**	**439**	**528**
31	298	356	305	324	305	311	330	306	354	373	**298**	**305**	**373**
32	369	409	364	377	436	369	383	359	356	407	**356**	**369**	**436**
33	388	383	334	315	375	407	394	334	351	326	**315**	**334**	**407**
34	6	5	8	6	5	9	8	6	10	7	**5**	**6**	**10**
Итого минут	**5359**	**5679**	**5004**	**5165**	**5036**	**5397**	**5365**	**4909**	**5669**	**5313**			
Итого часов	**89**	**95**	**83**	**86**	**84**	**90**	**89**	**82**	**94**	**89**			

С использованием методики сравнения сложных программных систем по критерию функциональной полноты[3] проведен пооперационный формализованный анализ семи рыночных ЭИС.

[3] Хубаев Г.Н. Сравнение сложных программных систем по критерию функциональной полноты // ПРОГРАММНЫЕ ПРОДУКТЫ И СИСТЕМЫ. – 1998. – №2. – С. 6–9.

По результатам анализа получены логические матрицы подобия, поглощения и включения. По матрицам построены соответствующие графы (рисунок 2).

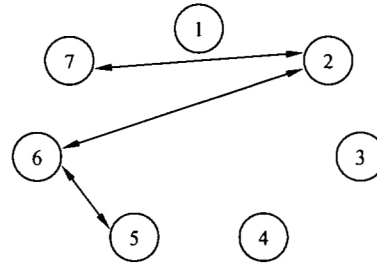


Рисунок 2 – Граф подобия по матрице Жаккарда G_o, при пороговом значении $\varepsilon_g = 0,5$

Анализ графа подобия (см. рисунок 2) позволяет выделить группу ЭИС, для вскрытия СЗ которых применяются схожие наборы элементарных операций – ЭИС 2, 5, 6 и 7.

Пооперационное сравнение процессов вскрытия защиты от копирования рыночных ЭИС позволило систематизировать сведения о составе операций процесса вскрытия, проранжировать СЗ ЭИС по числу операций по вскрытию, сформировать группу взаимосвязанных систем, тем самым расширить для разработчиков и владельцев ЭИС возможности для выбора лучшей для конкретных условий СЗ ЭИС.

Для визуализации анализируемых процессов и представления их в обозримом, структурированном виде и для формирования с минимальными трудозатратами совокупности имитационных моделей построены UML-модели процесса вскрытия защиты экономических информационных систем.

Диаграммы прецедентов и деятельности процесса вскрытия системы

защиты построены для каждой рассматриваемой ЭИС. Ниже приведены фрагменты диаграмм для процесса вскрытия СЗ ЭИС Microsoft Office 2003 Standard (рисунки 3, 4).

