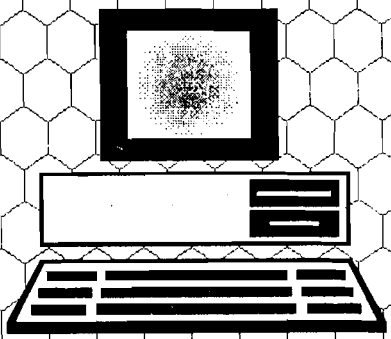
ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ

МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ИНЖЕНЕРНО-ФИЗИЧЕСКИЙ ИНСТИТУТ (ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ)

Б.И. Скородумов

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ЭЛЕКТРОННЫХ БАНКОВ



Москва 1995

ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ИНЖЕНЕРНО-ФИЗИЧЕСКИЙ ИНСТИТУТ (ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ)

Б. И. Скородумов

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ЭЛЕКТРОННЫХ БАНКОВ

Утверждено
редсоветом МИФИ
в качестве учебного пособия

Москва 1995

УДК 681.326

Скородумов Б.И. **Информационная безопасность.** Обеспечение безопасности информации электронных банков. Учебное пособие. М.:МИФИ 1995 - 104 с.

Учебное пособие является частью цикла учебной литературы под общим названием "Информационная безопасность". Пособие призвано ознакомить инженерно-технических работников и студентов с основными вопросами и состоянием проблемы обеспечения безопасности информации в современной автоматизированной банковской системе (электронном банке). В сжатой форме излагаются основные положения безопасности информации, результаты анализа состояния автоматизации отечественных банков и их специфика. Приводится перечень практических задач комплексного обеспечения безопасности информации и методология их решения на всём жизненном цикле электронного банка.

Пособие предназначено для студентов факультета "К", специализирующихся в области защиты информации в автоматизированных системах, и слушателей курсов переподготовки специалистов, а также для слушателей курсов повышения квалификации сотрудников ЦБ РФ по специальности "Телекоммуникационные системы и средства их защиты".

ISBN 5-7262-0212-0

СОДЕРЖАНИЕ

1. ВВЕДЕНИЕ

Приобщение отечественных банков к мировой банковской системе,которая начала автоматизироваться в 60-е годы, влечёт за собой широчайшее использование новейших информационных технологий в кредитно-финансовой сфере. Одновременно резко возрастают и качественно видоизменяются возможности банков в деле оказания услуг клиентам и решении собственных организационно-экономических вопросов.

Следует отметить, что современный электронный автоматизированный банк является системой, возможности и характеристики которой в целом превышают соответствующие показатели простой суммы составляющих элементов при отсутствии взаимодействия между ними. В эту систему входят аппаратные и программные средства вычислительной техники, организационные мероприятия, нормативно-методические материалы, технологии телекоммуникаций и т. п. При создании и эксплуатации автоматизированной банковской системы (АБС) необходимо учитывать место любого элемента в системе, его влияние на взаимодействующие элементы и структуру взаимосвязей. Всю совокупность средств автоматизации деятельности внутри и вне банка, которая реализуется посредством вычислительной и телекоммуникационной техники, для краткости можно назвать электронным банком. АБС является частным случаем (в прикладном смысле) автоматизированных систем обработки данных (АСОД). Прогрессивная технология на качественно новом уровне позволяет обеспечить следующие основные характеристики современного автоматизированного банка:

максимальную функциональность (платежи, бухучет, валютный обмен, расчет банковских рисков, займы, кредитование, мониторинг, статистика, клиринг, управление и т.д.);

интегрированность, заключающуюся в сосредоточении всей информации в едином центре;

оперативность информации и управления, определяемые круглосуточной работой в реальном масштабе времени;

функциональную гибкость, т.е. возможность быстрого изменения параметров или структуры системы;

развитую инфраструктуру, т.е. оперативный сбор, обработку и представление в единый центр информации со всех региональных или структурных подразделений;

минимизированные типично банковские риски (например, потери за счет ошибочных направлений платежей, фальсификация платежных поручений и т.д.) посредством обеспечения безопасности информации, которая подвергается воздействию случайных и преднамеренных угроз.

