ՀՀ ԳԻՏՈՒԹՅՈՒՆՆԵՐԻ ԱԶԳԱՅԻՆ ԱԿԱԴԵՄԻԱ
ԻՆՖՈՐՄԱՏԻԿԱՅԻ ԵՎ ԱՎՏՈՄԱՏԱՑՄԱՆ ՊՐՈԲԼԵՄՆԵՐԻ ԻՆՍՏԻՏՈՒՏ

Աբրահամյան Աշոտ Արտաշեսի

ՖԻՆԱՆՍԱԿԱՆ ՀԱՄԱԿԱՐԳԵՐԻ ՏԵՂԵԿԱՏՎԱԿԱՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ԿԱՌԱՎԱՐՄԱՆ ՊՐՈՑԵՍՆԵՐԻ ՈՐՈՇ ՄՈԴԵԼՆԵՐԻ ՄԱՍԻՆ

Ե.13.04 - «Հաշվողական մեքենաների, համալիրների, համակարգերի և ցանցերի մաթեմատիկական և ծրագրային ապահովում» մասնագիտությամբ տեխնիկական գիտությունների թեկնածուի գիտական աստիճանի հայցման ատենախոսության

ՍԵՂՄԱԳԻՐ

Երևան– 2014

НАЦИОНАЛЬНАЯ АКАДЕМИЯ НАУК АРМЕНИИ
ИНСТИТУТ ПРОБЛЕМ ИНФОРМАТИКИ И АВТОМАТИЗАЦИИ

Абраамян Ашот Арташесович

О НЕКОТОРЫХ МОДЕЛЯХ ПРОЦЕССОВ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ФИНАНСОВЫХ СИСТЕМ

АВТОРЕФЕРАТ

диссертации на соискание ученой степени кандидата технических наук по специальности

05.13.04 - «Математическое и программное обеспечение вычислительных машин, комплексов, систем и сетей»

Ереван – 2014

Ատենախոսության թեման հաստատվել է Հայ-Ռուսական (Սլավոնական) համալսարանում

Գիտակա նղեկավար՝ տեխ.գիտ.դոկտոր Վ.Ի. Թաիրյան

Պաշտոնական ընդդիմախոսներ՝ ֆիզ.մաթ.գիտ.դոկտոր Է.Մ. Պողոսյան
տեխ.գիտ.թեկնածու Գ.Ի. Մարգարով

Առաջատար կազմակերպություն՝ Հայաստանի ամերիկյան համալսարան

Պաշտպանությունը կայանալու է 2014թ. հունիսի 13-ին, ժամը 16:00-ին ՀՀ ԳԱԱ Ինֆորմատիկայի և ավտոմատացման պրոբլեմների ինստիտուտի 037 «Ինֆորմատիկա և հաշվողական համակարգեր» մասնագիտական խորհրդի նիստում, հետևյալ հասցեով՝ 0014, Երևան, Պ. Սևակի 1:
Ատենախոսությանը կարելի է ծանոթանալ ՀՀ ԳԱԱ ԻԱՊԻ-ի գրադարանում:
Սեղմագիրն առաքված է 2014թ. մայիսի13-ին:

037 մասնագիտական խորհրդի
Գիտական քարտուղար, ֆ.մ.գ.դ. Հ. Գ. Սարուխանյան

Тема диссертации утверждена в Российско-Армянском (Славянском) университете

Научный руководитель: д.т.н. В.И. Таирян

Официальные оппоненты: д.ф-м.н. Э.М. Погосян
к.т.н. Г.И. Маргаров

Ведущая организация: Американский университет Армении

Защита состоится 13-го июня 2014 г. в 16.00 часов на заседании специализированного совета 037 “Информатика и вычислительные системы” Института проблем информатики и автоматизации НАН РА по адресу: 0014, Ереван, ул. П. Севака 1.

С диссертацией можно ознакомиться в библиотеке ИПИА НАН РА.

Автореферат разослан13-го мая 2014 г.

Ученый секретарь специализированного
совета 037, д.ф.м.н. А.Г. Саруханян

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность проблемы. В современных условиях невозможно представить работу финансовой организации без использования информационных систем и технологий. При помощи локальных и глобальных сетей осуществляются электронные документообороты, электронные платежи и т.д. В последние годы электронные деньги приобретают все большее значение. Удобство и общедоступность электронных платежных системы интернет-банковских услуг привлекает огромное количество пользователей, и во многих странах банки и финансовые учреждения серьезно рассматривают полное прекращения денежного потока и перехода к форме безналичных платежей. Согласно исследованиям компании B2B International совместно с Лабораторией Касперского 98% опрошенных используют электронные платежи и интернет магазины. Естественно, эти тенденции привлекают нежелательное внимание преступных элементов. Резкий рост числа пользователей всех видов платежных систем привлек многочисленных киберпреступников, которые вкладывают постоянно растущие ресурсы в мошеннические схемы, с которыми они могут сначала получить доступ к финансовым данным пользователей, а затем к их деньгам. Хотя финансовые атаки являются одними из самых сложных и дорогостоящих видов атак, они, в тоже время, являются очень прибыльными, так как при успешном выполнении обеспечивают прямой доступ к деньгам жертв. Как только получен доступ к счету, остается только обналичить деньги. Программистам же занимающимся разработкой вредоносных программ или владельцам ботнета, предназначенного для запуска DDoS атаки или рассылки спама еще предстоит найти клиентов для покупки их услуг. В связи с этим возникает важнейший вопрос обеспечения информационной безопасности киберпространства финансовой системы, что на сегодняшний день является одной из самых актуальных проблем.

Согласно недавним исследованиям InfoWatch около 30% атак приходится на финансовые организации. По данным Национальной Ассоциации Инноваций и Развития Информационных Технологий (*НАИРИТ*), Института системного анализа Российской академии наук и Института социально-экономической модернизации, в России количество кибер-атак на финансовые системы за последний год увеличилось на 112%, что привело к убыткам равным 700 млрд. рублей. Похожая тенденция идет по всему миру. Число киберпреступлений, осуществленных сфере финансовых организаций растёт довольно быстро, в связи с чем выявляется потребность новых методов управления информационной безопасностью. Исследованию моделей управления информационной безопасностью и посвящена настоящая диссертационная работа.

Целью работы является исследование математических моделей целесообразных для управления информационной безопасностью финансовых систем.