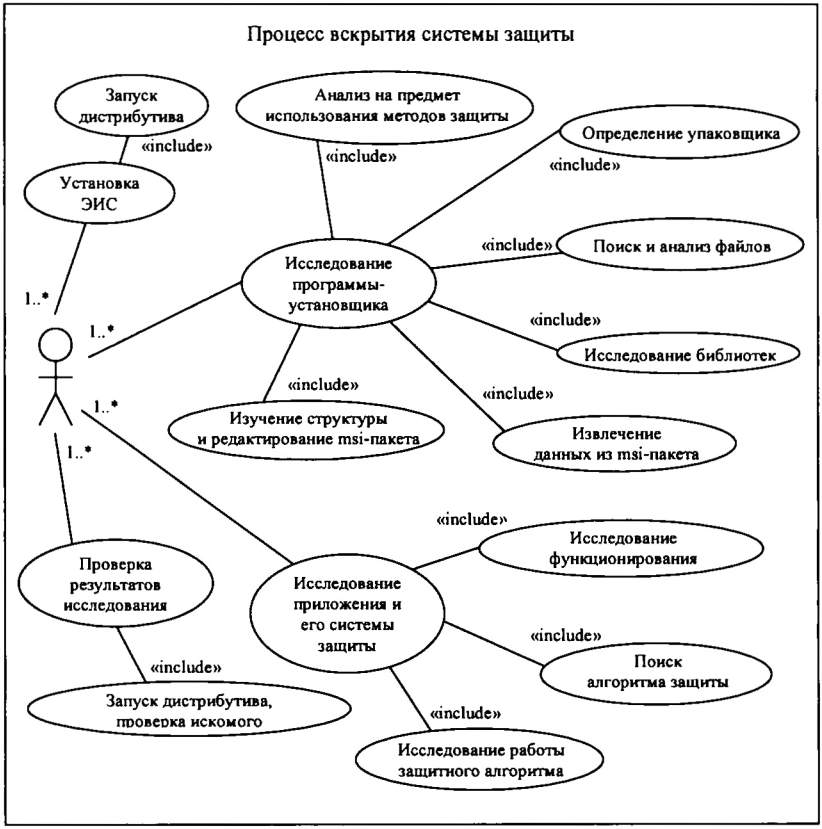


Рисунок 3 – Фрагмент диаграммы прецедентов, иллюстрирующий процесс вскрытия системы защиты ЭИС Microsoft Office 2003 Standard

Рисунок 4 – Фрагмент диаграммы деятельности для процесса вскрытия системы защиты ЭИС Microsoft Office 2003 Standard

В третьей главе «Имитационное моделирование и методы непараметрической статистики для оценки трудозатрат на вскрытие защиты от копирования ЭИС» представлены имитационные модели, построенные путем автоматического синтеза по UML-моделям, и результаты расчетов характеристик качества СЗ ЭИС.

Использование унифицированного языка моделирования UML при построении имитационной модели обеспечило единство процесса исследования системы на качественном и количественном уровне, снизило затраты труда на разработку моделей, позволило в унифицированном виде представить результаты имитационного моделирования.

Методика базируется на идеях, изложенных в работах[4], и предполагает реализацию следующих этапов:

– процессы вскрытия защиты информационных систем представляются в виде наборов элементарных операций и UML-диаграмм деятельности;

– для каждой операции процесса определяется время, необходимое на ее выполнение;

– определяются частотные характеристики процесса;

– автоматически синтезируется имитационная модель;

– проводится имитационное моделирование.

Использование методики и системы имитационного моделирования[5] позволяет определить трудозатраты на выполнение всего набора и отдельных подмножеств элементарных операций, провести сравнение СЗ по величине затрат труда на вскрытие защиты ЭИС.

---

[4] Хубаев Г.Н Безопасность распределенных информационных систем: обеспечение и оценка // Известия вузов. Северо-Кавказский регион. Технические науки. Спецвыпуск «МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ И КОМПЬЮТЕРНЫЕ ТЕХНОЛОГИИ». – 2002. – С.11–13. Хубаев Г.Н. Процессно-статистический подход к учету затрат ресурсов при оценке (калькуляции) себестоимости продукции и услуг: особенности реализации, преимущества // ВОПРОСЫ ЭКОНОМИЧЕСКИХ НАУК. – 2008. – №2. – С.158–166.

[5] Хубаев Г.Н., Щербаков С.М., Шибаев А.А. Конструктор имитационных моделей деловых процессов : Свидетельство об официальной регистрации программы для ЭВМ. – №2005612262. – М.: РОСПАТЕНТ, 2005.

Проведено моделирование процессов снятия защиты для каждой ЭИС.

Результатами моделирования являются статистические характеристики (математическое ожидание, дисперсия, среднеквадратическое отклонение, коэффициент вариации, асимметрия, эксцесс) и законы распределения (гистограммы) выходного параметра для всех рассматриваемых СЗ ЭИС. На гистограммах (рисунки 5–7) ось абсцисс – время выполнения соответствующих элементарных операций, а ось ординат – число реализаций при имитационном моделировании.

