

На правах рукописи

Савельева Александра Александровна

**МОДЕЛИ И МЕТОДЫ КОМПЛЕКСНОЙ ОЦЕНКИ АППАРАТНО-
ПРОГРАММНЫХ СРЕДСТВ ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ
И ЦЕЛОСТНОСТИ ИНФОРМАЦИИ**

Специальность 05.13.19 – «Методы и системы защиты информации,
информационная безопасность» (технические науки)

АВТОРЕФЕРАТ

диссертации на соискание ученой степени
кандидата технических наук

Москва – 2011

Работа выполнена в Национальном исследовательском университете
«Высшая школа экономики»

Научный руководитель: кандидат технических наук, доцент
Авдошин Сергей Михайлович

Официальные оппоненты: доктор технических наук, профессор
Щеглов Андрей Юрьевич

кандидат технических наук, доцент
Скородумов Борис Иванович

Ведущая организация: Московский энергетический институт (технический
университет)

Защита диссертации состоится «28» июня 2011 г. в 10 часов 00 минут на за-
седании диссертационного совета Д. 212.133.03 Московского государствен-
ного института электроники и математики (технического университета) по
адресу: 109028 Москва, Б.Трехсвятительский пер., д. 3.

С диссертацией можно ознакомиться в библиотеке Московского государ-
ственного института электроники и математики (технического университета)

Автореферат разослан «__» мая 2011 г.

Ученый секретарь
диссертационного совета Д. 212.133.03,
доктор технических наук, доцент



Леохин Ю.Л.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. На протяжении последних десятилетий непрерывно растет потребность организаций в надежных средствах защиты информации (СЗИ). В связи с этим внимание специалистов по обеспечению информационной безопасности (ИБ) привлекает проблема оценки влияния стоимости и качества СЗИ на бизнес. В России, как отмечается в работах Б.И. Скородумова, проблемы ИБ традиционно рассматривались преимущественно для защиты государственной тайны в военных или правительственных автоматизированных системах. В результате практика оценки средств обеспечения ИБ с экономических позиций пока не получила широкого распространения, несмотря на наличие глубоких теоретических исследований в этой области (в т.ч. работы А.И. Костогрызова, А.А. Кононова, А.А. Чемина и др.). Сегодня это существенно мешает развитию коммерческого сектора российской экономики. Задачи разработки методов и средств проведения экспертизы и контроля качества защиты информации включены в перечень приоритетных проблем научных исследований в области информационной безопасности Российской Федерации, который был утвержден Советом Безопасности Российской Федерации 7 марта 2008 г. Не только в нашей стране, но и за рубежом наблюдается сравнительно небольшой объем публикаций, посвященных методам и моделям комплексной оценки средств обеспечения конфиденциальности и целостности информации. Исследователи, как правило, фокусируются на математических аспектах оценки устойчивости к взлому, оставляя без внимания другие актуальные задачи (такие, как человеческий фактор и удобство использования систем защиты). Исключением являются работы Б.Йи (2001), В.П. Иванова (2004), У.Маурера (2005), К.Лампрехта (2006). Тем не менее, предлагаемые в указанных публикациях методы имеют ряд существенных недостатков, в числе которых:

- применимость только к системам, основанным на сохранении в секрете механизма защиты информации;
- отсутствие возможности учитывать контекст использования системы защиты (критичность защищаемой информации, оснащенность злоумышленника и др.);
- представление результатов оценки в форме, неудобной финансистам для принятия решений о необходимости инвестиций в СЗИ.

На сегодняшний день отсутствуют подходы к решению задачи комплексной оценки средств обеспечения конфиденциальности и целостности информации, позволяющие перейти от технических показателей способности системы противостоять угрозам со стороны злоумышленников к экономическим показателям окупаемости, понятным руководителям и финансистам. Современная тенденция использования принципов управления рисками при решении проблем, связанных с обеспечением ИБ (см. международный стандарт в области управления рисками информационной безопасности ISO/IEC 27005:2008 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности»), не коснулась практик оцен-

ки соответствия аппаратно-программных средств обеспечения конфиденциальности и целостности информации потребностям организации. Это создает трудности при оценке соответствия системы менеджмента информационной безопасности (СМИБ) организации, использующей такие средства, требованиям международного стандарта ISO/IEC 27001:2005 (ИСО-МЭК 27001-2006) «Информационные технологии - Методы обеспечения безопасности - Системы управления информационной безопасностью - Требования».

Таким образом, актуальным является исследование и разработка моделей и методов комплексной оценки аппаратно-программных средств обеспечения конфиденциальности и целостности информации, применимых в рамках внутреннего или внешнего аудита, а также анализа рисков реализации угроз нарушения ИБ активов организации.

Цель и задачи работы.

Объектом исследования являются методы и модели оценки средств защиты информации.

Предметом исследования является изучение применимости моделей и методов оценки средств защиты информации для получения комплексной оценки аппаратно-программных средств обеспечения конфиденциальности и целостности информации с технической и экономической точек зрения.

Цель исследования заключается в разработке и исследовании моделей и методов комплексной оценки аппаратно-программных средств обеспечения конфиденциальности и целостности информации.

Для достижения поставленной цели были решены следующие **задачи**:

- исследование существующих моделей и методов оценки аппаратно-программных средств обеспечения конфиденциальности и целостности информации;
- разработка модели аппаратно-программных средств обеспечения конфиденциальности и целостности информации, ориентированной на получение комплексной оценки с технической и экономической точек зрения;
- разработка модели угроз нарушения безопасности информационных активов организации, защищенных с использованием аппаратно-программных средств обеспечения конфиденциальности и целостности;
- разработка метода анализа рисков реализации угроз нарушения безопасности, использующего предложенные модели;
- разработка набора инструментальных средств, позволяющих оценить способность аппаратно-программных средств обеспечения конфиденциальности и целостности информации противостоять идентифицированным угрозам.
- разработка и исследование с использованием инструментальных средств новых теоретико-числовых алгоритмов, применимых для анализа стойкости к взлому методов защиты на основе трудноразрешимости задачи дискретного логарифмирования в простых полях;
- разработка метода построения оценки из предложенных компонент.

Методы исследования. При решении поставленных задач исследования использован математический аппарат теории матриц, теории множеств, теории чисел, линейной алгебры и теории алгоритмов. При разработке программного обеспечения использовались методы объектно-ориентированного программирования, компонентного программирования и восходящего проектирования.