Методы исследования. В работе исследовались теоретико-игровые методы моделирования, стеганографические методы скрытия информации и статистические методы анализа данных. Для численных экспериментов и наглядного представления методов моделирования разработана программа на языке C#.

Научная новизна.

- разработан метод управления информационной безопасностью с применением игр безопасности Штакельберга (приведена модель);

- предложен алгоритм вычисления оптимального распределения ресурсов информационной безопасности финансовых систем с использованием игр безопасности Штакельберга;
- применен новый подход обеспечения информационной безопасности банковских платежей с использованием специально обработанных звуковых файлов;
- проведен сравнительный анализ восприятия информационной безопасности в местных и иностранных банках Армении с использованием специального опросника.

Практическое значение. Разработанные в работе методы управления информационной безопасностью могут быть использованы в финансовых учреждениях для вычисления оптимальной стратегии распределения ресурсов для обеспечения защиты информации от несанкционированного доступа и кражи. А также, возможно повышение уровня безопасности банковских платежей при имплементировании описанного в работе специального метода обработки звуковых файлов.

Внедрение. Основные практические результаты работы использованы для модернизации системы безопасности АрмБизнесБанка, где используются в настоящее время. Соответствующий акт внедрения приложен к диссертации.

Положения, выносимые на защиту:

- утверждение целесообразности применения игр безопасности Штакельберга для управления информационной безопасностью;
- метод нахождения оптимальной стратегии распределения ресурсов обеспечения информационной безопасности в финансовых системах на основе игр безопасности Штакельберга;
- метод обеспечения информационной безопасности банковских платежей с применением специальной обработки звуковых файлов;

На основе результатов работы разработана программа для вычисления оптимальной стратегии защиты информации на языке C#.

Апробация работы. Основные результаты и материалы диссертационной работы обсуждались на семинарах кафедры математической кибернетики Российско-Армянского (Славянского) Университета (РАУ) и на научном семинаре Института проблем информатики и автоматизации. Результаты работы докладывались на годичной научной конференции РАУ, 2011 и на международном аспирантском форуме “Современная наука: тенденции развития, проблемы и перспективы" в РАУ, 2013.

Публикации

Основные результаты работы опубликованы в 3-х научных трудах, перечисленных в конце автореферата.

Структура и объем работы

Диссертация состоит из введения, трех глав, заключения и списка использованной литературы (90 наименований). Основной текст изложен на 105 страницах.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность и практическая значимость темы диссертационной работы, кратко изложено состояние предметной области, сформулированы цели и основные задачи исследования, выделены научные результаты, отличающиеся новизной, научные положения, выносимые на защиту, и практическая ценность полученных результатов.

Первая глава посвящена анализу существующих моделей управления информационной безопасностью и различных стратегий, которыми пользуются финансовые системы для обеспечения информационной безопасности.

Управление информационной безопасностью часто становится неэффективным в связи с недостаточным использованием математических методов. Теория игр является эффективным средством для моделирования разных задач информационной безопасности, так как позволяет моделировать проблемы, связанные с конкуренцией нескольких игроков, имеющих противоречивые цели. Следовательно, теория игр может обеспечить математические основы для анализа и моделирования проблем информационной безопасности.

Исследования в области применения теоретико-игровых моделей для обеспечения информационной безопасности в последние годы становятся все более популярными. Теоретико-игровые модели успешно используются для моделирования управления сетевой безопасностью.

Для моделирования используются следующие разновидности игр:

- Игры с полной информацией, где каждый игрок осведомлен о всех стратегиях и возможных выигрышах других игроков. Если по крайней мере один из игроков не владеет информацией о стратегии или выигрыша хотя бы одного другого игрока, то получается игра с неполной информацией.
- Байесовские игры, в которых информация о стратегиях и выигрышах других игроков является неполной, и отдельный игрок в начале игры определяет “тип” других игроков. Название игры определено использованием байесовского анализа прогнозирования результатов.
- Статические игры – игры с одним периодом, где игроки выбирают стратегию одновременно, т.е. без учета стратегий других игроков.
- Динамические игры – игры с множественными стадиями, в каждой из которых игроки могут пересмотреть собственные стратегии.
- Стохастические игры включают в себя вероятностные переходы через несколько состояний системы. Игра ведется как последовательность состояний. Игра начинается из первоначального состояния – игроки выбирают стратегии и получают выигрыши, зависящие от текущего состояния игры, а затем игра переходит в новое состояние с вероятностью, которая зависит от действий игроков и текущего состояния.

Вышеприведенные игры используются для моделирования управления информационной безопасностью при следующих ситуациях:

- Информационная война;
- атака, приводящая к отказу в обслуживании (Denial of Service – DoS);
- взаимодействие хакера и системы обнаружений вторжений (IDS);
- взаимодействие хакера и системного администратора;

В работах армянских ученых представлен эффективный метод динамического анализа безопасности систем и их защиты путем разработки оптимальных стратегий.

Выделяется класс проблем, в котором пространство возможных решений может быть определено комбинаторным деревом игры (SSGT – Space of Solutions represented by Game Trees) и разрабатываются алгоритмы формирования стратегии типа – промежуточные цели в первую очередь (IGAF – Intermediate Goals At First). SSGT это широкий класс проблем со следующими ограничениями:

- Имеются группы взаимодействующих участников, выполняющих действия в определенные моменты времени.
- Действия групп задаются конечными множествами.
- Заранее обозначены выигрыши для всех участников.
- Ситуации, в которых группы действуют и которые трансформируются в результате этих действий, имеют адекватные модели.

Многие проблемы безопасности принадлежат SSGT классу. Проблему нахождения оптимального распределения ресурсов информационной безопасности финансовых систем также может быть сведена к классу SSGT.

Игра Штакельберга это игра двух лиц (лидера и ведомого), где лидер осуществляет смешанную стратегию первым, а ведомый после наблюдения реагирует конкретной (строгой) стратегией, максимизируя свой выигрыш.

Игры безопасности Штакельберга успешно используются для моделирования управления физической безопасностью. Эта модель используется для расчетов оптимальной стратегии защиты в международном аэропорту Лос-Анжелеса (LAX).

