На правах рукописи

Гончаров Павел Игоревич

СОВЕРШЕНСТВОВАНИЕ ИНСТРУМЕНТАЛЬНЫХ СРЕДСТВ ВЫЯВЛЕНИЯ УТЕЧЕК ИНСАЙДЕРСКОЙ ИНФОРМАЦИИ В ФИНАНСОВО-КРЕДИТНЫХ ОРГАНИЗАЦИЯХ

08.00.13 - Математические и инструментальные методы экономики

Автореферат
диссертации на соискание ученой
степени кандидата экономических наук

Москва
2013

Работа выполнена на кафедре «Информационные технологии» ФГОБУВПО «Финансовый университет при Правительстве Российской Федерации»

Научный руководитель: доктор технических наук, старший научный сотрудник **Вепрев Сергей Борисович**

Официальные оппоненты: **Конявский Валерий Аркадьевич,**
доктор технических наук
ФГУП «Всероссийский научно-исследовательский институт проблем вычислительной техники и информатизации», научный руководитель

Дорофеев Михаил Львович
кандидат экономических наук
ФГБОУ ВПО «Российский экономический университет имени Г.В. Плеханова», доцент кафедры «Финансы и цены»

Ведущая организация **ФГБОУ ВПО «Московский государственный университет экономики, статистики и информатики» «МЭСИ»**

Защита состоится «21» декабря 2013г. в 10-00 часов на заседании диссертационного совета Д 505.001.03 на базе ФГОБУВПО «Финансовый университет при Правительстве Российской Федерации» по адресу: Ленинградский проспект, д.55, ауд. 213, Москва, 125993.

С диссертацией можно ознакомиться в диссертационном зале Библиотечно-информационного комплекса ФГОБУВПО «Финансовый университет при Правительстве Российской Федерации» по адресу: Ленинградский проспект, д.49, комн.203, Москва, 125993.

Автореферат разослан «20» ноября 2013г. Объявление о защите диссертации и автореферат диссертации «20» ноября 2013г. размещены на официальном сайте Высшей аттестационной комиссии при Министерстве образования и науки Российской Федерации по адресу http://vak.ed.gov.ru и на официальном сайте ФГОБУВПО «Финансовый университет при Правительстве Российской Федерации»: http://www.fa.ru.

Ученый секретарь
диссертационного совета Д505.001.03,
к.э.н., доцент О.Ю. Городецкая

I. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. Одним из важнейших факторов повышения эффективности функционирования предприятий и организаций в настоящее время является активное внедрение новых информационных технологий. Однако этот процесс сопровождается нарастанием зависимости общества от информационной сферы, а величина ущерба от возникающих в ней рисков постоянно увеличивается.

С ростом ценности коммерческой информации существенно возрастают и риски, связанные с утратой ее конфиденциальности вследствие неправомерных действий внешних и внутренних злоумышленников. При этом, чем крупнее и значимее компания, тем агрессивнее и профессиональнее производятся попытки несанкционированного доступа к её информации. В настоящее по разным оценкам до 35% экономических потерь связано с экономическим шпионажем.

Долгое время основными рисками в информационной сфере считались внешние угрозы. Поэтому основные усилия были сосредоточены на решении задачи защиты конфиденциальных данных от попыток доступа извне. Однако исследования последних лет убедительно показали, что основным источником утечки информации являются работники самой компании, имеющие доступ к конфиденциальным данным. Было установлено, что внешние и внутренние угрозы на сегодняшний день соотносятся друг с другом как 20 к 80. Таким образом, в 80% случаев осуществление несанкционированных действий и кража конфиденциальных данных производится при непосредственном участии сотрудников самой организации.

В настоящее время контроль информационных рисков от внутренних источников обеспечивается в основном комплексом организационно-правовых мер и ограниченного числа инструментальных средств, разработанных для определения совершившихся фактов утечки данных. Однако во многих случаях такой подход

является неприемлемым. В особенности это касается организаций финансово-кредитной сферы, где несанкционированный доступ к информационной системе может привести к осуществлению транзакций, наносящих существенный ущерб организации. Еще более сложную проблему представляет несанкционированный доступ к конфиденциальной коммерческой информации, которую инсайдер может использовать в личных корыстных целях. Предотвращение и расследование такого рода преступлений, в особенности, если они не сопровождаются передачей информации по техническим каналам, без наличия специализированного инструментария является крайне сложной, а порой и неразрешимой задачей.

В этой связи особую актуальность приобретает проблема создания и развития инструментальных средств, позволяющих устойчиво выявлять не только сами попытки несанкционированного доступа инсайдеров к информационной системе, но и проводить идентификацию их личности.

Степень разработанности проблемы. Общие вопросы управления информационными рисками и информационной безопасностью рассматривали в своих работах В.И. Авдийский, Р. Ален, И.Т. Балабанов, Н. Винер, В.А Галатенко, В.А. Герасименко, А.М. Дубров, В.Ю. Завгородний, П.Д. Зегжда, М. Кастельс, А.Н. Колмогоров, В.А. Конявский, В.В. Кульба, Б.А. Лагоша, М.М. Максимцов, С. Мун, Ф.Х. Найт, С.А. Петренко, В.К. Сенчаков, Д.И. Стенг, А.А. Стрельцов, Л.Дж. Хоффман, К. Шеннон, А.Ю. Щербаков и другие ученые. В их работах сформулирован научный подход к пониманию сущности информационных рисков, развит теоретико-методологический аппарат анализа и управления информационными рисками, а также предложен методологический инструментарий оценки и оптимизации расходов на управление информационными рисками. Однако в работах указанных ученых не представлено конкретных рекомендаций по выявлению и идентификации рисков, формируемых инсайдерами.