Основные положения, выносимые на защиту:

- новые многокритериальные классификации и параметрические модели злоумышленников, атак и средств обеспечения конфиденциальности и целостности, отличающиеся от существующих тем, что позволяют учитывать взаимосвязь между параметрами объектов при моделировании угроз нарушения конфиденциальности и целостности информации;
- модель угроз безопасности информационных ресурсов коммерческой организации, позволяющая выделить множество наиболее опасных атак и отличающаяся от существующих тем, что является формализованной, расширяемой и ориентированной на использование математического аппарата теории управления рисками;
- метод анализа рисков реализации угроз нарушения безопасности, использующий предложенные модели и отличающийся от существующих тем, что позволяет учитывать критичность защищаемых данных и возможности злоумышленника;
- новый детерминированный метод решения систем линейных уравнений в кольцах вычетов, позволяющий ускорить работу алгоритмов дискретного логарифмирования типа *index-calculus* и отличающийся от известных аналогов отсутствием требования факторизации;
- метод комплексной оценки аппаратно-программных средств обеспечения конфиденциальности и целостности информации на основе предложенной модели угроз и классификаций, отличающийся от известных аналогов тем, что позволяет перейти от технических показателей защищенности системы к экономическим показателям окупаемости.

Научная новизна:

1. Разработаны новые многокритериальные классификации злоумышленников, атак и средств обеспечения конфиденциальности и целостности информации, отличающиеся от существующих тем, что позволяют учитывать взаимосвязь между параметрами объектов при моделировании угроз нарушения конфиденциальности и целостности информации.
2. Создана модель угроз безопасности информационных ресурсов коммерческой организации, позволяющая выделить множество наиболее опасных атак и отличающаяся от существующих тем, что является формализованной, расширяемой и основывается на использовании математического аппарата теории управления рисками и разработанных классификациях.
3. Разработан новый детерминированный метод, позволяющий повысить временную эффективность алгоритмов дискретного логарифмирования типа *index-calculus*, основанный на алгоритме исключения Гаусса-

Жордана в кольцах вычетов и расширенном алгоритме Евклида, отличающийся от известных аналогов отсутствием требования факторизации.

4. Предложен метод комплексной оценки аппаратно-программных средств обеспечения конфиденциальности и целостности информации, базирующийся на предложенной модели угроз и классификациях, отличающийся от известных аналогов тем, что позволяет перейти от технических показателей способности системы противостоять угрозам со стороны злоумышленников к экономическим показателям окупаемости.

Практическая значимость. Полученные результаты могут быть использованы при проведении комплексной оценки аппаратно-программных средств обеспечения конфиденциальности и целостности информации в рамках внутреннего или внешнего аудита безопасности корпоративной информационной системы, а также анализа рисков нарушения ИБ объекта, защищенного с использованием криптографических средств.

Новое техническое решение в виде программного комплекса для решения задач дискретного логарифмирования, факторизации и проверки чисел на простоту защищено авторскими свидетельствами [20–24] и отличается от известных тем, что содержит необходимые примитивы для создания факторной базы, решета и разложения на множители; включает математическую библиотеку и графическое приложение, обеспечивающее пользователю удобный доступ к функциям библиотеки; обладает компонентной расширяемой архитектурой, упрощающей добавление новых функций в библиотеку.

Достоверность полученных результатов подтверждается внутренней непротиворечивостью логики исследования, корректным выбором и адекватным использованием математического аппарата, результатами внедрения и публикацией основных результатов диссертации в ведущих рецензируемых журналах.

Внедрение. Результаты диссертационной работы использованы в проектно-конструкторской деятельности ЗАО «ДиалогНаука» в виде:

5. Модели угроз нарушения конфиденциальности и целостности информации, позволяющей выявлять угрозы безопасности информации и ранжировать их по степени опасности;
6. Модели нарушителя, позволяющей определять возможности реализации выявленных внутренних угроз в информационной системе;
7. Метода анализа рисков, связанных с возможностью реализации нарушителем угроз безопасности в отношении конфиденциальности и целостности защищаемых информационных ресурсов.
8. Программного комплекса для оценки устойчивости к взлому аппаратно-программных средств обеспечения конфиденциальности и целостности информации.

Основные положения и результаты диссертационной работы вошли в отчёты по научно-исследовательской работе по теме «Исследование и разработка методов оценки эффективности использования криптографических средств защиты информации в сфере бизнеса и финансов», получившей гос-

ударственный грант по конкурсу № НК-623П «Проведение поисковых научно-исследовательских работ по направлению «Обработка, хранение, передача и защита информации» на 2009 – 2013 годы.

Научные результаты использованы в учебном процессе кафедры «Управление разработкой программного обеспечения» отделения программной инженерии Национального исследовательского университета «Высшая школа экономики» при разработке методических пособий по чтению лекций и проведению практических занятий в рамках курсов «Организация и технологии защиты информации» и «Технологии обеспечения информационной безопасности», а также отражены в методических материалах по курсу «Технологии и продукты Microsoft в обеспечении информационной безопасности», созданного при финансовой поддержке Microsoft.

Апробация работы. Полученные теоретические результаты прошли апробацию на: конференции «РусКрипто2006», научно-исследовательском семинаре МГТУ им. Н.Э.Баумана «Защита информации: аспекты теории и вопросы практических приложений», научно-технической конференции «Информационные технологии в бизнесе» в 2006 г., Межвузовской конференции «Актуальные проблемы современных компьютеров» в 2006 г., Юбилейной студенческой научной конференции, посвященной 70-летию МГУПИ, Международной студенческой школе-семинаре «Новые информационные технологии» в 2006 и 2008 гг., VIII Международной конференции «Модернизация экономики и общественное развитие», Весеннем коллоквиуме молодых исследователей SYRCoSE'2008 и SYRCoSE'2009, международной конференции SEC(R) 2008, XXXI, XXXII, XXXIV и XXXV Международных молодежных научных конференциях «Гагаринские чтения», VI Всероссийской конференции «Технологии Microsoft в теории и практике программирования» в 2009 г., 11-м Национальном форуме информационной безопасности и XVI Всероссийской научно-практической конференции «Проблемы информационной безопасности в системе высшей школы» в рамках «Научной сессии МИФИ-2009», семинаре «2009 Workshop on Cyber Security and Global Affairs», Oxford, XXXIII/XXXV/XXXVII Международных конференциях IT + S&E`06/08/10 «ИТ в науке, образовании, телекоммуникации и бизнесе», научном семинаре кафедры ИКТ МИЭМ под рук. д.т.н., проф. В.Н.Азарова в 2010 г., научном семинаре «Проблемы современных информационно-вычислительных систем» под рук. д. ф.-м. н., проф. В. А. Васенина в Институте проблем информационной безопасности МГУ имени М.В.Ломоносова в 2011 г.

Публикации. По теме диссертации опубликовано 33 печатных работы на русском и английском языке, из них 3 — в журналах из Перечня изданий, рекомендованных ВАК России [1-3].