Теория игр эффективна при моделировании процессов управления информационной безопасностью финансовых систем, из-за особенностей специфики возникающих проблем:

- политика информационной безопасности финансовых организаций является общедоступным документом;
- методы и средства обеспечения информационной безопасности должны соответствовать определенным стандартам, которые, в свою очередь, представляют из себя общедоступную информацию;
- конкретные технологии, которые используются в определенной организации являются общеизвестными, и, часто вендоры конкретных технологий или сами финансовые организации заявляют о применении тех или иных технологий для рекламных целей.

Еще одной важной задачей для финансовых систем, в частности для банков, является обеспечение информационной безопасности электронных платежей. Специфической чертой электронных банковских систем является специальная форма обмена электронными данными - электронных платежей, без которых ни один современный банк не может существовать.

Обмен электронными данными (ОЭД) — это межкомпьютерный обмен деловыми, коммерческими, финансовыми электронными документами. Например, заказами, платежными инструкциями, контрактными предложениями, накладными, квитанциями и т.п.

Частным случаем ОЭД являются электронные платежи - обмен финансовыми документами между клиентами и банками, между банками и другими финансовыми и коммерческими организациями.

Для определения общих проблем защиты систем ОЭД рассмотрим прохождение документа при ОЭД. Можно выделить три основных этапа:

- подготовка документа к отправке;
- передача документа по каналу связи;
- прием документа и его обратное преобразование.

С точки зрения защиты в системах ОЭД существуют следующие уязвимые места:

1. Пересылка платежных и других сообщений между банками или между банком и клиентом;
2. Обработка информации внутри организаций отправителя и получателя;
3. Доступ клиента к средствам, аккумулированным на счете.

Одно из наиболее уязвимых мест в системе ОЭД - пересылка платежных и других сообщений между банками, или между банком и банкоматом, или между банком и клиентом. При пересылке платежных и других сообщений возникают следующие проблемы:

- внутренние системы организаций Получателя и Отправителя должны быть приспособлены к получению/отправке электронных документов и обеспечивать необходимую защиту при их обработке внутри организации (защита оконечных систем);
- взаимодействие Получателя и Отправителя документа осуществляется опосредованно - через канал связи. Это порождает три типа проблем: взаимного опознавания абонентов (проблема установления аутентификации при установлении соединения); защиты документов, передаваемых по каналам связи (обеспечение целостности и конфиденциальности документов); защиты самого процесса обмена документами (проблема доказательства отправления/доставки документа);
- в общем случае Отправитель и Получатель документа принадлежат к различным организациям и друг от друга независимы. Этот факт порождает проблему недоверия - будут ли предприняты необходимые меры по данному документу (обеспечение исполнения документа).

С технической точки зрения эти проблемы решаются с помощью нескольких механизмов, отвечающих за обеспечение адекватной безопасности электронных банковских систем. Работа большинства этих механизмов обеспечивается службами сети с расширенным набором услуг (Value-Added Network, VAN). Службы, реализующие ОЭД, должны выполнять следующие функции:

- обеспечить защиту от случайных и умышленных ошибок;
- обеспечить адаптацию к частым изменениям количества пользователей, типов оборудования, способов доступа, объемов трафика, топологии;
- поддерживать различные типы аппаратного и программного обеспечения, поставляемого различными производителями;
- осуществлять управление и поддержку сети для обеспечения непрерывности работы и быстрой диагностики нарушений;
- реализовывать полный спектр прикладных задач ОЭД, включая электронную почту;
- реализовывать максимально возможное число требований партнеров;
- включать службы резервного копирования и восстановления после аварий.

В системах ОЭД должны быть реализованы следующие механизмы, обеспечивающие реализацию функций защиты на отдельных узлах системы ОЭД и на уровне протоколов высокого уровня:

- равноправная аутентификация абонентов;
- невозможность отказа от авторства сообщения/приема сообщения;
- контроль целостности сообщения;
- обеспечение конфиденциальности сообщения;
- управление доступом на конечных системах;
- гарантии доставки сообщения;
- регистрация последовательности сообщений;
- контроль целостности последовательности сообщений;
- обеспечение конфиденциальности потока сообщений.

Полнота решения рассмотренных выше проблем сильно зависит от правильного выбора системы шифрования. Система шифрования (или криптосистема) представляет собой совокупность алгоритмов шифрования и методов распространения ключей. Правильный выбор системы шифрования помогает:

- скрыть содержание документа от посторонних лиц (обеспечение конфиденциальности документа) путем шифрования его содержимого;
- обеспечить совместное использование документа группой пользователей системы ОЭД путем криптографического разделения информации и соответствующего протокола распределения ключей. При этом для лиц, не входящих в группу, документ недоступен;
- своевременно обнаружить искажение, подделку документа (обеспечение целостности документа) путем введения криптографического контрольного признака (имитовставки);
- удостовериться в том, что абонент, с которым происходит взаимодействие в сети является именно тем, за кого он себя выдает (аутентификация абонента/источника данных).

Следует отметить, что при защите систем ОЭД большую роль играет не столько шифрование документа, сколько обеспечение его целостности и аутентификация абонентов (источника данных) при проведении сеанса связи. Поэтому механизмы шифрования в таких системах играют обычно вспомогательную роль.

Надежность всей криптосистемы в целом во многом зависит от механизмов рассылки (распределения) ключей между участниками взаимодействия. Проблема рассылки ключей в настоящее время не имеет общих решений. В каждом конкретном случае она должна решаться с учетом особенностей функционирования всей защищаемой АСОИБ.

Жестким ограничением на реализацию мер по защите информации накладываются требования уже существующих стандартов ОЭД. Поскольку абсолютно неуязвимых систем не бывает, каждая организация должна самостоятельно решать вопрос об уровне защищенности собственной системы ОЭД: что лучше - затратить дополнительные средства на организацию и поддержание защиты или сэкономить и работать в условиях постоянного риска.

Необходимость поддержки электронных банковских услуг с помощью специальных банковских и других сетей, а также с помощью национальных клиринговых систем, радикально изменила отношения между банками и их клиентами. Только за последнее десятилетие стали доступны, а сейчас используются повсеместно, различные клиринговые системы, осуществляющие весь спектр банковских операций. Данные и инструкции вводятся, распределяются и обрабатываются в них в режиме реального времени.

Безопасность операций с наличностью и расчетных услуг требует принятия тех же общих мер, которые необходимы для защиты любой электронной финансовой услуги. Особое внимание необходимо обратить на защиту терминалов, подключенных к системам электронных платежей.