Исследования по теме проблемы снижения информационных рисков от деятельности злонамеренных инсайдеров проводили: А.А. Малюк, В.С. Горбатов,

К.В. Харский, С.И. Журин, А.В. Старовойтов, Ю.А. Журавлев, Б.А. Позин, В.И. Скиба, В.В. Курбатов, В.Л. Евсеев, С.А. Петренко, А.А. Панов, А.А. Зудочкина, М.В. Емельянников, А.А. Чемин, P. Russell, M. Randazzo, L. Ponemon, J.J.B. Carpenter, G. Doug, J. Ignacio Martinez-Moyano, Eliot Rich и др.

Вопросы управления информационной безопасностью и рисками описаны в отечественных и зарубежных отраслевых стандартах, а также в руководящих документах государственных регуляторов. В частности, вопросы управления рисками и методы защиты банковской информации систематизированы в стандарте Банка России по обеспечению информационной безопасности организаций банковской системы Российской Федерации (СТО БР ИББС), а также в руководящих документах ФСТЭК.

Проблемы управления рисками и методы защиты банковской информации от внутренних нарушителей рассматривались в работах А.А. Малюка, С.И. Журина, В.С. Горбатова, В.А. Баранова, А.А. Панова и других исследователей.

Анализ работ указанных авторов и официальных документов показал, что наряду с достаточно глубокой проработанностью проблемы имеют место дискуссионность подходов к выявлению и методам предотвращения некоторых видов утечки информации ввиду недостаточно совершенных инструментальных средств борьбы с утечками данных. Так, отсутствуют инструментальные средства для выявления инсайдеров, проходящих аутентификацию за чужим рабочим местом, а те инструментальные средства, которые выявляют таких нарушителей в процессе их работы, недостаточно эффективны и практически не используются.

При исследовании проблематики выявления внутренних нарушителей представляются перспективными идеи анализа клавиатурного почерка при аутентификации пользователя. Проблемы внедрения методов аутентификации и применения клавиатурного почерка были исследованы в работах таких ученых, как Д.Е. Рыбченко, В.Ю. Завгородний, Ю.Н. Мельников, Р.Р. Шарипов, М.Н. Казарин, В.Г. Абашин, Е.Ю. Костюченко и др. Однако, применительно к задаче выявления

инсайдера, проходящего аутентификацию под чужими учетными данными, подобные исследования до настоящего времени не проводились.

Необходимость совершенствования инструментальных средств предотвращения несанкционированного доступа к информации со стороны злонамеренных инсайдеров обусловили выбор темы исследования, предопределяя ее структуру, цель и задачи.

Целью диссертационного исследования является решение научной задачи совершенствования методов и инструментальных средств, позволяющих снизить риск утечки инсайдерской информации.

Для достижения указанной цели были поставлены и решены следующие задачи:

1. Систематизировать экономические риски, связанные с утечкой инсайдерской информации в финансово-банковской сфере.
2. Провести анализ существующих методов и инструментов снижения рисков несанкционированного доступа инсайдеров к информационной системе организации.
3. Провести экспериментальные исследования в целях получения эмпирических данных о возможности выявления несанкционированных попыток входа в информационную систему и идентификации злонамеренных инсайдеров на основе анализа присущих им особенностей клавиатурного ввода данных.
4. Создать математическую модель аутентификации пользователя, позволяющую выявлять санкционированные и несанкционированные попытки входа в систему, и разработать поддерживающий её инструментальный комплекс.
5. Оценить экономическую эффективность применения разработанного инструментального средства для компании финансовой сферы.

Объект исследования. Угрозы утечки конфиденциальной информации в результате несанкционированной деятельности инсайдеров.

Предмет исследования. Математические модели и инструментальные методы защиты информации.

Теоретические и методологические основы исследования. Правовую базу исследования составили законодательные акты Российской Федерации, официальные политические и нормативные правовые документы в области информационной безопасности. Методологическую базу составили современные результаты научных исследований отечественных и зарубежных ученых, диссертации в области управления информационными рисками. В качестве теоретической основы использованы результаты фундаментальных и прикладных исследований, опубликованных в периодических изданиях, монографиях и материалах научных конференций. В процессе диссертационного исследования были использованы следующие методы: абстракции, системного и сравнительного анализа, синтеза, дедукции, экспертных оценок, статистико-вероятностный. Совокупность используемой методологической базы позволила обеспечить достоверность, обоснованность теоретических выводов и практических решений. Информационно-статистической базой исследования послужили данные российских и зарубежных компаний, занимающихся сбором информации об инсайдерских инцидентах, Центрального банка Российской Федерации, материалы международных организаций из отрасли информационной безопасности, информационных агентств, Интернет-ресурсы.

Гипотеза исследования. Количественно измеряемые особенности клавиатурного ввода данных являются уникальным биометрическим параметром, позволяющим устойчиво идентифицировать конкретного пользователя информационной системы.

Эмпирическая база исследования. Использованная в диссертации информация была получена на основе анализа доступных документов и статистики,

экспертных оценок, данных СМИ, а также в ходе экспериментов по сбору и обработке биометрических данных пользователей информационной системы ОАО «Концерн «Системпром».

Область исследования. Диссертация выполнена в рамках п. 1.10 – Разработка и развитие математических моделей и методов управления информационными рисками Паспорта специальности 08.00.13 – Математические и инструментальные методы экономики (экономические науки).

Научная новизна заключается в разработке комплекса моделей и инструментов предотвращения несанкционированного доступа к конфиденциальной информации за счет устойчивой идентификации пользователей информационных систем на основе анализа особенностей их клавиатурного почерка.