Объём и структура работы. Работа состоит из введения, четырёх глав, заключения и четырех приложений. Основное содержание работы изложено на 111 страницах (с приложениями – 123 страницы), включая 18 рисунков, 4 таблицы и список литературы из 129 наименований.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении дана общая характеристика работы: обоснована ее актуальность, дан общий обзор предметной области, сформулированы цель и задачи исследования, обозначены объекты исследования работы, определена научная новизна и практическая значимость исследования.

В первой главе проведен анализ рациональных предпосылок использования средств криптографической защиты информации в коммерческих организациях и определены основные области применения криптотехнологий (раздел 1.1). Показано, что потребность в использовании криптосистем влечет за собой необходимость применения для оценки качества криптографических средств комплексных методов оценки (раздел 1.2). В табл. 1 представлены результаты проведенного анализа современных моделей и методов оценки качества СЗИ на базе предложенных в работе критериев их применимости для оценки криптосистемы (раздел 1.3). Показано, что ни один из рассмотренных методов полностью не соответствует заданным критериям.

Таблица 1

Сравнительный анализ методов оценки качества средств защиты информации

<i>Используемый мат. аппарат / инструменты</i>	<i>Применимость к современным криптосистемам</i>	<i>Экономические показатели</i>	<i>Возможности злоумышленника</i>	<i>Наличие автоматизированных средств</i>
Анализ криптостойкости (Ростовцев А.Г. и др., 1998)	+	-	±	±
Теория массового обслуживания и теория катастроф (Иванов В.П., 2004)	±	+	±	-
Теория игр (Yee B. S., 2001)	+	±	±	-
Анализ информационных рисков (АванГард - ИСА РАН, 2002; ГРИФ – Digital Security, 2006)	-	+	+	±
Анализ криптопротоколов (Bodey et. al., 2003; Boreale M. et.al., 2002; Cheminod M. et.al., 2008)	±	-	-	+
Экспериментальная оценка скорости online-транзакций (Lamprecht C. et.al., 2006)	+	±	-	+

На основе выявленных недостатков существующих методов оценки качества СЗИ сделан вывод, что при построении новых моделей и методов комплексной оценки аппаратно-программных средств обеспечения конфиденциальности и целостности информации необходимо учитывать взаимосвязь между особенностями криптосистемы, потенциальных злоумышленников и возможными сценариями атак на защищаемые информационные активы (раздел 1.4).

Для разработки, внедрения, обеспечения функционирования, мониторинга, анализа, поддержки и улучшения СМИБ организации стандарты семейства ИСО МЭК 27000 предполагают использование процессного подхода.

С учетом перечисленных оснований в разделе 1.5 сформулирована цель исследования и определены задачи, которые необходимо решить для ее достижения, а именно: разработать метод комплексной оценки аппаратно-программных средств обеспечения конфиденциальности и целостности информации в соответствии с предложенной процессной моделью, представленной на рис. 1.

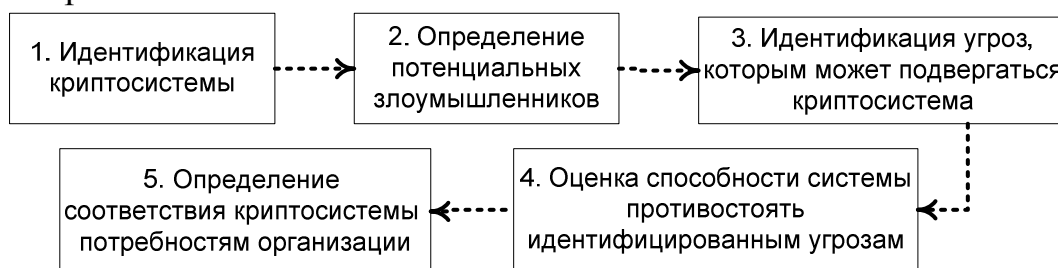


Рис. 1 - Модель процесса комплексной оценки аппаратно-программных средств обеспечения конфиденциальности и целостности информации

Во второй главе предложено осуществлять комплексную оценку аппаратно-программных средств обеспечения конфиденциальности и целостности информации в 3 этапа, и показано, какие методы и инструменты потребуются на каждом из них (Табл.2 и раздел 2.1 диссертации).

Таблица 2

Метод комплексной оценки аппаратно-программных средств обеспечения конфиденциальности и целостности информации

Этап	Необходимые методы/инструменты
Построение модели угроз	Модель угроз и классификации криптосистем, злоумышленников и атак для формализации контекста использования СКЗИ в коммерческой организации
Оценка устойчивости криптосистемы к взлому	Метод анализа рисков, использующий разработанную модель угроз Средства оценки криптостойкости
Оценка эффективности криптосистемы в денежном выражении	Набор финансовых показателей для оценки эффективности криптосистем с экономических позиций

Для моделирования угроз безопасности криптосистемы рассматривать взаимосвязь трех элементов: атаки, злоумышленника и криптосистемы, параметрические модели которых задаются в виде векторов $\vec{a} \in A$, $\vec{b} \in B$ и $\vec{c} \in C$. Для описания параметров моделей предложены новые классификации, которые отличаются от существующих классификаций Ф.Баурера (2000), Ж.Брассара (1988), Б.Шнайера (2003), М.В.Степашкина (2006), О.Кирхгоффа (1883), К.Ладвера (1994), У.Лингвиста (1997), Н.Полоскиса (2006) и Д.Вебера (1998) тем, что являются многокритериальными и позволяют учитывать взаимосвязь между параметрами объектов при моделировании угроз нарушения конфиденциальности и целостности информации. (в используемой нотации $A \subseteq A_1 \times A_2 \times \dots \times A_9$, $B \subseteq B_1 \times B_2 \times \dots \times B_6$, $C \subseteq C_1 \times C_2 \times \dots \times C_6$ и A_i ($i=1, 9$), B_j ($j=1, 6$), C_k ($k=1, 6$) — множество значений $i/j/k$ -го параметра модели, определяю-

шего тип атаки / злоумышленника / криптосистемы в соответствии с критериями разработанных классификаций (см. рис. 2-4), подробное описание которых дано в разделах 2.2 – 2.4 текста диссертации.

В разделе 2.5 описана разработанная модель угроз, позволяющая выделить множество наиболее опасных атак и отличающаяся от существующих тем, что является формализованной, расширяемой и основывается на разработанных классификациях. Пусть $I: C \times A \rightarrow [0; 1]$ — функция ущерба от применения атаки $\vec{a} \in A$ к криптосистеме $\vec{c} \in C$. Семейство функций $I_{gh}: C_g \times A_h \rightarrow \mathbb{R}_+$, $g = \overline{1,6}$, $h = \overline{1,9}$, где \mathbb{R}_+ - множество неотрицательных действительных чисел, задает уровень взаимного влияния параметра криптосистемы $c \in C_g$ и параметра атаки $a \in A_h$: $I_{gh}(c, a) = 0$, если атака не применима к криптосистеме со значением параметра; $0 < I_{gh}(c, a) < 1$, если значение параметра криптосистемы снижает вероятность успешного применения атаки с указанным значением параметра; $I_{gh}(c, a) = 1$, если указанные параметры не влияют на применимость атаки к взлому криптосистемы; $I_{gh}(c, a) > 1$, если значение параметра криптосистемы указывает на то, что атака применима для ее взлома. $P: B \times A \rightarrow [0; 1]$ - вероятность того, что злоумышленник $\vec{b} \in B$ предпримет атаку $\vec{a} \in A$, т.е. обладает ресурсами для ее осуществления и сочтет эту атаку целесообразной, а функция P_{th} задает уровень взаимного влияния параметра злоумышленника b_i и параметра атаки a_h и определяется аналогично функции I_{gh} на основе экспертных оценок.