Важность последней характеристики обусловлена утверждением за информацией статуса материального ресурса. Содержащиеся в ЭВМ сведения об активах (стоимость кредита, результаты подсчета баланса, счета-квитанции, остатки на счетах и т.п.) представлены в виде цифровой информации, данных. Смена формы представления материальных активов на представляемые или символические активы в экономической жизни началось давно. Например, бумажные деньги заменили золото, акции представляют материальные ценности. Теперь цифровая информация, представляющая активы, хранится не только на бумаге в видимой и легко доступной для человека форме, но и в невидимой, считываемой только машиной, форме на электронных устройствах для хранения данных.

Новизна в форме представления активов повлияла на изменение видов финансовых преступлений, которые, как показывает мировой опыт, перемещаются в сферу электронной обработки данных.

Необходимо отметить, что финансовые потери определяются не только преступными воздействиями. Статистика финансовых потерь [1] в банках Великобритании за 1991 год сообщает, что треть убытков было обусловлено случайными причинами, например, авариями банковских автоматизированных систем обработки данных, которые произошли из-за халатности персонала или стихийных бедствий.

Банки, являясь финансовыми учреждениями, проводят разноплановую работу по снижению любых потерь, в том числе по обеспечению комплексной безопасности информационных ресурсов [2]. Например, английский Barklays Bank на защиту своей АСОД тратит ежегодно 25 млн. фунтов стерлингов.

В нашей стране процесс автоматизации банков находится на начальной стадии, что не снижает, а увеличивает актуальность проблемы обеспечения безопасности банковской информации.

2.БЕЗОПАСНОСТЬ ИНФОРМАЦИИ ЭЛЕКТРОННОГО БАНКА

2.1. Понятие безопасности информации

Начало развития автоматизации отечественных банков сопровождается поиском рациональных путей решения сопутствующих проблем, к которым относится обеспечение безопасности информации АБС. Решение этой проблемы объективно осложнено отсутствием достаточного отечественного опыта в данной области деятельности. Поэтому необходимо осмысленно использовать соответствующий зарубежный опыт и отечественный научно-технический задел по обеспечению безопасности информации в различных государственных АСОД, который относится к "высоким технологиям" двойного, гражданского и военного, назначения.

Стоит отметить, что основы упомянутого научно-технического задела полностью не сформированы. В частности, основополагающие концептуальные документы [3-7] были выпущены в 1992 году и соответствующая терминология не устоялась. Например, в документе [7] термин “безопасность информации” определяется как состояние защищенности

информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних и внешних угроз. В более позднем документе [6] это важное понятие трактуется несколько по-иному, с учетом вероятностного характера различных факторов, которые его определяют. В новой трактовке безопасность информации - состояние информации, информационных ресурсов и информационных систем, при котором с требуемой вероятностью обеспечивается защита информации (данных) от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), копирования, блокирования и т.п.

Незавершенность последней формулировки и другие ее погрешности не позволяют с достаточной степенью четкости определить цель обеспечения безопасности информации и задачи ее достижения. Важность этого понятия очевидна, и поэтому попытаемся предложить расширительную формулировку, которая учитывает последние международные результаты в этой области техники [8] и аналогичные отечественные наработки [2,9,10]. Таким образом, безопасность информации - состояние устойчивости информации к случайным или преднамеренным внешним воздействиям, исключающее недопустимый риск ее уничтожения, искажения и раскрытия, которые приводят к материальному ущербу владельца или пользователя информации. Это определение наиболее полно учитывает главное назначение любой информационной АБС - исключение потерь, получение прибыли владельцем и пользователями данного инструментария в условиях реальных рисков.