Если банк выполняет операции повышенного риска, то реализуемые процедуры обеспечения безопасности должны включать парольную защиту, многоуровневую авторизацию пользователей, контроль операций, ведение системного журнала. Также следует осуществлять разграничение доступа пользователей к терминалам и другим внешним устройствам, которые должны быть защищены физически. Для обеспечения безопасности данных, передаваемых по линиям связи, необходимо использовать криптографические методы.

Система безопасности центральной АСОИБ должна включать многоуровневый контроль доступа к периферийным устройствам и центральной базе данных.

Если операции повышенного риска не выполняются, некоторые требования к безопасности могут быть ослаблены или ликвидированы совсем. Задачи по обеспечению безопасности определяются для каждого конкретного случая индивидуально в процессе анализа риска.

Несмотря на технологическую насыщенность сферы информационной безопасности, организации часто сталкиваются с большими проблемами по причине человеческого фактора, что на сегодняшний день является одним из самых важных в этой сфере.

Причины, способствующие ошибочным действиям человека, можно объединить в несколько групп:

- недостатки информационного обеспечения или их отсутствие (специальные обработчики таких ситуаций в программном обеспечении, наглядные материалы и инструкции). Особенно сильно эта проблема проявляется в экстремальных ситуациях и в условиях дефицита времени на принятие решения;
- ошибки, вызванные воздействием внешних факторов (отвлечение внимания от возникшей проблемы);
- ошибки, вызванные физическим и психологическим состоянием и свойствами человека (внезапный стресс при общей монотонной работе, эмоциональная напряжённость, импульсивность или, наоборот, подавление реакции на проблему);
- ограниченность ресурсов поддержки и исполнения принятого решения;
- отсутствие учёта человеческого фактора в списке возможных причин инцидента.

В последнее время проводится достаточно много исследований, направленных на минимизацию угроз, связанных с человеческим фактором.

Во второй главе дано описание игр безопасности Штакельберга и байесовских игр безопасности Штакельберга. Приведено обоснование целесообразности их применения в управлении информационной безопасностью финансовых систем. Приведены числовые эксперименты и разработана программа для вычисления оптимальной стратегии для защиты информации.

Игра Штакельберга это игра двух лиц (лидера и ведомого), где лидер осуществляет смешанную стратегию первым, а ведомый после наблюдения реагирует конкретной (строгой) стратегией, максимизируя свой выигрыш.

В общей форме игры Штакельберга, смешанную стратегию лидера можно представить в виде N-мерного вектора $\mathbf{L}\epsilon R^n$. Ожидаемые выигрыши лидера и ведомого - линейные комбинации вектора **L** с весовыми коэффициентами, зависящими от выбора ведомого. По заданной стратегии лидера **L**, ведомый максимизирует ожидаемый выигрыш выбирая одну из чистых стратегий из набора F. Для каждой чистой стратегии f, выбранной ведомым, выигрыш лидера будет $\boldsymbol{\mu}_f^T\mathbf{L}+\mu_{f,0}$, а выигрыш ведомого $\mathbf{v}_f^T\mathbf{L}+\nu_{f,0}$, где μ_f и $\mathbf{v}_f$ векторы из R^n, а $\mu_{f,0}$, $\nu_{f,0}$ принадлежат R. Обозначим через U и V матрицы выигрышей лидера и ведомого соответственно. Таким образом:

$$U=\begin{pmatrix}\mu_{1,0} \cdots & \mu_{F,0}\\ \boldsymbol{\mu}_1 \cdots & \boldsymbol{\mu}_F\end{pmatrix},\ V=\begin{pmatrix}\nu_{1,0} \cdots & \nu_{F,0}\\ \mathbf{v}_1 \cdots & \mathbf{v}_F\end{pmatrix}.$$

Байесовское расширение игр Штакельберга дает возможность учитывать множественные типы ведомых. Каждый тип имеет собственную матрицу выигрышей. Это расширение дает возможность моделирования для разных типов злоумышленников во многих аспектах.

Формально, байесовская игра Штакельберга это игра Штакельберга между лидером и ведомым, чей тип случайно выбран из множества типов ведомых {1, 2, …, I}. Каждому типу $1 \le i \le I$ сопоставлена вероятность появления p^i, а также матрицы выигрышей U^i и V^i для лидера и ведомого соответственно. Лидер применяет свою смешанную стратегию зная распределение всех возможных типов ведомых, но не зная конкретно тип ведомого, который принимает участие в игре. Ведомый знает свой собственный тип i и действует оптимальным образом согласно матрице выигрышей V^i.

Ожидаемые выигрыши можно определить при помощи смешанной стратегии лидера **L** и вектора конкретных стратегий ведомого **f**= (f^1, f^2, …,f^I) , где f^i – конкретная стратегия ведомого типа i. Таким образом, для ведомого типа i, ожидаемый выигрыш $v^i(\mathbf{L},f^i)=(\nu^i_{f^i})^T\boldsymbol{L} + \nu_{f^i,0}$. Ожидаемый выигрыш лидера $u(\mathbf{L},\mathbf{F})= \sum_{i=1}^{I} p^i u^i(\boldsymbol{L}, f^i)$, где $u^i(\boldsymbol{L}, f^i)= (\boldsymbol{\mu}^i_{f^i})^T\boldsymbol{L} + \mu_{f^i,0}$ожидаемый выигрыш лидера против ведомого типа i.

В работе рассматривается сильное равновесие Штакельберга. В байесовских играх Штакельберга определяется конкретная стратегия каждого типа ведомого при данной смешанной стратегии лидера **L**. Определим вектор функций **g**=(g^1,…, g^I), где g^i сопоставляет смешанную стратегию лидера с конкретной стратегией ведомого типа i. Пусть **g(L)** вектор действий ведомого по данной **L** согласно **g**, т.е. **g(L)**=(g^1(**L**),…, g^I(**L**)). Это позволяет формально определить сильное равновесие Штакельберга.