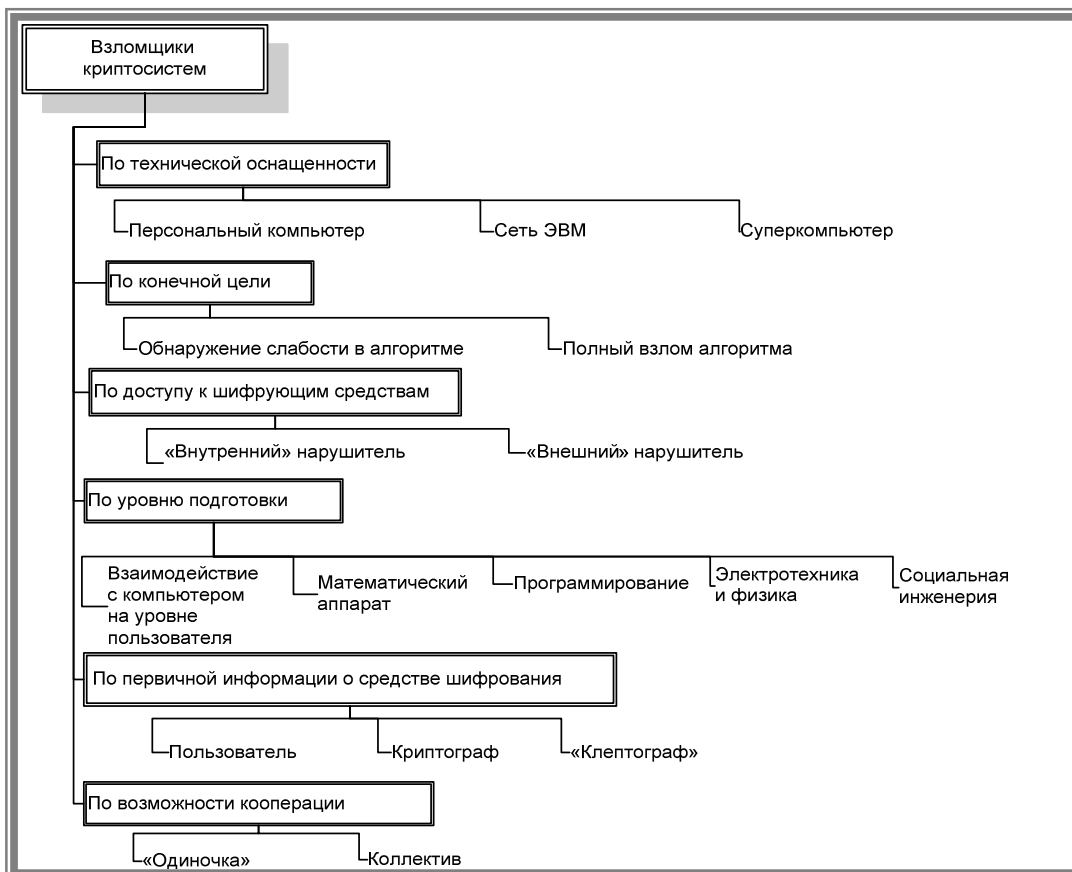


Рис. 2. Классификация злоумышленников

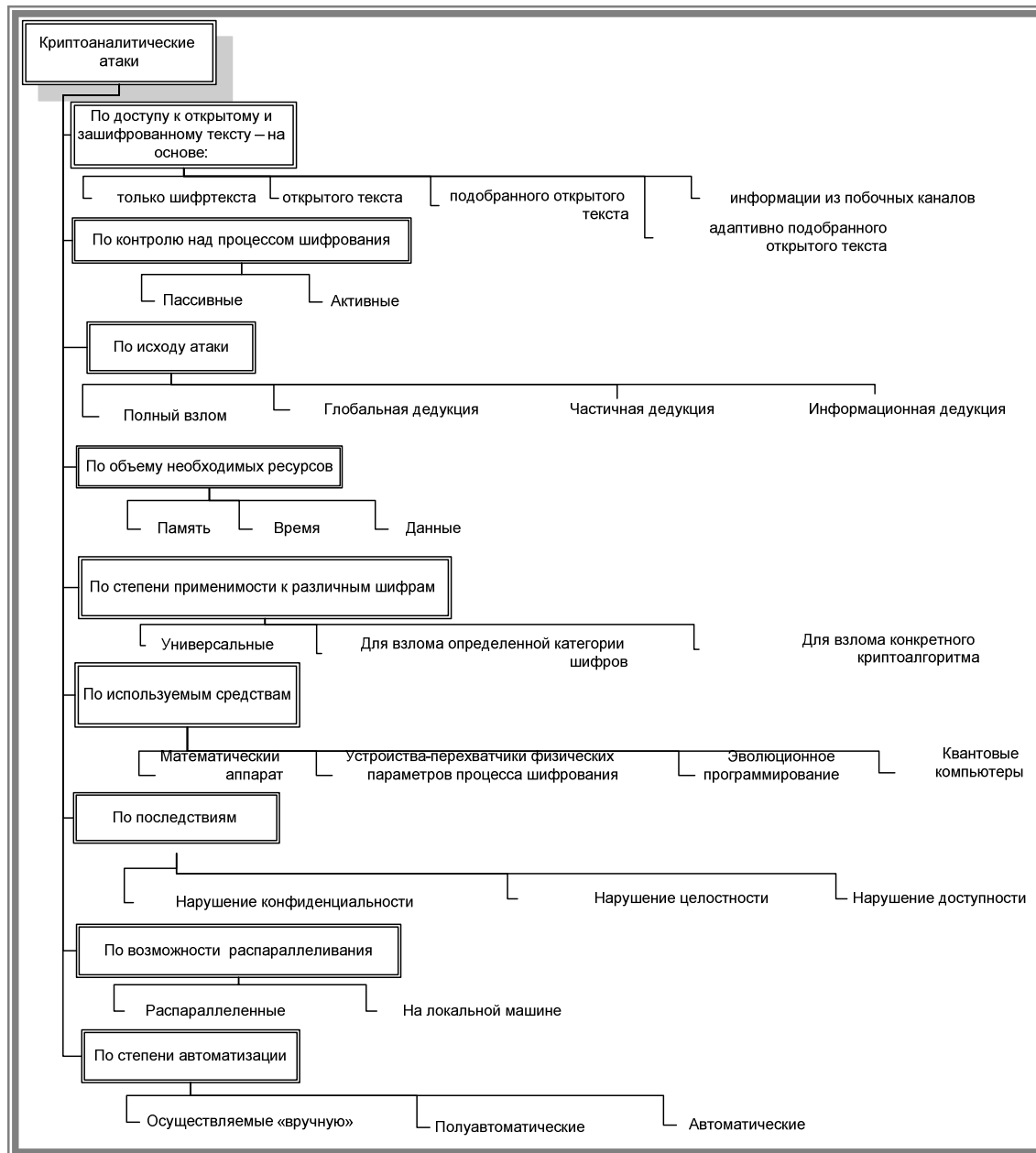


Рис. 3. Классификация атак

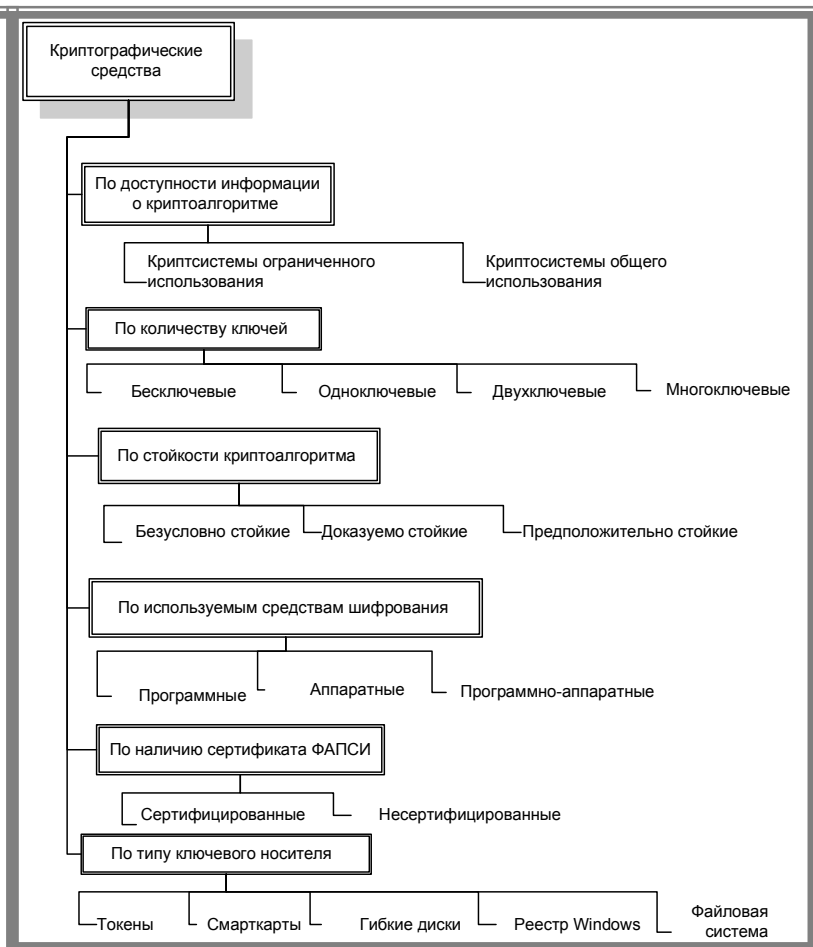


Рис. 4. Классификация криптографических средств

Для выделения основных угроз предлагается использовать разработанную модель и методы качественного анализа рисков. Пусть функция $\mathfrak{R}: A \times B \times C \rightarrow [0; 1]$ задает рискообразующий потенциал атаки $\vec{a} \in A$ при попытке взлома криптосистемы $\vec{c} \in C$ злоумышленником $\vec{b} \in B$. Тогда общая формула для определения рискообразующего потенциала атаки имеет вид:

$$\mathfrak{R}(\vec{a}, \vec{b}, \vec{c}) = \min_{h=1,9} \left(\prod_{g=1,6} \overline{I}_{gh}(c_g, a_h) \cdot \prod_{t=1,6} \overline{P}_{th}(b_t, a_h) \right), \text{ где}$$

$$\overline{I}_{gh}(c, a) = \frac{I_{gh}(c, a)}{\sum_{\xi \in C_g} I_{gh}(\xi, a)} \text{ и } \overline{P}_{th}(b, a) = \frac{P_{th}(b, a)}{\sum_{\beta \in B_t} P_{th}(\beta, a)}$$

Криптосистема $\vec{c} \in C$ подвержена атаке $\vec{a} \in A$ со стороны злоумышленника $\vec{b} \in B$, если $\mathfrak{R}(\vec{a}, \vec{b}, \vec{c}) > \theta$, т.е. рискообразующий потенциал превышает заданное пороговое значение $\theta \in [0; 1]$. Значение θ является настраиваемым параметром модели угроз и задается с учетом критичности защищаемых данных и средств злоумышленника и/или аудитора системы защиты.