Отсюда вытекает определение защиты информации как комплекса мероприятий, проводимых с целью предотвращения ущерба от действия угроз безопасности информации, где угроза является потенциальной возможностью нарушения безопасности информации. Из предложенных определений следует вторичность защиты информации по отношению к ее безопасности, необходимость строгой аргументации и экономической обоснованности применения средств защиты, что реально возможно только после детального анализа объекта защиты (в нашем случае информация в АБС) и различных угроз безопасности информации.

2.2. Современная отечественная АБС

За последние несколько лет в нашей стране был сделан рывок в автоматизации банковской деятельности, который ознаменовался завершением в целом первого этапа автоматизации и переходом к новому этапу совершенствования АБС. Процесс автоматизации можно условно подразделить на этапы с обобщением и выделением типичных функциональных признаков многих действующих отечественных АБС. При этом следует учитывать показатели массовой продукции отечественных фирм, которые занимаются автоматизацией банков [11].

Средний, типичный, коммерческий банк обслуживает около 1500 клиентов, ведет 300-600 кредитных договоров, выполняет до 2000 проводок в день и хранит информацию по каждому из клиентов не менее трех лет.

На первом этапе автоматизации функциональное назначение АБС типичного банка ограничивалось реализацией повседневных, рутинных задач (кредитные и кассовые операции, расчеты, учет, отчетность), которые можно подразделить на несколько групп. Например, отчетность может включать следующие группы документации:

операционный день;

балансы за день, оборотные балансы за отчетный период, сводные балансы;

статистику;

подсистемы валют, вкладчиков и кредитов.

Для решения перечисленных задач используется оборудование локальных вычислительных систем (ЛВС) преимущественно с сетевой операционной системой (ОС) NetWare фирмы Novell, в которых применяются персональные ЭВМ типа IBM PC с операционной системой MS DOS, организованные по схеме "интелектуальные рабочие станции - файл-сервер". Используются

различные простейшие системы управления базами данных (СУБД), такие как Fox Pro, Clipper, Clarion и т. д.

В таких АБС не всегда встречаются минимальные средства обеспечения безопасности информации, которые должны содержать:

подсистему защиты информации от несанкционированного доступа (НСД);

оборудование и процедуры страхового копирования и дублирования;

подсистему защиты информации в телекоммуникациях;

систему бесперебойного первичного электропитания, свободную от флуктуаций силовой, электрической сети.

Функционирование и взаимодействие перечисленных средств необходимо осуществлять посредством организационных мероприятий. Наиболее часто встречается использование отдельных фрагментов этих средств. Например, применяются агрегаты бесперебойного питания (АБП) от электрической сети, позволяющие в несколько минут завершить вычислительный процесс, но не обеспечивающие работу ЛВС в случае более продолжительной аварии. Используемые криптографические средства электронной цифровой подписи, необходимые для безопасного взаимодействия с клиентами или абонентами по телекоммуникациям, как правило, не сертифицированы. Дублирование обычно ограничено использованием зеркальных накопителей на жестких магнитных дисках (НЖМД). Редко встречается регулярное сканирование информационных ресурсов ЛВС, которое должен осуществлять сетевой администратор.

Так как MS DOS создавалась для широкого применения и не имеет средств защиты информации, в банках часто опираются на слабые защитные свойства сетевой ОС NetWare, которая предназначена для обычных условий применения в офисах и на промышленных предприятиях. Повсеместно применяется программно реализованная парольная система, призванная защитить от несанкционированного входа в систему. При этом общая ошибка пользователей MS DOS заключается в том, что они помещают процедуру вхождения с паролями в автоматические

batch-файлы и не достигают необходимой защиты. Краткое перечисление слабых, фрагментарных средств защиты информации большинства отечественных АБС позволяет сделать вывод о несовершенстве их систем обеспечения безопасности информации и как следствие возрастание угроз стабильности развития банков.