Определение. Для данной байесовской игры Штакельберга с матрицами выигрышей (U^1,V^1),…,(U^I, V^I) и распределением типов **p**, пара стратегий (**L, g**) является сильным равновесием Штакельберга тогда и только тогда, когда:

1. Лидер действует наилучшим образом:
   $u(\mathbf{L},\mathbf{g}(\mathbf{L}))\ge u(\mathbf{L}', \mathbf{g}(\mathbf{L}')), \forall \mathbf{L}'$
2. Ведомый действует наилучшим образом:
   $v^i(\mathbf{L}, g^i(\mathbf{L}))\ge v^i(\mathbf{L}, f), \forall\ 1\le i\le I, \forall 1\le f\le F$
3. Ведомый выбирает наилучший ответ стратегии лидера:
   $u^i(\mathbf{L}, g^i(\mathbf{L}))\ge u^i(\mathbf{L}, f), \forall\ 1\le i\le I.$

Стратегия лидера, которая удовлетворяет сильному равновесию Штакельберга, является оптимальной, т.к. она максимизирует ожидаемый выигрыш лидера, допуская, что ведомый действовал наилучшим образом.

Проблема определения оптимальной стратегии лидера **L*** эквивалентна нахождению смешанной стратегии лидера **L**и конкретной стратегии ведомого **f=g(L)**, которые удовлетворяют трем условиям сильного равновесия Штакельберга. Математически стратегия лидера **L*** может быть определена в результате решения следующей задачи максимизации:

$$(\mathbf{L}^*, \mathbf{f}^*)=\max_{\boldsymbol{x},\boldsymbol{j}}\{u(\boldsymbol{x},\boldsymbol{f})|\vartheta^i(\boldsymbol{x},f^i)\ge\vartheta^i(\boldsymbol{x},f'),\forall 1\le f'\le F\}.$$

Данную задачу максимизации можно решить используя методы линейного программирования. Идея состоит в переборе всех конкретных стратегий ведомого $\mathbf{f}\in\{1,\dots,F\}^I$.

Для каждого **f**, оптимальная стратегия лидера **L*(f)** определяется решением задачи линейного программирования:

$$\max_{L} u(\boldsymbol{L}, \boldsymbol{F})$$

$$\text{т. ч. } A\boldsymbol{F} \le \boldsymbol{b}, \boldsymbol{F} \ge 0$$

$\vartheta^i(\boldsymbol{L}, f^i) \ge \vartheta^i(\boldsymbol{L}, f'), \forall 1 \le i \le I, \forall 1 \le f' \le F$, где **f**лучший ответ ведомого.

Оптимальное решение одной из задач линейного программирования, в которой $u(\boldsymbol{L}, \boldsymbol{F})$(ожидаемый выигрыш лидера)имеет наибольшое значение определяет оптимальную стратегию лидера **L*.**

Так как ведомые разных типов независимы друг от друга, то наибольшее число возможных комбинаций лучших ответов ведомого равно F^I, где I количество типов ведомых. Таким образом, приведенный выше метод состоит из F^Iлинейных программ, что, естественно, ведет к экспоненциальному росту времени расчетов при увеличении количества типов ведомых.

В общем случае, проблема нахождения оптимальной стратегии для лидера в байесовской игре Штакельберга является NP-полной. Но, несмотря на это, некоторые недавние исследования привели к определенным практическим результатам. Например, метод DOBSS[1] является эффективным методом решения байесовской игры Штакельберга. Метод заключается в преобразовании множество задач линейного программирования в одну задачу целочисленного программирования:

$$\max_{\boldsymbol{L},\boldsymbol{u},\boldsymbol{v},\boldsymbol{q}^1,\ldots,\boldsymbol{q}^I} \sum_{i=1}^{I} p^i u^i$$

$$\text{т. ч. } A\boldsymbol{L} \le \boldsymbol{b}, \boldsymbol{F} \ge 0$$

$$\sum_{f=1}^{F} q_f^i = 1, \forall i$$

$$q_f^i \in \{0,1\}. \forall i, \forall f$$

$$u^i \le u^i(\boldsymbol{L}, f) + \left(1 - q_f^i\right)M, \qquad \forall i, \forall f$$

$$0 \le \vartheta^i - \vartheta^i(\boldsymbol{L}, f) \le \left(1 - q_f^i\right)M, \qquad \forall i, \forall f$$

Идея метода состоит в представлении чистой стратегии каждого типа ведомого в бинарный вектор $\boldsymbol{q^i} = \left(q_1^i, \ldots, q_F^i\right)$. В частности, $q_f^i = 1$, если ведомый типа i выбрал стратегию f, $q_f^i = 0$ в противном случае. Очевидно, что $\sum_{f=1}^{F} q_f^i = 1$, т.к. только один q_f^i может быть равным 1. M – бесконечно большая константа. Переменная u^i – ожидаемый выигрыш лидера против ведомого типа i, который определяется как $u^i(\boldsymbol{L}, f)$, когда ведомый выбирает стратегию f (т.е. $q_f^i = 1$). ϑ^i- ожидаемый выигрыш ведомого типа i, т.е. $\max_{1 \le f \le F} \vartheta^i(\boldsymbol{L}, f)$.

[1]P. Paruchuri, J. P. Pearce, J. Marecki, M. Tambe, F. Ordonez, and S. Kraus, "Playing Games with Security: An Efficient Exact Algorithm for Bayesian Stackelberg Games," in *Proc. of The 7th InternationalConference on Autonomous Agents and Multiagent Systems (AAMAS)*,2008.

Приведенный метод может быть использован для моделирования проблем информационной безопасности. В частности, в роли лидера может выступать служба информационной безопасности (или организация), а в роли ведомого хакер (или организованная преступная группировка). Лидер действует первым, применяя разные методы информационной безопасности для защиты информационного пространства своей организации. Ведомый имеет возможность исследовать текущее состояние информационной сети и делать ответный ход конкретной стратегией в зависимости от результатов исследований. Можно смоделировать множество типов ведомых, т.к. существует много разных видов атак на информационные системы. Служба информационной безопасности осведомлена о статистическом распределении известных атак.

Служба информационной безопасности организации считается лидером исходя из следующих соображений:

1. Во многих организациях политика информационной безопасности является общедоступным документом;
2. Потенциальные инструменты и меры безопасности являются стандартными и известными. Злоумышленники могут изучить систему безопасности, которая внедрена в данной организации в результате исследования состояния информационной системы. Более того, такая информация часто общедоступна через компании, которые разрабатывают системы безопасности или через, собственно, эту организацию.
3. Каждая система безопасности имеет свои недостатки и уязвимые места, что дает возможность злоумышленникам выбрать наилучший способ атаки.