В разделе 2.6 приведены результаты сравнения существующих методов обоснования инвестиций в средства обеспечения ИБ. Выделен набор финансово-экономических показателей для оценки эффективности СКЗИ с экономических позиций.

В разделе 2.7 проведен анализ разработанного метода и выявлены его основные достоинства и ограничения применимости.

Третья глава посвящена анализу и повышению эффективности методов криптоанализа асимметричных шифров. Криптостойкость асимметричных методов шифрования имеет наибольшее значение для функционирования механизмов, используемых в финансовых системах. Разработка новых и усовершенствование существующих методов криптоанализа является теоретической базой для создания инструментальных средств криптоанализа, которые используются на этапе 2 разработанного комплексного процесса комплексной оценки аппаратно-программных средств обеспечения конфиденциальности и целостности информации.

В разделе 3.1 приведен обзор методов решения задач факторизации и дискретного логарифмирования, на трудноразрешимости которых основана стойкость современных алгоритмов асимметричной криптографии.

В разделе 3.2 на основе анализа алгоритмов дискретного логарифмирования «index-calculus», использующих факторную базу, выделены два направления повышения их эффективности:

- исследование структуры матриц системы линейных уравнений (СЛУ) в классе вычетов (КВ), полученных в результате поиска гладких элементов;
- анализ применимости существующих алгоритмов решения СЛУ в КВ к системам, возникающим при дискретном логарифмировании с использованием методов «index-calculus».