Дальнейшее совершенствование отечественных АБС возможно на пути приближения к лучшим зарубежным образцам, которые поддерживают, практически, любой вид банковской деятельности, имеют богатые информационно-аналитические возможности, достаточно развитую систему безопасности информации, подсистему электронных платежей с применением пластиковых идентификационных карточек, надежные средства телекоммуникаций и гибкую, развиваемую архитектуру "клиент-сервер". Основной особенностью этой архитектуры является малая зависимость от типа ЭВМ, например, IBM RS/6000, Hewlett-Packard (HP 9000), DEC (Alpha/5900,5000,5200) и др. ЭВМ работает в большинстве случаев под управлением многозадачной, многопользовательской операционной системы UNIX или подобных, типа OS/2, VAX VMS, OS/400.

Структурированная система защиты информации от НСД обязательно входит в перечень базовых модулей любой современной зарубежной АБС. Она включает подсистемы управления доступом и криптографических средств защиты информации. Помимо этого производится обязательная регистрация действий пользователей, а также несанкционированного входа в систему и доступа к записям. Подсистема обеспечения целостности информации, особенно в базе данных, является главной в каждой системе и включает совокупность аппаратных, программных и организационных мер и методов защиты. Особое внимание уделяется поддержке и контролю функционирования системы защиты информации (СЗИ).

Не меньшее внимание уделяется воздействию среды, в которой функционирует АБС, на устойчивость работы вычислительной техники [12]. При этом учитываются многообразные факторы, начиная от заземления и завершая условиями трассировки коммуникаций. Тщательно анализируются возможные нештатные аварийные ситуации с целью компенсации их воздействий на

вычислительный процесс, например, с помощью резервного центра обработки данных.

Особенности российской банковской системы накладывают свой отпечаток на специфику безопасности информации отечественного электронного банка и предполагают их рассмотрение.

2.3. Специфика системы безопасности информации электронного банка

Как уже отмечалось в разделе 2.1, при обеспечении безопасности информации отечественных АБС целесообразно учитывать зарубежный и отечественный опыт защиты информации в различных государственных АСОД. Очеведно, что это надо делать осторожно, принимая во внимание особенности российских банков и, соответственно, их системы защиты информации.

Перечислим упомянутые особенности. К ним относятся:

а) специфические правила бухгалтерского учета;

б) неразвитость банковской деятельности;

в) становление систем клиринговых рассчетов;

г) нестабильность и незавершенность банковского законодательства.

Данные особенности поясняют стремительное и продолжающееся развитие отечественных АБС. Известно, что нет двух коммерческих банков с полностью идентичной технологией обработки документов. В этих быстро меняющихся условиях можно только укрупненно рассматривать специфику безопасности информации электронных банков и давать общие рекомендации по ее обеспечению. Изложим специфические черты обеспечения безопасности информации АБС по сравнению с аналогичными государственными системами.

Основной особенностью любой АБС и ее подсистем является главенство критерия эффективность/стоимость при выборе технических или организационных решений построения системы защиты информации.

Другая особенность заключается в обработке коммерческой информации, связанной с понятием "банковская тайна". Как будет показано далее, отечественная законодательная база в области коммерческой (банковской) тайны не сформирована, что существенно затрудняет классификацию быстроменяющейся банковской информации и, следовательно, построения системы ее защиты.

Зарубежная статистика правонарушений в АБС и соответствующий отечественный опыт позволяют сделать вывод о приоритете целостности и доступности информационных ресурсов над их конфиденциальностью.

Следующая особенность заключается в относительной юридической и организационной независимости субъектов взаимодействия в сфере экономики, что требует дополнительных усилий по юридически значимому подтверждению (проверке подлинности) участников конкретной финансовой процедуры, а также документированных результатов их сотрудничества.

Изложенная специфика и перечисленные особенности АБС выдвигают дополнительные требования к системам обеспечения безопасности банковской информации. Следует отметить, что это не оказывает существенного влияния на конкретные элементы и средства таких систем по сравнению с результатами классификации банковской информации.