Новыми являются следующие научные результаты:

1. Проведена систематизация информационных рисков и их последствий, связанных с несанкционированной деятельностью инсайдеров в финансовой сфере.
2. На основе развернутых эмпирических исследований сделан вывод о том, что количественно измеримые особенности клавиатурного ввода (клавиатурная подпись) пользователей информационных систем являются их устойчивой биометрической характеристикой, позволяющей проводить их идентификацию.
3. Предложен метод контроля правомерности доступа пользователей к конфиденциальной информации на основе анализа соответствия их клавиатурной подписи данным, оперативно фиксируемым при их аутентификации в информационной системе.
4. Разработана математическая модель анализа соответствия клавиатурного почерка пользователя оперативным данным, фиксируемым при его аутентификации.
5. Разработан комплекс инструментальных средств формирования выводов о

соответствии клавиатурного почерка пользователя фактическим параметрам клавиатурного ввода аутентификационных данных.

6. На основе анализа эмпирических данных, полученных в результате использования предложенного инструментария, сделан вывод о высокой надежности автоматически формируемых им выводов о правомерности доступа данного пользователя к запрашиваемой им информации.
7. Предложены механизмы встраивания разработанного инструментального комплекса оперативной идентификации пользователей в действующие автоматизированные банковские системы.
8. Представлена методика расчета экономической эффективности использования разработанного инструментария, основанная на оценке возврата инвестиций.

Теоретическая значимость исследования заключается в совершенствовании математических и инструментальных методов защиты информации от несанкционированного доступа, обеспечивающих снижение риска от утечки инсайдерской информации.

Практическая значимость заключается в том, что разработанные в исследовании математическая модель и инструментальные средства ориентированы на широкое применение в информационных системах финансово-кредитных организаций.

Самостоятельное практическое значение имеют:

- методика и инструментальные средства автоматического сбора информации, необходимой для формирования базы данных сведений о клавиатурных подписях сотрудников организации;
- метод контроля правомерности доступа пользователей к конфиденциальной информации на основе анализа соответствия их клавиатурной подписи данным, оперативно фиксируемым при их аутентификации в информационной системе;

- математическая модель анализа соответствия клавиатурного почерка пользователя оперативным данным, фиксируемым при его аутентификации;
- комплекс инструментальных средств формирования выводов о соответствии клавиатурного почерка пользователя фактическим параметрам клавиатурного ввода аутентификационных данных;
- рекомендации по использованию разработанного инструментального средства в финансово-кредитных и иных организациях.

Отдельные положения и результаты исследования могут быть использованы при изучении дисциплин «Банковские информационные технологии» и «Электронный банкинг».

Апробация и внедрение результатов исследования. Основные результаты изложены и обсуждены на научной конференции «Современные тенденции развития теории и практики управления в системах специального назначения» в честь 20-летия ФГУП «Концерн «Системпром» (Москва, ФГУП «Концерн «Системпром», 13 мая 2011 г.); Современные тенденции развития теории и практики управления в системах специального назначения (Москва, ОАО «Концерн «Системпром», 15 мая 2012 г.); Всероссийская научная конференция «Современные тенденции развития теории и практики управления в системах специального назначения» (Москва, ОАО «Концерн «Системпром», 13 мая 2013 г.).

Диссертационное исследование выполнено в рамках научно-исследовательских работ ФГОБУ ВПО «Финансовый университет при Правительстве Российской Федерации» по теме «Инновационное развитие России: социально-экономическая стратегия и финансовая политика» по межкафедральной подтеме «Информационные технологии как фактор инновационного развития экономики».

Результаты диссертационного исследования используются в практической деятельности Коммерческого банка «Рублевский», филиал «Гостиный Двор».

Использование представленных в диссертационной работе методов и рекомендаций, позволило автоматизировать контроль выполнения политики информационной безопасности банка в части запрета использования сотрудниками чужих АРМ.

Материалы исследования используются ООО «СМП Лтд» отделом информационной безопасности для снижения рисков от внутренних источников угроз утечки конфиденциальной финансовой информации.

Разработанный модуль анализа клавиатурной подписи используется ОАО «Концерн «Системпром» и ЗАО «Всесоюзный институт волоконно-оптических сетей связи и обработки информации» как составная часть комплексных систем защиты информации.

В учебном процессе материалы исследования используются кафедрой системного анализа экономического факультета ФГБОУ ВПО «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации» в преподавании учебных дисциплин «Комплексное обеспечение безопасности автоматизированных систем. Модуль – Личная информационная безопасность руководителя» и «Практический маркетинг. Модуль – конкурентная разведка».

Публикации и апробация работы. По теме диссертации опубликовано пять печатных работ общим объемом публикаций 4,28 п. л. (авторский объем – 3,88). В том числе три работы авторским объемом 3,43 п. л. – в журналах, определенных ВАК Минобрнауки России.

Структура и диссертации. Диссертация состоит из введения, трех глав и выводов по каждой главе, заключения и списка литературы из 59 наименований. Объем диссертации составляет 133 страницы, в том числе 26 рисунков и 8 таблиц.

II. ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

1. Систематизация информационных рисков и их последствий, связанных с несанкционированной деятельностью инсайдеров.

На основании изучения исследований профильных организаций в работе выявлено, что наиболее актуальными источниками информационных угроз в настоящее время являются:

- внутренние источники, реализующие угрозы в рамках своих полномочий и за их пределами (авторизованные пользователи и операторы автоматизированных систем, представители менеджмента организации и пр.);
- комбинированные источники угроз: внешние (например, конкуренты) и внутренние, действующие в сговоре.