На основе известного теоретического положения¹ (вероятность того, что целое число, произвольным образом выбранное из диапазона от 1 до x , является y -гладким ($y \leq x$), асимптотически (при $x \rightarrow \infty$) стремится к u^{-u} , где $u = \log x / \log y$) выдвинута гипотеза **1 о структуре матриц СЛУ в КВ, полученных в результате поиска гладких элементов**: это неравномерно разреженные СЛУ больших размеров, причем плотность заполнения столбцов, соответствующих самым малым простым числам из факторной базы, очень высока, а столбцы, соответствующие большим простым числам, сильно разрежены. Никакая перестановка не позволяет привести матрицу такой структуры к специальному виду (ленточной, блочно-диагональной и др.), для которых разработаны эффективные методы хранения и решения.

На основе анализа существующих алгоритмов поставлена задача разработки нового алгоритма, который эффективно использует свойство разреженности матриц; применим для решения СЛУ как в простых полях, так и в КВ; не требует факторизации; имеет лучшие оценки временной сложности, чем существующие методы.

В разделе 3.3 предложен новый алгоритм решения СЛУ в КВ, представляющий собой модификацию метода Жордана и в общем виде описанный на рис. 5. Для простоты рассмотрен случай, когда число уравнений системы равно числу неизвестных. Алгоритм легко модифицируется для решения системы, имеющей матрицу произвольного размера.

<i>Модиф_Жордан</i> (A, p)	
1.	$n \leftarrow \text{Число_Строк}(A)$
2.	$i \leftarrow n$
3.	<i>ДЛЯ</i> $j = i + 1, n$ <i>ЦИКЛ</i>
4.	<i>ВЫЧИСЛИТЬ</i> x', y', r', s' : $\left\{ \begin{array}{l} \text{НОД}(a_{ii}, a_{ji}) = a_{ii} \cdot x' + a_{ji} \cdot y' \\ 0 = a_{ii} \cdot r' + a_{ji} \cdot s' \end{array} \right\}$
5.	$\begin{pmatrix} A(i, *) \\ A(j, *) \end{pmatrix} \leftarrow \begin{pmatrix} x' & y' \\ r' & s' \end{pmatrix} \times \begin{pmatrix} A(i, *) \\ A(j, *) \end{pmatrix}$
6.	<i>ЕСЛИ</i> коэффициент a_{ii} необратим в \mathbb{Z}_{p-1}
7.	<i>ТО</i> выйти из алгоритма {матрица вырождена}
8.	<i>ИНАЧЕ</i> {обнуляем все элементы i -го столбца выше ведущего}
9.	$A(i, *) \leftarrow A(i, *) \cdot a_{ii}^{-1}$
10.	$A(j, *) \leftarrow A(j, *) - A(i, *) \cdot a_{ji}, \quad j = \overline{1, i-1}$
11.	$i \leftarrow i - 1$
12.	<i>ЕСЛИ</i> $i > 1$
13.	<i>ТО</i> перейти к шагу 2;
14.	<i>ИНАЧЕ</i> вернуть(A)

Рис. 5. Разработанный алгоритм решения СЛУ в КВ

¹ Das A. The discrete logarithm problem and its application to cryptography, Workshop on Cryptography and Data security, Jun 2000

Доказательство корректности алгоритма. Поскольку преобразования матрицы в описанном модифицированном алгоритме базируются на элементарных преобразованиях строк матрицы (умножение любой строки матрицы на обратимый элемент кольца; прибавление к любой ее строке другой строки, умноженной на произвольный элемент кольца; транспозиция строк), то полученная на выходе алгоритма матрица строчно эквивалентна исходной. Тогда по утверждению² соответствующие системы уравнений являются равносильными. Что и требовалось доказать. ■

В табл. 2 представлены результаты сравнения для системы n уравнений с m неизвестными в кольце вычетов \mathbb{Z}_{p-1} , $p-1 = \prod_{k=1}^t q_k^{\alpha_k}$ асимптотической временной сложности предложенного алгоритма и аналогов, описанных в современной литературе – детерминированных (в отличие вероятностных³) алгоритмов решения СЛУ в полях Гауа и кольцах вычетов. Для вывода формулы оценки сложности предложенного алгоритма $\Theta(n \cdot (nm + \log p))$ была использована оценка временной сложности алгоритма Евклида⁴ $T(a, b) = \Theta(1 + \log_{\varphi}(b/\text{НОД}(a, b)))$, где $a > b \geq 0$, $\varphi = (1 + \sqrt{5})/2$. Описание вывода формулы приведено в подразделе 3.3.3. диссертации.

Оценка временной сложности метода сведения к семейству систем над полями дана при условии использования для разложения на множители числа $p-1$ наиболее эффективного на сегодняшний день⁴ алгоритма «квадратичного решета» Померанца, имеющего временную сложность $L(p)^{1+o(1)}$, где $L(p) = e^{\sqrt{\ln p \ln \ln p}}$.

На основе полученных оценок выдвинута гипотеза **2 о существенной зависимости времени работы разработанного алгоритма от порядка исключения неизвестных для матриц, полученных в результате поиска гладких элементов**, а именно: при обработке матрицы от старших коэффициентов к младшим («обратный ход») алгоритм закончит работу в $c > 1$ раз быстрее, чем от младших к старшим (при «прямом ходе»).

Таблица 2.
Временная сложность алгоритмов решения СЛУ в КВ

Алгоритм	Временная сложность
Модифицированный метод Жордана	$\Theta(n \cdot (nm + \log p))$
Метод сведения к семейству систем над полями	$\Theta\left(n \cdot (n \cdot m \cdot \sum_{k=1}^t \alpha_k + \log p) + \sqrt{\ln p \ln \ln p} \cdot e^{\sqrt{\ln p \ln \ln p}}\right)$
Метод сведения к системе диофантовых уравнений (с построением матрицы Смита)	$\Theta(n^2 m^2 \log p)$

² Глухов М.М., Елизаров В.П., Нечаев А.А. Алгебра: Учебник. В 2-х т. Т. I - М.: Гелиос АРВ, 2003.(с. 185, Следствие из Теоремы 1)

³ Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. М.: МЦНМО, 2004.

⁴ Кормен Т., Лейзерсон Ч., Ривест Р. Алгоритмы: построение и анализ. М.: МЦНМО, 1999.

Четвертая глава работы посвящена практической реализации важного компонента комплексной оценки аппаратно-программных средств обеспечения конфиденциальности и целостности информации - набора инструментальных средств, позволяющих оценить способность криптографических средств противостоять идентифицированным угрозам. Глава содержит также описание экспериментальных исследований, направленных на оценку и повышение эффективности разработанного алгоритма решения СЛУ в КВ.