2.4. Классификация банковской информации

В предыдущем разделе отмечалась сложность классификации банковской информации, связанная с неразвитостью банковской

деятельности и соответствующего законодательства в России. Поэтому рассмотрим основные аспекты этой проблемы.

Из всего многообразного информационного потока, проходящего через коммерческий банк, целесообразно выделять сведения, которые составляют банковскую тайну, являющуюся составной частью коммерческой тайны. Отметим ряд особенностей банковской тайны по сравнению с коммерческой тайной:

банковская тайна является производной отношений двух сторон: банка и клиента;

для коммерческой тайны важна только охрана сущности, а для банковской - охрана самого факта ее наличия, т.е. отношений банка и клиента;

предоставление коммерческой тайны третьим лицам определяется возможной прибылью (для банка такое всегда имеет вынужденный характер);

сохранение коммерческой тайны стимулируется возможной прибылью, что дополняется для банка повышенной ответственностью;

любая купля-продажа банковской тайны всегда незаконна.

Понятие "банковская тайна" введено законом Российской Федерации от 2 декабря 1990 года "О банках и банковской деятельности", статья 25 "Банковская тайна" которого гласит [13]:

"Банки, включая Банк России, гарантируют тайну по операциям, счетам и вкладам своих клиентов и корреспондентов. Все служащие банка обязаны хранить тайну по операциям, счетам и вкладам банка, его клиентов и корреспондентов.

Справки по операциям и счетам юридических лиц и иных организаций могут выдаваться самим организациям, их вышестоящим органам, судам, следственным органам, органам арбитража, аудиторским организациям, а также финансовым органам по вопросам налогообложения (валютный контроль).

Справки по счетам и вкладам граждан выдаются, кроме самих клиентов и их представителей, судам и следственным органам по делам, находящимся в их производстве, в случаях, когда на

денежные средства и иные ценности наложен арест, обращено взыскание или применена конфискация имущества."

Как следует из приведенной выдержки, банковская тайна охватывает операции, счета и вклады банка, его клиентов и корреспондентов. Законодательные исключения из этого положения касаются отдельных операций, которые связаны с деятельностью судебных и налоговых ведомств. Ответственность банка за сохранение тайны может быть увеличена и дополнена в договорах банка и клиента.

При определении охраняемой коммерческой и, тем более, банковской информации необходимо выяснить:

степень известности информации третьим лицам;

финансовую или иную ценность охраняемых сведений;

возможность реального сохранения тайны;

непротиворечивость охраны конкретных сведений действующему законодательству;

соотношение средств, затрачиваемых на защиту информации и ее реальной стоимости.

По результатам подобного анализа составляется перечень сведений, подлежащих разной степени защиты, который может включать следующие группы информации:

1. Финансово-учетная информация:

   источники и объемы финансирования и кредитования;

   условия кредитов;

   подробные балансы и финансовая отчетность;

   показатели акционерного капитала;

   данные управленческого учета.

2. Сведения о банковских услугах:

   изменение видов и объемов услуг;

   условия оказания услуг;

   расчеты цен на отдельные услуги;

планы и результаты маркетинговых исследований;

банки данных по клиентам.

3. Организационно-управленческая информация:

банки данных о работниках;

организационные сведения о банке;

сведения о кадровых изменениях;

материалы заседаний правления.

4. Социальная информация:

сведения о зарплате;

сведения о социальных конфликтах.

На основании представленного анализа определяется степень конфиденциальности информации, а также материально-техническое и организационное обеспечение сохранности сведений в АБС на весь их жизненный цикл [14].

2.5. Анализ угроз информации электронного банка

Практика работы отечественных и зарубежных АБС показала, что накапливаемая, хранимая и обрабатываемая банковская информация является уязвимой, т.е. подвержена опасности уничтожения, искажения и раскрытия. Событие или действие, которое может вызвать нарушение функционирования АБС, включая уничтожение, искажение, раскрытие или несанкционированное использование ее информационных ресурсов, называется угрозой [2]. Возможность реализации угроз в АБС зависит от наличия в ней уязвимых мест. Количество и специфика уязвимых мест или критических зон определяется видом решаемых задач, характером обрабатываемой информации, архитектурой, структурой и

топологией АБС, ее аппаратно-программыми особенностями, наличием средств защиты и их характеристиками.