Анализ инцидентов подтверждает, что внутренние угрозы более опасны, чем внешние и наиболее громкие скандалы и утечки конфиденциальных данных последних лет, повлекшие за собой крупные потери для компаний, произошли в результате участия внутренних нарушителей.

Проведен анализ отраслевой специфики утечки и интересующей злонамеренных инсайдеров информации, что позволило сделать вывод о том, что информационные активы, которыми обладают финансово-кредитные организации, имеют не только особенную ценность для злоумышленников, но и добавляют дополнительные риски в связи с особенностями их обработки. Помимо крупных баз данных, содержащих персональные данные, особый интерес злоумышленников вызывают детали конкретных сделок, интеллектуальная собственность и другие данные, которые не требуется копировать на внешние носители или передавать по сети, а достаточно запомнить.

На основании обобщения исследований отечественных и зарубежных

компаний была произведена оценка экономических потерь от действий внутренних нарушителей. Всего по данным событий инсайдерских инцидентов в мире за 2011 год оценочный ущерб составил $20,586 млрд. В среднем, каждая утечка информации обошлась в $25,13 млн. Суммарное число скомпрометированных записей персональных данных составило свыше 350 млн. Суммарный ущерб российских компаний от утечек данных оценивается экспертами в более чем $1 млрд.

Утечки конфиденциальной информации могут приводить к следующим видам ущерба для организаций финансово-кредитной сферы:

- упущенная выгода в результате испорченной репутации банка на рынке;
- манипуляции при выдаче кредита;
- штрафы от контролирующих организаций (Центробанк, платёжные системы, Роскомнадзор и другие);
- судебные иски, компенсации по ним;
- снижение котировок акций в результате снижения репутации или публикации инсайдерской информации;
- прямые убытки: стоимость научно-технических разработок, стоимость проигранных тендеров и т.д.

Общая сумма ущерба от каждой конкретной утечки информации складывается из «стоимости» каждого источника ущерба. В зависимости от величины компании средняя стоимость утечки информации обходится от 2 до 25 млн. долл. Особое значение имеют репутационные издержки. По данным из различных источников следствием средней информационной утечки является отток 2,67% клиентов компании, что является достаточно высоким показателем в масштабах крупной организации.

В работе проведен развернутый анализ инструментальных средств защиты от утечки конфиденциальных данных (*DLP*-система (*Data Leak Protection*)), а также

проблем, возникающих при их использовании. В результате сделан вывод, что *DLP*-системы снижают многие риски, связанные с внутренним нарушителем, но у злоумышленника остается возможность сфотографировать экран монитора или запомнить данные, доступ к которым у него уже есть, и передать третьим лицам. От такого типа утечки не может защитить ни одна *DLP*-система.

Показано, что особую проблему составляют противоправные действия, связанные с использованием информационных ресурсов за счет доступа к ним с чужого рабочего места или под чужой учетной записью. По данным авторитетных источников такого рода инциденты случались в 81% случаев, повлекших финансовые потери или ухудшение репутации банка.

2. Сбор и обработка эмпирических данных о количественно измеримых индивидуальных особенностях клавиатурного ввода.

В работе показано, что для борьбы со злонамеренными инсайдерами, использующими чужие учетные данные для входа в информационную систему, неэффективно использование алгоритмов анализа действий в сети или в АРМ, а также организационных мероприятий.

Поэтому было предложено использовать скрытые методы аутентификации для пресечения доступа к конфиденциальной информации уже на этапе доступа в систему. Основная проблема при использовании данного подхода состоит в том, что необходимо выявлять персональные особенности работы каждого пользователя с компьютером для идентификации его личности, чтобы использовать скрытую аутентификацию, позволяющую выявить попытку использования чужих учетных данных.

Для проведения скрытой аутентификации был выбран метод, основанный на клавиатурном почерке, как наиболее незаметный, не требующий дополнительных технических средств и доступный для применения при удаленном доступе с любого устройства.

В работе проведён опыт по получению биометрических характеристик

клавиатурного ввода и их анализу. Так как производится дополнительная скрытая аутентификация, то можно использовать только метод набора определенной ключевой фразы, а не случайно выдаваемого текста. В качестве ключевой фразы используется пара: имя пользователя и пароль.

В качестве основных параметров для контроля были использованы:

- время между вводом символов;
- время между вводом *Ctrl+Alt+Delete* и началом ввода логина;
- время между окончанием ввода логина и переноса фокуса на поле «пароль»;
- время между окончанием ввода пароля и передачей на проверку.

Модифицированная библиотека *msgina.dll*, отвечающая за процедуру аутентификации в операционной системе *Windows XP* была внедрена на пяти АРМ предприятия ОАО «Концерн «Системпром» в период с декабря 2012 по апрель 2013 г. для набора статистики, необходимой для подтверждения или опровержения гипотезы о возможности использования особенностей клавиатурного ввода как устойчивой биометрической характеристики.

Анализ полученных данных подтвердил, что клавиатурная подпись является устойчивой биометрической характеристикой. Для проверки гипотезы в работе была выбрана информационно-аналитическая система *Deductor*, в которой был проведён анализ данных следующими методами:

- линейной регрессии (построение линейной модели);
- логистической регрессии (построение бинарной модели);
- с помощью нейросети.

В качестве примера далее приведены данные анализа, полученные с помощью трех способов для одного из пользователей, на АРМ которого происходил съем биометрических характеристик.

При анализе полученных данных *методом линейной регрессии* в случае

наличия всего 167 замеров, где 139 замеров от легального пользователя и 28 являющихся имитацией действий нарушителя, верно классифицировано 166 замеров, или 99,4%; неверно – 1, или 0,6%;

При анализе полученных данных *методом логистической регрессии* в случае наличия такого же количества замеров, были распознаны все 100% случаев.