Игры безопасности Штакельберга можно успешно применять для моделирования управления информационной безопасностью в финансовых организациях. Для простоты описания применения данной модели рассмотрим банк, как пример финансовой организации. В этом случае отдел информационной безопасности банка является лидером, а злоумышленники или хакеры - ведомыми.

У банка имеются множество активов, которые должны быть защищены. Отдел информационной безопасности применяет разные методы безопасности для защиты этих активов. Эти методы четко указаны в политике информационной безопасности банка и в разработанных стандартах государственного регулирования. Все эти документы открыты для общественности. Более того, общеизвестными являются и конкретные технологии, которые используют различные банки. Эти обстоятельства дают возможность злоумышленникам наблюдать за состоянием защищенности конкретного банка. После тщательного исследования банковской сети хакеры выбирают оптимальную стратегию атаки, которая зависит от стратегии лидера.

На основе статистики атак на банковские системы, отдел информационной безопасности получает сведения о типах атак и вероятностях их осуществления. Имея эту информацию, банк должен выбрать оптимальную стратегию для принятия мер защиты. Необходимо учитывать то, что злоумышленники имеют возможность исследовать стратегию лидера, и ответить наилучшим образом, максимизируя свой результат. Оптимальную стратегию лидера можно определить вычислением сильного равновесия Штакельберга в игре безопасности.

На основе предложенного метода проведены конкретные расчеты применительно к банковскому веб-приложению. В числовой эксперимент включены наиболее распространенные уязвимости и противодействия.

Таблица 2.1 Стратегии ведомого и лидера

Уязвимость	**Противодействие**
SQL injection (SQLi)	Escaping routines (ER)
Cross-Site Scripting (XSS)	Escaping routines (ER)
Broken Authentication and Session Management (BASM)	Session Security (SS)
Insecure Direct Object Reference (IDOR)	Access Control (AC)
Cross-Site Request Forgery (CSFR)	CSFR Guard (CSFRG)
Security Misconfiguration (SM)	Environment Securing (ES)
Failure to Restrict URL Access (FRUA)	Access Control (AC)
Insufficient Transport Layer Protection (ITLP)	Secure Sockets Layer (SSL)

Противодействия являются стратегиями лидера, а уязвимости стратегиями ведомого. Построенная матрица выигрышей имеет следующий вид. Здесь учитывается и возможное отсутствие атаки (бездействие ведомого - NA):

Таблица 2.2 Матрица выигрышей

	SQLi	XSS	BASM	IDOR	CSRF	SM	FRUA	ITLP	NA
ER	7, -1	7, -1	-5, 2	-2, 0.5	-5, 2	-4, 2	-2, 0.5	-5, 1	-1, 0
SS	-6, 3	-6, 3	2, -2	-3, 0.5	-6, 2	-5, 2	-3, 0.5	-6, 1	-2, 0
AC	-6, 3	-6, 3	-6, 2	-2, -0.5	-6, 2	-5, 2	-2, -0.5	-6, 1	-2, 0
CSRFG	-6, 3	-6, 3	-6, 2	-3, 0.5	0, -2	-5, 2	-3, 0.5	-6, 1	-2, 0
ES	-6, 3	-6, 3	-6, 2	-3, 0.5	-6, 2	3, -1	-3, 0.5	-6, 1	-2, 0
SSL	-6, 3	-6, 3	-6, 2	-3, 0.5	-6, 2	-5, 2	-3, 0.5	0, -3	-2, 0

Рассмотрим случай, когда имеются два типа ведомых A и B, у которых одинаковые матрицы выигрышей, но различные множества стратегий. Ведомый типа A может выбрать любую стратегию, кроме бездействия (NA), а ведомый типа B может выбрать любую стратегию кроме CSRF и ITLP. Расчеты проведены при следующих начальных условиях:

- вероятность появления ведомого A- 0.4;
- вероятность появления ведомого B - 0.6.

Результаты расчетов:

- максимальный ожидаемый выигрыш лидера=-0.09499999999999931
- максимальный ожидаемый выигрыш ведомого A=1.3076923076923077
- максимальный ожидаемый выигрыш ведомого B=1.1
- чистая стратегия ведомого A: XSS
- чистая стратегия ведомого B: SQLi
- смешанная стратегия лидера:
  - ER: 0.4542307692307692
  - SS: 0.20423076923076922

- AC: 0.0
- CSRFG: 0.06923076923076923
- ES: 0.2723076923076923
- SSL: 0.0

Результаты совпадают с общей статистикой атак на веб-приложения, где атаки SQLi и XSSзанимают лидирующие позиции.

Третья глава посвящена описанию одного метода обеспечения информационной безопасности банковских платежей на основе стеганографии и проведен сравнительный анализ восприятия информационной безопасности со стороны сотрудников местных и иностранных банков, работающих в Армении.

Специфической чертой электронных банковских систем является специальная форма обмена электронными данными - электронных платежей, без которых ни один современный банк не может существовать.

Обмен электронными данными (ОЭД) — это межкомпьютерный обмен деловыми, коммерческими, финансовыми электронными документами. Например, заказами, платежными инструкциями, контрактными предложениями, накладными, квитанциями и т.п.

Частным случаем ОЭД являются электронные платежи - обмен финансовыми документами между клиентами и банками, между банками и другими финансовыми и коммерческими организациями.

Естественно, у банков возникает задача обеспечения информационной безопасности ОЭД. Для защиты электронных банковских платежей передается звуковой файл с добавлением идентификаторов отправителя, получателя, суммы и времени платежа методом стеганографии.

Идея подхода заключается в том, что музыкальное произведение рассматривается как совокупность трэков (с технической точки зрения), в которые соответствующим образом встраивается передаваемое сообщение. Музыкальное произведение в оцифрованном виде (wave, .mp3, .wma и др.) преобразовывается в 2^k-битовый вектор. Передаваемое сообщение (текст, музыка, изображение) также преобразовывается в 2^k-битовый вектор. Одним из обратимых преобразований векторам ставится в соответствие третий вектор. Ключом является вышеуказанное обратимое преобразование, при знании которого получатель выделяет из принятого вектора переданное ему сообщение.

Краткое описание метода имеет следующий вид:

- исходное сообщение и стеганографический контейнер приводятся к форме цифровых сигналов;
- полученные цифровые сигналы преобразовываются в 2^k-битовые вектора;
- осуществляется процесс стеганографической «обработки» - вектор сообщения «встраивается» в вектор контейнера так, чтобы размер контейнера не изменился.