Обобщая, можно выделить две основные группы угроз: природные и связанные с человеческим фактором. Последние, в свою очередь, подразделяются на техногенные и непосредственно создаваемые людьми.

Природные угрозы (пожары, наводнения, землетрясения, ураганы и т.д.) обусловлены прямым физическим воздействием на АБС и приводят к уничтожению или повреждению информационных ресурсов или всей системы. По данным, приведенным в литературе [1,2], от 20 до 30% всех нарушений составляют стихийные бедствия, которые приводят к полной или частичной потере информвционных ресурсов.

Угрозы, созданные людьми прямо или косвенно, преднамеренно или случайно, составляют самую большую часть всевозможных воздействий на АБС. Зачастую трудно определить источник и характер угроз, т.к. сложно выделить, тем более, если это скрывается, первопричину различных нарушений в функционировании АБС или нанесении ущерба информационным ресурсам. Например, отключение или флуктуации электропитания могут иметь техногенный характер, что обусловлено подключением к электросети множества различных потребителей, которые не всегда выдерживают регламентированные условия эксплуатации. В результате возникают броски или провалы напряжений электропитания средств вычислительной техники (СВТ), что зачастую приводит к сбоям в работе ЭВМ. Более серьезные нарушения приводят к авариям АБС и полным пропаданиям электропитания на срок от нескольких минут до нескольких часов и даже суток, что, в свою очередь, может вызвать полный паралич АБС и нанести колоссальный финансовый ущерб. В еженедельнике "Computer Word Moscow" N 30 (138) от 11 августа 1994 года в статье "Как защитить свои активы" говорится о последствиях взрыва в Центре международной торговли (Нью-Йорк, февраль 1993 года) спустя полтора года для информационных систем Уолл-стрит. Из 350 пострадавших фирм 150 обанкротились, т.к. катастрофа их застигла врасплох и они не смогли обеспечить необходимый уровень восстановления данных в своих информационны системах. Среди

успешно преодолевших трудности отмечены фирмы Bankers Trust New York и Salomon. Последняя за четыре предыдущих года вложила более 200 млн. долларов на повышение устойчивости работы своей автоматизированной информационной системы в условиях непредвиденных ситуации. Там же приводится печальный пример программного сбоя мейнфрейма во время выполнения процесса верификации заявок по ценным бумагам корпорации Paine Webber и отмечается, что разовые убытки от подобных случайностей находятся в пределах от 10 до 30 тыс. долларов.

Общие потери банков и других финансовых организаций США (начало 90-х годов) от воздействий на их электронные системы достигали нескольких десятков миллиардов долларов в год. Из них в 2 миллиарда долларов оцениваются потери, связанные с системами электронных платежей, в которых используются пластиковые карточки с магнитной полосой, что составляет 0,5-10 % от общего объема платежей. Средняя величина ущерба от банковской кражи с применением электронных средств составляет около 9 тыс. долларов.

В силу высокой стоимости банковской информации, за последнее десятилетие в зарубежной печати отмечалось множество случаев несанкционированного получения или воздействия на информацию АБС. Целесообразно перечислить обобщенные результаты анализа преступных действий, которые представляют потенциальную и реальную угрозу для отечественных АБС [2,15]:

хищение носителей информации и производственных отходов;

считывание данных в массивах других пользователей;

чтение остаточной информации в памяти системы после выполнения санкционированных запросов;

копирование носителей информации с преодолением средств защиты;

маскировка под зарегистрированного пользователя;

использование программных ловушек;

использование недостатков системы управления базами данных (СУБД) и операционных систем;

включение в библиотеки программ специальных блоков типа "троянский конь";