Анализ полученных данных с помощью *построения нейросети* проводился для различного количества нейронов (7, 12, 13, 30), различной крутизны сигмоиды и методом *Back-Propagation*, где коррекция весов производится после предъявления каждого примера обучающего множества. В результате анализа рассмотренной выше выборки были распознаны все 100% случаев.

По результатам эксперимента были выявлены закономерности, позволяющие провести скрытую аутентификацию пользователя. Все выбранные параметры, если анализировать общую картину для каждого пользователя, достаточно стабильны, но при этом для большинства параметров случаются «выпады», т.е. увеличение времени, из-за того, что пользователь отвлекся на что-либо, или из-за возникновения ошибок. Чаще всего «выпады» (рис. 1) случаются у легальных пользователей, так как они более расслаблены и случайные ошибки у них проявляются чаще. Нарушитель же более собран и сосредоточен, поэтому в большинстве замеров ошибки и, как следствие, увеличение интервалов времени замечаются гораздо реже.

Анализ полученных данных для каждого пользователя привел к выводу, что распределение интервалов между нажатиями клавиш и дополнительные характеристики имеют гамма-распределение.

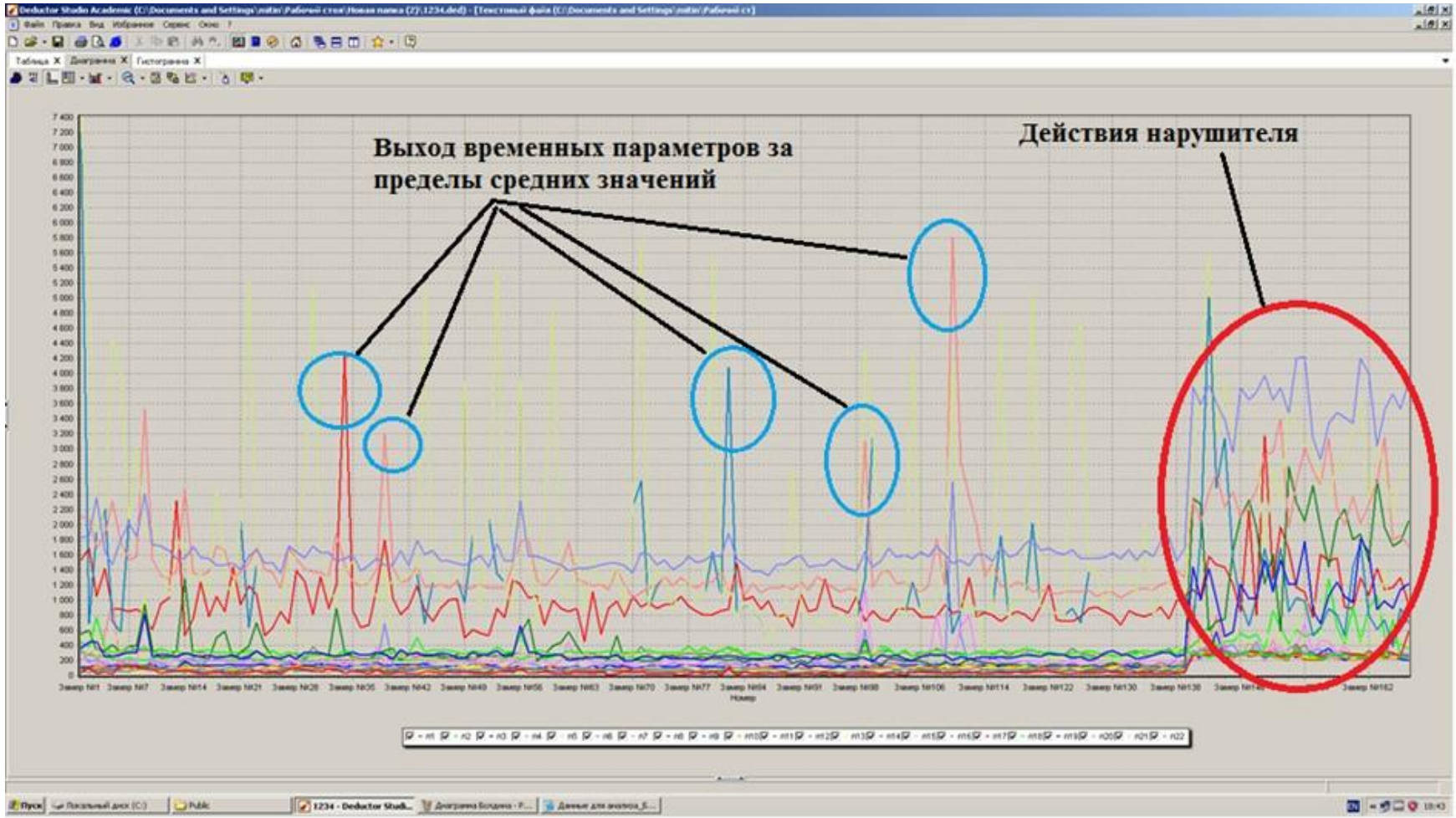

Рис. 1. – Визуализация фиксируемых параметров

Исходя из особенностей гамма-распределения, можно сделать вывод, что после продолжительной тренировки нарушителем будет увеличиваться число ошибок первого рода. Для выработки иного метода, позволяющего противостоять квалифицированным внутренним нарушителям, осуществляющим прямую атаку на клавиатурную подпись, потребовалось провести ряд проверок. Так, с помощью эмпирических методов удалось обнаружить, что, несмотря на то, что интервалы между нажатиями клавиш и дополнительные характеристики носят нормальный характер, разница между парами символов для каждого пользователя гораздо более выражена. То есть, набор учетных данных имеет устойчивое соотношение между временными интервалами между рассматриваемыми параметрами. Вследствие указанных выше причин необходимо производить нормировку.