В разделе 4.1 определен набор основных требований к инструментальным средствам криптоанализа асимметричных шифров, на основе которого в разделе 4.2 проведен сравнительный анализ существующих программных решений и обоснована целесообразность разработки новых инструментальных средств. В разделе 4.3 описана реализация программного комплекса «Инструментальные средства криптоанализа асимметричных шифров» (далее – КРИПТО). КРИПТО включает два компонента: динамическую библиотеку КОНСТРУКТОР и приложение АНАЛИТИК. В КРИПТО реализованы самые эффективные на сегодня алгоритмы дискретного логарифмирования, которые имеют субэкспоненциальную временную сложность: алгоритм Копперсмита-Одлыжко-Шреппеля и решето числового поля. В числе алгоритмов факторизации – метод Полларда и «ЕСМ» (вероятностный алгоритм Ленстры для факторизации целых чисел с помощью эллиптических кривых). Для проверки чисел на простоту реализованы вероятностный алгоритм Миллера-Рабина и детерминированный алгоритм Миллера.

Для выполнения операций с длинными числами в библиотеке КОНСТРУКТОР использована известная свободно распространяемая математическая библиотека NTL (a Library for doing Number Theory). Выбор базовой библиотеки обусловлен её функциональностью, скоростью, компактностью и переносимостью. Приложение АНАЛИТИК написано на языке С#, обладает удобным графическим интерфейсом и обеспечивает пользователю доступ к функциям библиотеки КОНСТРУКТОР.

Целью проведения экспериментов, описанных в разделе 4.4, была проверка гипотез 1 и 2, а также экспериментальная оценка эффективности разработанного алгоритма решения СЛУ в КВ по сравнению с наилучшим из существующих аналогов – методом сведения к семейству систем над полями Галуа. Алгоритмы были реализованы в составе КРИПТО.

Эксперименты проводились на наборе исходных данных из матриц различных размерностей (от $n \sim 10$ до $n \sim 10^3$), полученных на первом этапе алгоритмов «index-calculus». На экспериментальных данных разработанный алгоритм показал время работы в 1,4 - 2 раза лучше, чем метод сведения к семейству систем над полями Галуа.

В результате проведенных экспериментов подтвердилась гипотеза 1 о структуре матриц, выдвинутая в разделе 3.2. Кроме того, было обнаружено, что в исходной матрице среди ненулевых элементов практически отсутствуют значения, по величине сравнимые с p .

С целью проверки гипотезы 2 для двух модификации разработанного алгоритма («прямой» и «обратный» ход) были построены графики функции плотности матрицы на i -й итерации алгоритма $D(i)$, которая вычислялась по формуле $D(i) = \frac{|N_i|}{n \cdot i} \cdot 100\%$, где $N_i = \{a_{kj} \in A_{n \times m} \mid a \neq 0, k = \overline{1, n}, j = \overline{1, n-i}\}$ - множество ненулевых коэффициентов на i -й итерации – см. рис. 6 (а). На рис. 6 (б) представлен график зависимости количества элементарных операций от плотности элементов в матрице, описываемый функцией $O(i) = \frac{n(n-i)D(i)}{100\%}$.

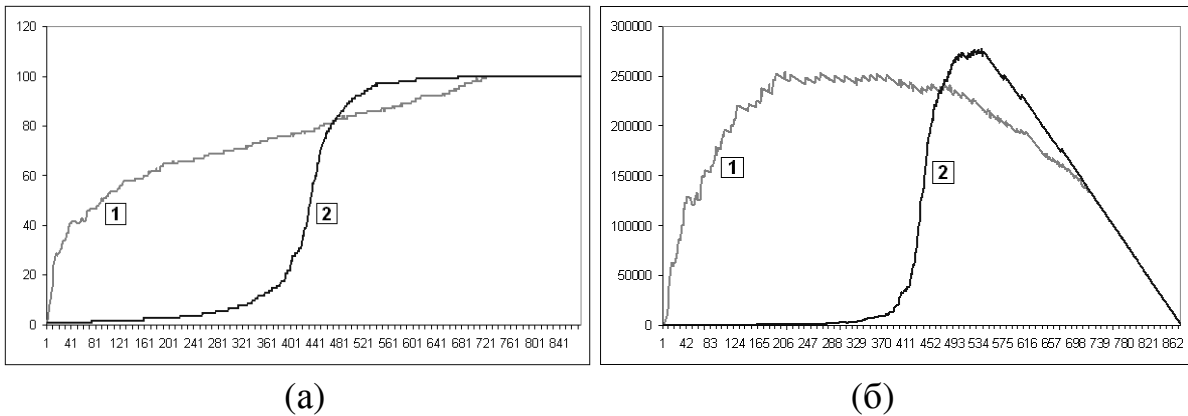


Рис. 6 – Плотность матрицы (а) и количество операций (б) на i -м шаге алгоритма: 1 – «прямой» ход, 2 – «обратный» ход

На рис. 7 показаны графики зависимости соотношения «больших» элементов M матрицы от номера i итерации алгоритма $M(i) = \frac{|\Lambda_i|}{|N_i|} \cdot 100\%$, где $\Lambda_i = \{a_{kj} \in A_{n \times m} \mid a \neq 0, a_{ij} = \Theta(p), k = \overline{1, n}, j = \overline{1, n-i}\}$ - множество больших коэффициентов на i -й итерации. Изменение порядка исключения неизвестных с учетом знания структуры матрицы позволяет вдвое сократить мультипликативную постоянную в оценке временной сложности предложенного алгоритма решения СЛУ в КВ, что подтверждает гипотезу 2 ($c \approx 2$).

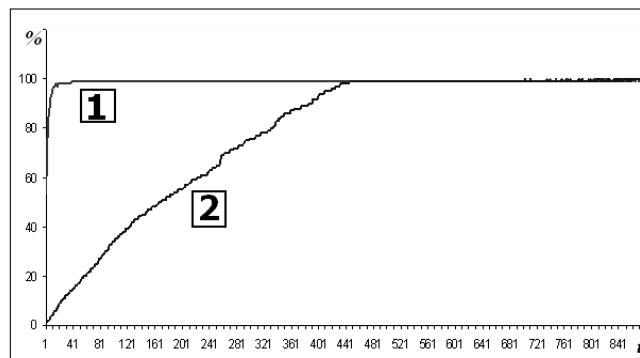


Рис. 7 – Процентное соотношение «больших» элементов матрицы к общему числу элементов на i -м шаге алгоритма: 1 – «прямой» ход, 2 – «обратный» ход

Полученные результаты по улучшению методов решения СЛУ в КВ для задачи дискретного логарифмирования имеют большое значение для достижения цели работы, т.к. прогресс в криптоанализе приводит к пересмотру безопасности шифров и поэтому является важной частью комплексной оцен-

ки аппаратно-программных средств обеспечения конфиденциальности и целостности информации.