незаконное подключение к аппаратуре и линиям связи;

перехват электронных излучений;

применение средств перехвата информации (закладок);

злоумышленный вывод из строя механизмов защиты;

модификация программного обеспечения путем незаметного добавления новых функций;

получение несанкционированного доступа, т.е. нарушение конфиденциальности информации;

отказ от факта получения информации, которая была получена;

отказ от факта формирования информации;

утверждение о том, что информация получена от некоторого пользователя, хотя на самом деле она сформирована самим же нарушителем;

несанкционированное расширение или превышение установленных регламентированных полномочий;

распространение и использование компьютерных вирусов.

Приведенный неполный перечень угроз АБС заканчивается вирусной опасностью, которая весьма актуальна для отечественных систем, большинство ЭВМ которых работают под управлением операционной системы (ОС) MS DOS. Наибольшее число компьютерных вирусов создано для распространения в вычислительных системах с указанной ОС [16].

Проиллюстрируем приведенный перечень типично банковским примером распространенной на практике атаки типа "салями". Атакой называется несанкционированное действие субъекта АБС, использующего реальную уязвимость системы, для достижения нерегламентированных целей. Смысл этой атаки заключается в направлении (обычно программными средствами) несущественных результатов округлений проводимых операций с деньгами на определенный счет. Если учесть гигантское число операций в автоматизированном банке, то за сравнительно короткий срок

злоумышленник может накопить на своем счете весьма солидную сумму. Как свидетельствует практика, сумма, собранная из таких мелочей за год, может исчисляться тысячами долларов в среднем по размерам банке.

Возможны более серьезные (в финансовом смысле) последствия преднамеренных воздействий на АБС. Например, в 1989 году рассматривалось дело группы сообщников по компьютерному ограблению чикагского "Ферст нэшнл бэнк". В состав этой группы входили сотрудники банка, которым удалось внедриться в электронную систему банковских операций и перевести сумму свыше 69 млн. долларов из банка в Чикаго в два австрийских банка, расположенных в Вене. Во время попытки перевода этих средств на личные счета в Америке преступники были пойманы. Можно привести множество аналогичных примеров по материалам зарубежной печати. Анализ подобной статистики показывает,что от 70 до 90 % всех преступных воздействий на АБС осуществляют сотрудники банков [2]. При этом следует учесть невысокую раскрываемость таких преступлений, которая, по оценкам экспертов, не превышает 10 %. Это обусловлено двумя причинами:

техническая сложность раскрытия преступлений в АБС;

нежелание банков, терять свой авторитет.

За рубежом в последние годы отмечался рост вирусных угроз и увеличение числа попыток несанкционированного доступа к информации в электронных банках.

Подробная зарубежная статистика нарушений начала 90-х годов такова:

около 3% - внешние нарушения (проникновение на территорию);

70-75% - внутренние нарушения, из них:

10% - совершены обиженными и недовольными служащими-пользоватемями системы;

10% - совершены из корыстных побуждений персоналом системы;

50-55% результат неумышленных ошибок персонала и пользователей системы в результате преступной халатности или некомпетентности.

Таким образом, основная угроза информации, обрабатываемой АБС, находится внутри банка.

В нашей стране также все чаще стали появляться сообщения в печати о компьютерных банковских преступлениях. В еженедельнике "Коммерсантъ" N 40 (90) от 30 сентября - 6 октября 1991 года можно прочитать сообщение о крупном хищении валюты во Внешэкономбанке СССР, которое было совершено начальником отдела вычислительного центра этого банка. Кража проводилась с помощью компьютерной программы, автором которой был сам преступник. Эта программа использовалась в банке около 10 лет. По данным журнала "Деньги" N 4 за 1994г. в сентябре указанного года по модему в сеть ОПЕРУ Сбербанка Москвы были направлены фальшивые авизо на общую сумму 62 млрд. рублей. Служба безопасности зафиксировала фальшивки и стала выявлять нарушителя. Пока продолжался этот процесс в Сбербанк пришло еще несколько фальшивок на 53 млрд. рублей. В результате была обнаружена квартира, в которой с помощью персональной ЭВМ и модема фабриковались фальшивые авизо. В одном из случаев через новую компьютерную сеть Московского РКЦ Центробанка неизвестные злоумышленники пытались украсть 68 млрд. рублей. Хищение было случайно выявлено. По данным Центрального банка России, ежеквартально выявляется фиктивных платежей на десятки миллиардов рублей, которые преступники внедряют в сети подразделений банка. По данным МВД России с 1992-1994гг. из банковских структур преступниками по фальшивым кредитовым авизо и поддельным мемориальным ордерам было похищено более 7 триллионов рублей.