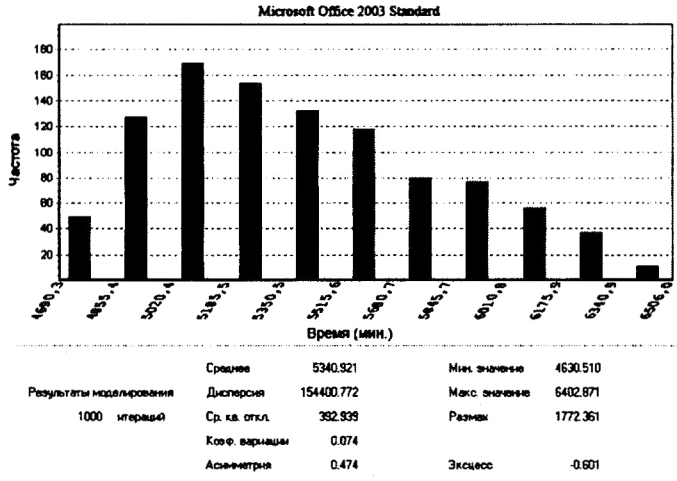


Рисунок 5 – Результаты моделирования процесса вскрытия системы защиты ЭИС Microsoft Office 2003 Standard

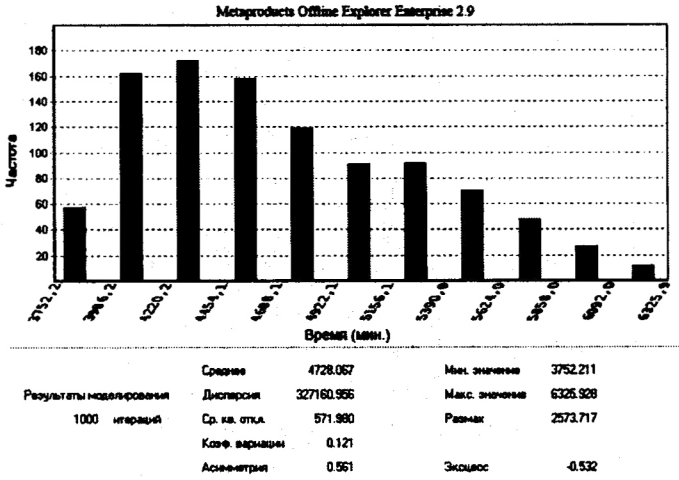


Рисунок 6 – Результаты моделирования процесса вскрытия системы защиты ЭИС Metaproducts Offline Explorer Enterprise 2.9

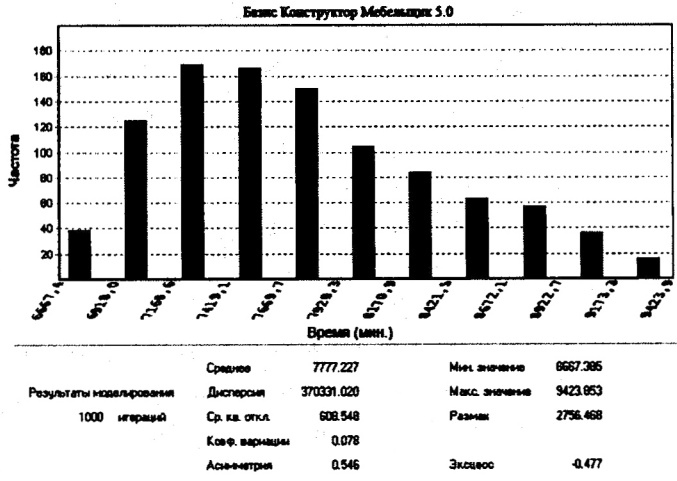


Рисунок 7 – Результаты моделирования процесса вскрытия системы защиты от копирования рыночной ЭИС «Базис Конструктор Мебельщик 5.0»

Результаты имитационного моделирования представлены в таблице 6.

Таблица 6 – Результаты имитационного моделирования по рассматриваемым ЭИС

Наименование ЭИС	Статистические характеристики										Цена (руб.)
	мин.	сред.	мода	макс.	размах	дисперсия	ср. кв. откл.	коэф. вар.	асимметрия	эксцесс	
Microsoft Office 2003 Standard	4631	5341	5103	6403	1772	154401	393	0,07	0,47	-0,60	9734
Metaproducts Offline Explorer Enterprise 2.9	3757	4713	4304	6162	2405	304730	552	0,12	0,44	-0,78	10850
Circuit Magic 1.02	1485	1945	1744	2625	1139	65394	256	0,13	0,48	-0,51	2170
Jungle Creature Decompiler.NET 2.0	2649	3097	2899	3749	1100	62753	251	0,08	0,47	-0,59	17050
Соло на клавиатуре 8.1	767	1059	922	1449	683	24400	156	0,15	0,46	-0,67	450
Metaproducts Offline Explorer Enterprise 4.9	5467	6384	5985	7744	2276	259332	509	0,08	0,46	-0,64	15469
Базис Конструктор Мебельщик 5.0	6667	7777	7294	9424	2756	370331	609	0,08	0,55	-0,48	41850