Таким образом обеспечиваются решения следующих проблем при выполнении банковских платежей:

- равноправная аутентификация абонентов;
- невозможность отказа от авторства сообщения/приема сообщения;
- контроль целостности сообщения;
- обеспечение конфиденциальности сообщения;
- управление доступом на оконечных системах;
- обеспечение конфиденциальности потока сообщений.

Принимая во внимание факт, что на сегодняшний день одним из наиболее слабых сторон информационной безопасности кроется в человеческом факторе, выявляется потребность исследования состояния этой сферы.

Для исследования был имплементирован опрос, касающийся восприятия информационной безопасности среди сотрудников банка. Опросник составлен в государственном университете Нью-Йорка, Албани и состоит из 70 вопросов. В опросе приняли участие 102 сотрудника разных банков, из которых 62 были работниками местных банков. Опрошенные работники занимали следующие позиции в своих банках:

- агенты;
- работникиотдела ИТ;
- работникиотделабэк-офис;
- работникикредитногоотдела;
- менеджеры;
- бухгалтеры.

Для проверки равенства средних значений был применен тест Стьюдента. Приведем результаты анализа:

- В местных банках больше надеются на интуицию и опыт, чем следуют указаниям.
- В местных банках для получения желаемого результата работники могут отходить от правил.
- В иностранных банках большое внимание уделяют инструкциям.
- В местных банках думают, что важнее получить результат, чем делать все по правилам.

По остальным критериям средние значения ответов работников местных и иностранных банков разнятся незначительно.

Из результатов можно сделать вывод, что в местных банках основная проблема связана с дисциплиной и строгим соблюдением инструкций.

Во время анализа были выдвинуты следующие гипотезы:

- Гипотеза 1: Существует связь между восприятием уязвимостей ИБ и стремлением соблюдения правил ИБ.
- Гипотеза 2: Существует связь между восприятием уязвимостей ИБ и соблюдением правил ИБ.

На основе корреляционного анализа с применением критерия Пирсона был получен следующий результат: мы можем быть на 95% уверены, что между восприятием уязвимостей ИБ и стремлением соблюдения правил ИБ существует негативная корреляция.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ ДИССЕРТАЦИОННОЙ РАБОТЫ

1. Построена теоретико-игровая модель управления информационной безопасностью с применением игр безопасности Штакельберга и ее байесовским расширением [1].
2. Разработан метод управления информационной безопасностью финансовых систем при использовании байесовских игр безопасности Штакельберга [1,2].
3. Построена модель для нахождения оптимального распределения ресурсов информационной безопасности при множественных типах атак на информационную систему финансовых учреждений [2].
4. Разработан новый подход для обеспечения информационной безопасности банковских платежей с применением специальной обработки звуковых файлов [3].
5. На основе результатов исследования разработан программный комплекс на языке C# для расчетов оптимальной стратегии защиты информационной системы финансовых организаций. Проведен сравнительный анализ восприятия информационной безопасности в местных и иностранных банках, работающих в Армении.

СПИСОК РАБОТ ОПУБЛИКОВАННЫХ ПО ТЕМЕ ДИССЕРТАЦИИ

1. Абраамян А.А. Управление информационной безопасностью с использованием игр безопасности Штакельберга. Сборник трудов X международной научно-практической конференции Европейская наука XXI века – 2014, сс. 74-82.
2. A. Abrahamyan. *Stackelberg Security Games for Information Security Management of Financial Systems*. Mathematical Problems of Computer Science41,pp. 74-80, 2014
3. Таирян С.В., Абраамян А.А. Об одном подходе к обеспечению информационной безопасности банковских платежей. Труды шестой годичной научной конференции РАУ, СС. 59-61, 2012.

Ամփոփում

Աբրահամյան Աշոտ Արտաշեսի

Ֆինանսական համակարգերի տեղեկատվական անվտանգության կառավարման պրոցեսների որոշ մոդելների մասին

Ատենախոսական աշխատանքը նվիրված է ֆինանսական համակարգերի տեղեկատվական անվտանգության կառավարման պրոցեսների մոդելավորմանը: Աշխատանքում հետազոտվում է տեղեկատվական անվտանգության կառավարման խաղային մոդել՝ հիմնված Շտակելբերգի անվտանգության խաղերի վրա: Առաջարկվում է նաև ձայնային ֆայլերի հատուկ մշակման հիման վրա բանկային էլեկտրոնային վճարումների անվտանգության ապահովման մեթոդ: Կատարվել է տեղեկատվական անվտանգության ընկալման համեմատական վերլուծություն՝ տեղական և արտասահմանյան առևտրային բանկերում:

Աշխատանքի արդիականությունը
Ներկայիս պայմաններում հնարավոր չէ պատկերացնել ֆինանսական կազմակերպության աշխատանքը առանց տեղեկատվական տեխնոլոգիաների օգտագործման: Լոկալ և գլոբալ ցանցերի միջոցով իրականացվում են էլեկտրոնային փաստաթղթաշրջանառություն, էլեկտրոնային վճարումներ և այլն: Վերջին տարիների ընթացքում էլեկտրոնային հաշիվները ձեռք են բերում առավել մեծ կարևորություն: Էլեկտրոնային վճարային համակարգերի հարմարավետությունը և հանրամատչելիությունը գրավում է մեծ քանակությամբ օգտվողների, և շատ երկրներում բանկերը և ֆինանսական հիմնարկությունները բավականին լրջորեն ուսումնասիրում են բացարձակ անկանխիկ վճարումների անցնելու հնարավորությունները: Համաձայն B2B International ընկերության կատարած հետազոտությունների՝ հարցվածների 98%-ը օգտվում է էլեկտրոնային վճարման համակարգերից և ինտերնետ-խանութներից: Բնական է, որ այսպիսի տենդենցները գրավում են ոչ այդքան ցանկալի ուշադրություն: Էլեկտրոնային վճարային համակարգերի օգտագործողների կտրուկ աճը գրավել է բազմաթիվ կիբեր-հանցագործների, որոնք ավելի մեծ ռեսուրսներ են ներդնում խարդախ ծրագրերի մեջ՝ ցանկանալով մուտք գործել օտար հաշիվներ և հասնել պահված գումարներին: Այս ամենը հաշվի առնելով, առաջանում է անհրաժեշտություն նոր մեթոդների մշակման և կիրառման ֆինանսական համակարգերի տեղեկատվական անվտանգության կառավարման համար:

Հետազոտության արդյունքների կիրառական նշանակությունը
Աշխատանքում մշակված տեղեկատվական անվտանգության կառավարման մեթոդները կարող են օգտագործվել ֆինանսական համակարգերում տեղեկատվական

անվտանգության ռեսուրսների օպտիմալ բաշխման հաշվարկների համար: Նաև, հնարավոր է բանկային վճարումների տեղեկատվական անվտանգության մակարդակի բարձրացում՝ աշխատանքում նկարագրված ձայնային ֆայլերի հատուկ մշակման մեթոդը օգտագործելով:

Ներդրումներ

Գիտական աշխատանքի հիմնական կիրառական արդյունքները ներդրվել են և օգտագործվում են ՀայԲիզնեսԲանկ-ի տեղեկատվական անվտանգության համակարգի բարելավման նպատակով: Ներդրման ակտը կցված է ատենախոսությանը:

Պաշտպանության են ներկայացվում հետևյալ դրույթները.

- Շտակելբերգի անվտանգության խաղերի կիրառության նպատակահարմարության հաստատում՝ տեղեկատվական անվտանգության կառավարման ոլորտում:
- Ֆինանսական համակարգերի տեղեկատվական անվտանգության ռեսուրսների օպտիմալ բաշխման հաշվարկամ մեթոդ՝ հիմնված Շտակելբերգի անվտանգության խաղերի վրա:
- Բանկային վճարումների տեղեկատվական անվտանգության ապահովման մեթոդ՝ ձայնային ֆայլերի հատուկ մշակմամբ:

Աշխատանքի հիմնական արդյունքները

1. Մշակվել է տեղեկատվական անվտանգության կառավարման խաղային մոդել՝ Շտակելբերգի անվտանգության խաղերի և նրա բայեսյան ընդլայնման կիրառությամբ [1]:
2. Մշակվել է ֆինասական համակարգերի տեղեկատվական անվտանգության կառավարմանմ եթոդ՝ բայեսյան Շտակելբերգի անվտանգության խաղերի կիրառմամբ [1,2]:
3. Կառուցվել է մոդել, որըթույլ է տալիս հաշվարկել տեղեկատվական անվտանգության ռեսուրսների օպտիմալ բաշխումը ֆինանսական հաստատությունների համար՝ տարբեր կիբեր-հարձակումների դեպքում [2]:
4. Մշակվել է բանկային վճարումների տեղեկատվական անվտանգության ապահովման նոր մոտեցում՝ ձայնային ֆայլերի հատուկ մշակմամբ [3]:
5. Հետազոտության արդյունքների հիման վրա C# լեզվով մշակվել է ծրագրային համալիր՝ օպտիմալ պաշտպանական ռազմավարության հաշվարկների համար:Կատարվել է տեղեկատվական անվտանգության ընկալման համեմատական վերլուծություն՝ տեղական և արտասահմանյան առևտրային բանկերում:

SUMMARY

Ashot A. Abrahamyan

ABOUT SOME MODELS OF INFORMATION SECURITY MANAGEMENT PROCESSES IN FINANCIAL SYSTEMS

Under present conditions, it is impossible to imagine the work of financial institutions without information technologies. Electronic circulation of documents and electronic payments are done via local and global networks. In recent years, electronic money has been growing in importance. The convenience and universal accessibility of electronic payment systems and online banking services attract huge numbers of users, and in many countries, banks and financial institutions are seriously considering the complete discontinuation of cash flow in favor of cash-free payments. A 2013 survey conducted by B2B International in cooperation with Kaspersky Lab also demonstrates the growing popularity of digital payments: 98% of those polled say they regularly use online banking or payment systems, or shop online.

Of course, these trends attracted unwanted attention. The dramatic growth in the number of users of all types of payment systems has attracted cybercriminals, and they are investing ever-growing resources into fraud schemes with which they can first gain access to users' financial data and then to their actual money. Although financial attacks are among the most complicated and expensive types of attacks, they are highly lucrative because, once successful, they provide direct access to the victims' money. Once an online banking account is accessed, all that remains is to take the money and cash it in, whereas a malware writer or the owner of a botnet designed to launch DDoS attacks or send spam still has to find clients to buy their services.

Taking into consideration these facts there are a lot of serious issues regarding to information security of financial systems. This thesis is devoted to the research of models and methods of information security management processes in financial institutions.

Particularly, application of Bayesian Stackelberg security games is suggested for information security resource allocation management modeling in financial systems. Based on that model the optimal defense strategy can be calculated in different circumstances and with multiple types of attackers. A new method is suggested for information security assurance of bank electronic payments with specially processed audio files. And, taking into consideration the crucial fact, that nowadays human factor is considered as one of the most challenges in information security, a comparative analysis of information security perception is performed in domestic and foreign banks of Armenia with use of special designed survey.

Practical Significance

The developed methods of information security management can be effectively used in financial institutions for computing optimal information security resource allocation. Also, it is possible to

increase the level of information security in banking payment system with the use of proposed method of special processing of audio files.

Implementation

The main practical results are implemented and used in ArmBusinessBank to upgrade information security system. Corresponding statement of implementation is attached.

The following statements are presented to defense:

- Approval of suitability of Stackelberg security games used in information security management domain;
- A method of computing information security resource allocation strategy with use of Bayesian Stackelberg games;
- Banking payments information security assurance with use of specially processed audio files.

Main Results

1. A game-theoretic model is developed for information security management using Stackelberg security games with its Bayesian extension [1].
2. A method is developed for managing information security in financial systems with use of Stackelberg games [1, 2].
3. A model for calculation of optimal resource allocation strategy of information security measures is developed taking into consideration multiple types of cyber-attacks to financial systems [2].
4. A new method is proposed for information security assurance of banking payments using specially processed audio files [3].
5. Based on research results a program complex is developed with C# to calculate the optimal resource allocation strategy. A comparative analysis is implemented of information security perception in domestic and foreign banks of Armenia with use of special survey.

Ծավալը՝ 20էջ: Տպաքանակը՝ 100:
ՀՀ ԳԱԱ ԻԱՊԻ կոմպյուտերային պոլիգրաֆիայի լաբորատորիա:
Երևան, Պ. Սևակի 1