В заключении приведены основные результаты, полученные в процессе проведенных исследований:

- разработаны требования к новому методу комплексной оценки аппаратно-программных средств обеспечения конфиденциальности и целостности информации на основе анализа стандартов семейства ИСО МЭК 27000 и изучения существующих моделей и методов;
- разработаны новые многокритериальные классификации злоумышленников, атак и средств обеспечения конфиденциальности и целостности;
- разработана модель угроз безопасности информационных ресурсов организации;
- разработан метод анализа рисков реализации угроз нарушения безопасности, использующий предложенные модели;
- разработан метод комплексной оценки аппаратно-программных средств обеспечения конфиденциальности и целостности информации;
- разработан комплекс программ для решения задач дискретного логарифмирования, факторизации и проверки чисел на простоту;
- разработан новый детерминированный метод решения систем линейных уравнений в кольцах вычетов, позволяющий ускорить работу алгоритмов дискретного логарифмирования типа index-calculus.

Приложение содержит копии документов, подтверждающих внедрение результатов диссертационной работы.

ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

1. Авдошин С.М., Савельева А.А. О новом подходе к проблеме анализа эффективности криптосистем // Информационные технологии, № 8, 2009, С. 2-9.
2. Авдошин С.М., Савельева А.А. Криптоанализ: вчера, сегодня, завтра. // Открытые системы. № 3, 2009, с. 22-25.
3. Авдошин С.М., Савельева А.А. Алгоритм решения систем линейных уравнений в кольцах вычетов // Информационные технологии, №2, 2006, С. 50-54.
4. Савельева А.А. Инструментальные средства криптоанализа // Сборник материалов Всероссийского конкурса инновационных проектов аспирантов и студентов по приоритетному направлению развития науки и техники «Информационно-телекоммуникационные системы». М. - ГНИИ ИТТ «Информика», 2005. – 132 с. С. 44.
5. Савельева А.А. Метод решения систем линейных уравнений в кольцах вычетов // XXXI Гагаринские чтения. Тезисы докладов Международной молодежной научной конференции. Т.4. М. - МАТИ, 2005. – С. 29-30.
6. Савельева А.А. Анализ стойкости криптосистем, основанных на сложности задачи дискретного логарифмирования // Информационные технологии в бизнесе: Тезисы докладов научно-технической конференции студентов, аспирантов и молодых специалистов. Москва, 2006. С. 130-134.
7. Савельева А.А. Криптоанализ шифров, основанных на сложности задачи дискретного логарифмирования в конечных полях. // XXXII Гагаринские чтения. Тезисы докладов Международной молодежной научной конференции. Т.4. М.- МАТИ, 2006. – 154 с.

8. Савельева А.А. Исследование алгоритмов дискретного логарифмирования и способы повышения их эффективности // «Новые информационные технологии: Сб. тез. докладов XIV Международной студенческой школы-семинара». М.- МИЭМ, 2006. С. 411-412.
9. Савельева А.А. Новый подход к решению систем уравнений в задачах дискретного логарифмирования // Программное и информационное обеспечение систем различного назначения на базе персональных ЭВМ: Межвузовский сборник научных трудов / Под ред. д.т.н., проф. Михайлова Б. М. М.- МГУПИ, 2006. Вып. 9 - С. 193-197.
10. Авдошин С.М., Савельева А.А. Криптоанализ: современное состояние и перспективы развития // М.: Новые технологии, 2007. – 32 с. – (Приложение к журналу «Информационные технологии»; N 3, 2007). С. 2-32.
11. Савельева А.А. Исследование эффективности алгоритмов дискретного логарифмирования, использующих факторную базу // Модернизация экономики и общественное развитие: сб. студенч. работ. М.: Изд. Дом ГУ ВШЭ, 2007. – 498 с.
12. Авдошин С.М., Савельева А.А. Криптотехнологии Microsoft // М.: Новые технологии, 2008. – 32 с. – (Приложение к журналу «Информационные технологии»; N9, 2008). С. 2-32.
13. Авдошин С.М., Савельева А.А. Проблемы оценки криптозащищенности информационных систем // «Новые информационные технологии». Тезисы докладов XVI Международной студенческой школы-семинара - М.: МИЭМ, 2008. – 297 с. С. 15-29.
14. Savelieva A. Formal methods and tools for evaluating cryptographic systems security // St. Petersburg, ISP RAS, In Proceedings of the Second Spring Young Researchers Colloquium on Software Engineering (SYRCoSE'2008), 2008, Vol 1. Pp. 33-36.
15. Авдошин С.М., Савельева А.А. Оценка эффективности криптографической защиты информационных ресурсов в корпоративных системах // Труды международной конференции Software Engineering Conference (Russia) 2008, Москва. С. 298 – 316.
16. Савельева А.А. Оценка экономической эффективности средств обеспечения информационной безопасности // XXXIV Гагаринские чтения. Научные труды Международной молодежной научной конференции в 8 томах. Т. 6. – М.: МАТИ, 2008. С. 80-81.
17. Savelieva A. Modeling Security Threats to Cryptographically Protected Data // In Proceedings of the Third Spring Young Researchers' Colloquium on Software Engineering (SYRCoSE 2009). May 28-29, 2009. – Moscow, Russia. Pp. 56 – 60.
18. Савельева А.А. Разработка программного комплекса для анализа стойкости асимметричных шифров. - В сб.: “Технологии Microsoft в теории и практике программирования: Труды VI Всерос. конференции студентов, аспирантов и молодых ученых. Центр. регион. Москва, 1-2 апреля 2009 г.” - М.: Вузовская книга, 2009, с. 51-52.
19. Савельева А.А. Математическая модель угроз безопасности информационных ресурсов. - В сб.: “XXXV ГАГАРИНСКИЕ ЧТЕНИЯ. Научные труды Международной молодежной научной конференции. М., 7-10 апреля 2009 г.” - М.: МАТИ, 2009. Т.4, с. 152-153.
20. Авдошин С.М., Савельева А.А. Программа решения систем линейных уравнений в кольцах вычетов. Свидетельство об официальной регистрации программы для ЭВМ № 2005612258. Зарегистрировано в Реестре программ для ЭВМ 02.09.2005.
21. Авдошин С.М., Савельева А.А. Программа решения систем линейных уравнений в кольцах вычетов. Свидетельство об отраслевой регистрации разработки № 5410. Зарегистрировано Государственным координационным центром информационных технологий в Отраслевом фонде алгоритмов и программ 23.11.05.
22. Авдошин С.М., Савельева А.А. Инструментальные средства криптоанализа асимметричных шифров. Свидетельство о государственной регистрации программы для ЭВМ № 2008612526. Зарегистрировано в Реестре программ для ЭВМ 10.03.2008.
23. Авдошин С.М., Савельева А.А. Инструментальные средства криптоанализа асимметричных шифров. Свидетельство об отраслевой регистрации разработки № 10193 Зарегистрировано в ОФАП (Отраслевом фонде алгоритмов и программ) 18.03.2008.