Также было обнаружено, что еще более выраженный результат получается при нормализации входных данных. Это достигается за счет деления параметров одного замера на сумму всех замеров.

Эксперимент показал, что наиболее устойчивыми и стабильными являются те временные параметры, которые имеют меньшую продолжительность. Чем больше временной интервал, тем чаще случаются выпадения из него. Вследствие указанной выше причины *ИАС Deductor* или аналогичные будут давать однозначный ответ при аутентификации, что может привести к ошибкам первого или второго рода. При действиях подготовленного нарушителя это может привести к признанию злонамеренного инсайдера легальным пользователем. Для предотвращения подобных событий был выработан критерий доверия. Для каждого пользователя на основе полученных данных рассчитывается диапазон значений критерия, по которому будет определяться, кто пытается пройти проверку – однозначно пользователь, нарушитель, или существует неопределенность и требуется вмешательство администратора.

3. Математическая модель анализа параметров клавиатурной подписи при аутентификации.

***Разработка критерия*:**

Разница между вводом *i*-го символа в текущем замере и эталонным:

$$(t_i^* - t_i)^2; \qquad (1)$$

где t_i^* – среднее время перехода $П_i$ и t_i – текущее время перехода $П_i$.

Сравнение возводится во вторую степень, так как t_i^* может быть меньше t_i.

Суммируются значения всех параметров:

$$\sum_{i=1}^{n}(t_i^* - t_i)^2, \qquad (2)$$

где n – количество всех параметров, фиксируемых для данного пользователя.

Нормированное время:

$$\tau_i = \frac{t_i}{\sqrt{\sum_{i-1}^{n} t_i^2}}; \qquad (3)$$

$$\tau_i^* = \frac{t_i^*}{\sqrt{\sum_{i-1}^{n} t_i^{*2}}}. \qquad (4)$$

Обозначается:

$$T = \sqrt{\sum_{i-1}^{n} t_i^2}, \qquad (5)$$

где T – нормированное время всех периодов для одного замера.

$$T^* = \sqrt{\sum_{i-1}^{n} t_i^{*2}}, \qquad (6)$$

где T^* – среднее время периодов всех замеров, соотнесенное с конкретным пользователем.

Сравнение при нормированном времени:

$$\sum_{i=1}^{n} \left(\frac{t_i^*}{T^*} - \frac{t_i}{T}\right)^2. \qquad (7)$$

Эмпирически полученные данные показывают, что чем меньше время

параметра, тем реже пользователь в нем ошибется. Поскольку значимость конкретного параметра набора зависит от устойчивости его набора конкретным пользователем (индивидуальные навыки), требуется вывести весовые коэффициенты важности каждого параметра. Для эталонного значения он определяется статистическими параметрами устойчивости ввода данных. Чем меньше отклонений совершает пользователь при текущем наборе заданного параметра от среднестатистического, тем важнее будет его значение:

$$k_i^* = T^* \ \sigma_i. \qquad (8)$$

Вес параметра k_i^* берется пропорциональным обратной величине среднеквадратического отклонения σ_i. Поскольку полученные экспериментальные данные показали, что чем меньше для конкретного пользователя интервал набора заданного параметра, тем устойчивее он осуществляет его набор; весовой коэффициент важности связываем с временем набора. Поскольку при текущем наборе не имеется статистических данных, весовой коэффициент определяется обратно пропорциональным времени набора:

$$k_i = T \ t_i. \qquad (9)$$

В итоге получается коэффициент важности:

$$V = \frac{T^* T}{\sigma_i t_i} \sum_{i=1}^{n} \left(\frac{t_i^*}{T^*} - \frac{t_i}{T} \right)^2 = \sum_{i=1}^{n} \frac{t_i T^* - t_i^* T^{\,2}}{t_i T^* \, \sigma_i T}. \qquad (10)$$

Поскольку значение *V* может быть больше единицы, для удобства представления и сравнения значений следует произвести нормирование:

$$W = e^{-\sum_{i=1}^{n} \frac{t_i T^* - t_i^* T^{\,2}}{t_i T^* \, \sigma_i T}}. \qquad (11)$$

Значение *W* задает критерий легальности клавиатурной подписи.

4. Инструментарий идентификации пользователя на основе клавиатурной подписи при входе в информационную систему.

В результате создания математической модели и ее опытной апробации был создан программный комплекс аутентификации пользователя на основе клавиатурной подписи. Модуль основан на клиент-серверной архитектуре и состоит из двух частей: клиентской, собирающей биометрические данные при вводе учетных данных с АРМ пользователей, и серверной, производящей их анализ.

Полученные экспериментальные данные позволяют сделать вывод о достаточно точной аутентификации пользователя по его клавиатурной подписи. Полученный результат предоставляет возможность не только проведения аутентификации пользователя, но возможность идентификации личности злонамеренного нарушителя. Для этого требуется наличие базы подписей всех пользователей системы. Использование помимо логина и пароля некоторого идентификатора одинакового для всех пользователей позволяет создать такую базу данных. Инсайдер в этом случае встречается с еще более сложной задачей – не только войти в систему под чужими параметрами, но и скрыть свои. Очевидно, что намеренное грубое искажение своей подписи приведет к идентификации инсайдера как такового. Если же инсайдер будет пытаться войти незаметно в систему, то неизбежно будет набирать свою подпись достаточно устойчиво, что, по ранее полученным данным, отраженным в базе, позволит определить его личность. Схема работы программного комплекса представлена на рис. 2.