Ранее[6] высказано и *содержательно* обосновано предположение о том, что закон распределения времени вскрытия защиты информационной системы имеет правостороннюю (положительную) асимметрию.

Однако для любого средства защиты важно оценить среднее значение времени, необходимого на его взлом. Но поскольку закон распределения времени вскрытия не является нормальным (предполагается положительная асимметрия), то для оценки значимости математического ожидания времени взлома можно использовать непараметрические критерии, в частности критерий рандомизации.

С использованием критерия рандомизации выполнена оценка значимости математического ожидания времени вскрытия защиты для каждой из выбранных ЭИС.

В случае, когда значения среднего времени вскрытия защиты рассматриваемых ЭИС близки друг к другу, целесообразно провести сравнительную оценку времени вскрытия СЗ также с использованием критерия рандомизации. Результаты сравнения ЭИС Microsoft Office 2003 Standard и Metaproducts Offline Explorer Enterprise 2.9 с использованием критерия рандомизации представлены в диссертации.

Заключение диссертации содержит результаты проведенного исследования, основные выводы и предложения.

[6] Хубаев Г.Н. Оценка времени вскрытия защиты информационных систем: статистический подход // Проблемы экономики. – 2008. – №6. – С. 135–138

Основные положения диссертации нашли свое отражение в следующих публикациях.

Статьи в периодических научных изданиях, выпускаемых в РФ и рекомендованных ВАК РФ.

1. Костин А.М. Визуальное и имитационное моделирование при оценке трудозатрат на вскрытие защиты экономических информационных систем // Экономические науки : научно-информационный журнал. 2009. – №3(52). – С.325–330. – 0,3 п.л.

2. Костин А.М. Алгоритм оценки трудозатрат на вскрытие экономических информационных систем // Вестник Ростовского государственного экономического университета «РИНХ» : научно-практический журнал. 2009. – №2(28). – С.300–307. – 0,4 п.л.

Статьи в периодических научных изданиях, в материалах конференций и в сборниках научных трудов вузов

3. Костин А.М. Реализация системы защиты для информационной системы автоматизации учетно-рассчетных задач в коммунальном хозяйстве // Информационные системы, экономика, управление трудом и производством : ученые записки / Под ред. Наливайского В.Ю. – Ростов н/Д : РГЭУ «РИНХ», 2006. – Вып. 10. – С.38–40. – 0,25 п.л.

4. Костин А.М. Зубач Л.В. Обеспечение защищенности прикладных информационных систем // Проблемы федеральной и региональной экономики : ученые записки / Под ред. Бугаяна И.Р. – Ростов н/Д : РГЭУ «РИНХ», 2007. – Вып. 10. – С.135–144. – В соавторстве, авторских – 0,5 п.л.

5. Костин А.М. Обеспечение защищенности информационной системы автоматизации ведения налогового учета на предприятии // Проблемы федеральной и региональной экономики : ученые записки / Под ред. Наливайского В.Ю. – Ростов н/Д : РГЭУ «РИНХ», 2006. – Вып. 9. – С.70–76. – 0,58 п.л.

6. Исследование защищенности от копирования экономических информационных систем : отчет о НИР / РГЭУ «РИНХ»; рук. Хубаев Г.Н.; исполн.: Костин А.М. [и др.]. – Ростов н/Д, 2009. – 155с. – (с грифом «ДСП»).

Печать цифровая. Бумага офсетная. Гарнитура «Таймс».
Формат 60x84/16. Объем 1,2 уч.-изд.-л.
Заказ № 1511. Тираж 130 экз.
Отпечатано в КМЦ «КОПИЦЕНТР»
344006, г. Ростов-на-Дону, ул. Суворова, 19, тел. 247-34-88