Как утверждалось выше, для снижения информационных рисков от деятельности инсайдеров важен комплексный подход. Поэтому внедрение отдельно взятого программного комплекса анализа клавиатурной подписи не даст полного эффекта без использования других средств защиты данных. Поэтому следует называть этот комплекс модулем системы защиты информации.

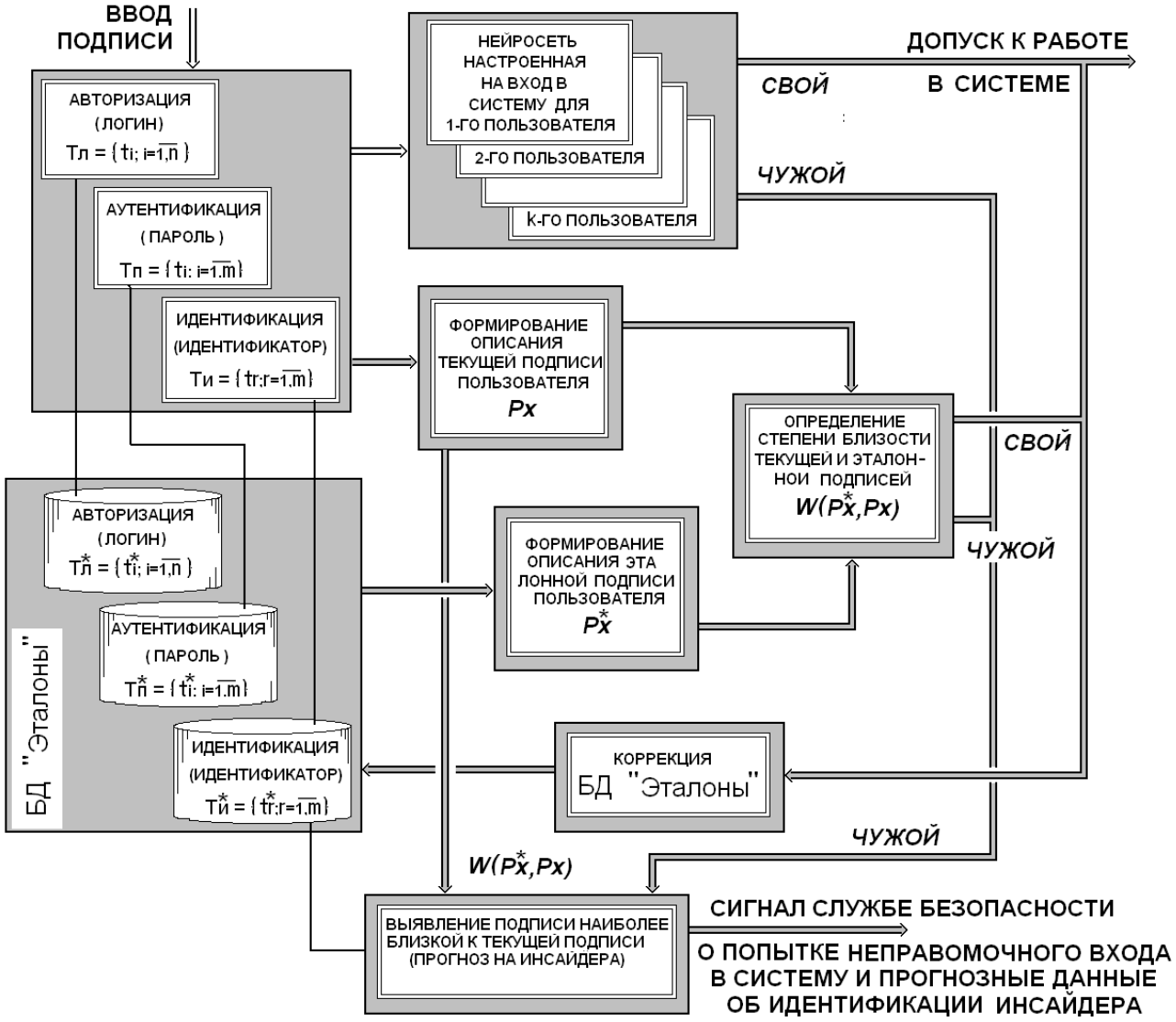

Рис. 2. – Схема работы модуля проверки клавиатурной подписи

5. Оценка экономической эффективности модуля проверки клавиатурной подписи.

Для оценки целесообразности внедрения модуля проверки клавиатурной подписи требуется определить количество инсайдеров, способных реализовать информационные угрозы, для предотвращения которых он предназначен.

Угрозы работы на чужом АРМ с помощью чужих учетных данных могут реализовывать три категории внутренних нарушителей:

1. Системные администраторы и офицеры безопасности – лица или обладающие легитимным доступом в защищаемые системы, либо способные без особых проблем получить такой доступ ввиду своих особых полномочий или статуса в компании.
2. Квалифицированные специалисты, способные тем или иным способом получить учетные данные зарегистрированных пользователей.
3. Высококвалифицированные специалисты, обладающие навыками использования методов «агентурной разведки» (подкуп, шантаж, убеждение, принуждение), которые могут быть внедрены в компанию.

Если предположить, что лояльность и осведомленность в ИБ всех сотрудников компании примерно одинакова, то долю обсуждаемых в исследовании типов злонамеренных инсайдеров от общего числа сотрудников можно вычислить как:

$$I = \frac{I_1 + I_2 + I_3}{E}; \qquad (12)$$

где I – искомое количество инсайдеров указанного типа;

I_1 – количество администраторов и офицеров безопасности в компании;

I_2 – количество квалифицированных сотрудников в области информационных технологий в компании;

I_3 – оценочное количество сотрудников, имеющих навыки «агентурной разведки;

E – общее число сотрудников.

В соответствии с проведенными в работе оценками, процент таких инсайдеров для компании, работающей в финансово-кредитном секторе, не превышает 15–20% от общего числа сотрудников. При этом следует учитывать, что речь идет о банковской организации, а не о компании, работающей в ИТ или

ИБ сферах, где доля потенциальных нарушителей будет гораздо больше.

Оценку экономической эффективности внедрения разработанного программного комплекса в работе рекомендовано проводить на основе оценки возврата инвестиций. В качестве полученной выгоды выступает оценка сокращаемых среднегодовых потерь, а в качестве вложенных средств – денежные средства, прямо или косвенно затраченные на механизмы безопасности и обеспечивающие сокращение потерь.

$$\begin{bmatrix} Возврат \\ инвестиций \end{bmatrix} = \begin{bmatrix} Уменьшение \\ среднегодовых \\ потерь \end{bmatrix} - \begin{bmatrix} Стоимость \\ защитных \\ мер \end{bmatrix}$$

Максимизация возврата инвестиций – одна из важнейших экономических задач информационной безопасности. Для определения того, насколько эффективно защитные меры сокращают потери, используется коэффициент возврата инвестиций (*ROI*), который определяется как отношение величины возврата инвестиций к стоимости реализации контрмер, которая включает в себя расходы на их планирование, проектирование, внедрение, эксплуатацию, мониторинг и совершенствование.

$$\begin{bmatrix} Коэффициент \\ возврата \\ инвестиций \end{bmatrix} \left(ROI \right) = \frac{\begin{bmatrix} Уменьшение \\ среднегодовых \\ потерь \end{bmatrix} - \begin{bmatrix} Стоимость \\ защитных \\ мер \end{bmatrix}}{\begin{bmatrix} Стоимость \\ защитных \\ мер \end{bmatrix}}$$

Для применения показателя *ROI* при оценке эффективности контрмер против инсайдеров на основе разработанного комплекса необходимо оценить затраты на внедрение модуля анализа клавиатурной подписи. Они складываются из следующих составляющих:

- первоначальная стоимость лицензий на программный модуль;
- стоимость оказания технической поддержки;
- стоимость серверного оборудования;
- стоимость трудозатрат технических специалистов на внедрение и администрирование системы;
- стоимость обучения администраторов, разработка части политики защиты от инсайдеров, использующих чужие учетные данные.

Ориентировочная стоимость внедрения модуля проверки цифровой подписи в финансовой компании на 1000 рабочих мест составляет 900 тыс. руб.

Средняя стоимость утечки конфиденциальной информации для российской компании финансово-кредитного сектора, имеющего 1000 АРМ, составит примерно 2,6 млн. долл. Как было показано выше, риск утечки информации подобного рода распространяется примерно на 15–20% всех пользователей в компании. Исходя из этих предположений, вероятные потери могут составить величину порядка 13,26 млн. руб. В этом случае ежегодный возврат инвестиций в модуль проверки клавиатурной подписи составит:

$$\Delta ALE = 13\ 260 \text{ тыс.} - 900 \text{ тыс.} = 12\ 360 \text{ тыс. руб.}$$

Коэффициент возврата инвестиций для модуля проверки клавиатурной подписи равен:

$$ROI = 12\ 360 \text{ тыс.} / 900 \text{ тыс.} \approx 13{,}7.$$

Исходя из полученной оценки коэффициента возврата инвестиций, следует сделать вывод о том, что внедрение разработанного в результате исследования модуля проверки клавиатурной подписи является экономически обоснованным.

Список работ, опубликованных по теме диссертации.

Статьи в журналах, определенных ВАК Минобрнауки России:

1. Гончаров П.И. Угроза безопасности информации от утечки инсайдерской информации и современные методы борьбы с ними / П.И. Гончаров // Вестник экономической интеграции. – 2013. – № 1–2. – С. 68–76. (0,81 п.л.);

2. Гончаров П.И. Оценка экономической эффективности внедрения дополнительной скрытой аутентификации, предназначенной для выявления сотрудников, работающих под чужими учетными данными / П.И. Гончаров // Вестник экономической интеграции. – 2013. – № 9 (66).– С. 21–36. (1,5 п.л.);

3. Гончаров П.И. Использование дополнительной скрытой аутентификации при вводе учётных данных для выявления фактов работы за чужим рабочим местом / П.И. Гончаров // Вестник экономической интеграции. – 2013. – № 9(66). – С. 120–131. (1,12 п.л.);

Статьи опубликованные в других научных изданиях:

4. Гончаров, П.И. Применение скрытых методов защиты информации для предотвращения утечек инсайдерской информации / П.И. Гончаров, П.А. Нащёкин // Научно-технический сборник ОАО «Концерн «Системпром». 2012. № 1(2) / Под ред. Ю.В. Бородакия. – М.: Изд-во «ОАО «Концерн «Системпром», 2012. – Инв. № Д-1673с от 2012 г. (0,75/0,35 п.л.);

5. Гончаров П.И. Развитие специальных систем и комплексов мониторинга и воздействия на общественное мнение в ГИС Интернет / П.И. Гончаров // Материалы Всероссийской научной конференции «Современные тенденции развития теории и практики управления в системах специального назначения». – Т. V – «Комплексная информационная безопасность систем специального назначения» / Под общ. ред. академика РАН, д-ра техн. наук, профессора Ю.В. Бородакия. – М.: ОАО «Концерн «Системпром», 2013. – С. 23-25. (0,1 п.л.).