Бурному росту банковских компьтерных преступлений в России способствует три объективные причины:

растущая криминализация общества;

быстрая и бессистемная автоматизация банков, которые находятся в фазе бурного становления;

отсутствие полной законодательной базы.

Последнее частично компенсируется Указом Президента от 03.04.95г. N 334, который подкрепляет положение нормативных документов, созданных для обеспечения безопасности информации в автоматизированных системах.

Быстрая бессистемная автоматизация банков обостряет проблемы безопасности информации. В настоящее время, когда большинство российских коммерческих банков находится в неприспособленных для этого вида деятельности зданиях, занимая помещения, которые граничат с жилым сектором или площадями других предприятий, не представляет большой сложности восстановление информации с экрана монитора банковской персональной ЭВМ. Для решения задачи восстановления информации, отображенной на экране монитора используются его электромагнитные излучения, которые перехватываются обычным бытовым телевизором, например типа "Ладога-205", с обычной типовой антенной. Способ формирования изображения на мониторе персональной ЭВМ такой же, как и в ТВ-приемнике. Устойчивый прием негативного изображения по данным работы [17] осуществляется на расстоянии до 15 метров.

Приведенный пример только подчеркивает особенности обеспечения безопасности информации в отечественных условиях. Ранее отмечалась индивидуальность каждого банка и, соответственно, его АБС. Поэтому обеспечение безопасности информации каждого банка должно строиться строго индивидуально при использовании общей методологии, которая будет описана далее, и типовых элементов или модулей средств защиты информации.

3.МЕТОДОЛОГИЯ ЗАЩИТЫ ИНФОРМАЦИИ В ЭЛЕКТРОННОМ БАНКЕ

3.1. Модель нарушителя и анализ рисков

В предыдущем разделе, исходя из статистических материалов, пришли к выводу, что максимальную угрозу для АБС представляют

непреднамеренные и преднамеренные действия персонала банка. Причины таких действий делятся на следующие группы: халатность, некомпетентность, самоутверждение и корыстные цели. Первые три причины на практике часто переплетаются и трудно разделимы. По данным [1,2] большую часть всех нарущений представляют неумышленные ошибки персонала. Злонамеренные воздействия случаются реже, но несут больший финансовый ущерб. Естественно, что максимальный ущерб могут нанести высококвалифицированные специалисты, имеющие непосредственный доступ, с наибольшими полномочиями, к АБС. Перечисленные факторы следует учитывать при разработке модели потенциального нарушителя и оценки степени риска.

Риск есть стоимостное выражение вероятностного события, ведущего к потерям. С учетом определения безопасности информации, изложенного в разделе 2.1, для ее обеспечения необходимо определить величину недопустимого риска и с помощью средств защиты обеспечить непревышение данной величины. Систематический анализ АБС дает всестороннюю информацию о состоянии системы и степени риска [2].

Анализ риска позволяет помимо количественной и качественной оценки предельных величин ущерба выяснить одновременно ряд характеристик АБС:

ориентировочная стоимость системы защиты информации;

разносторонняя оценка предполагаемых методов и средств защиты;

отработка средств и методик подобного анализа.

Процесс анализа риска состоит из следующи этапов:

инженерно-техническое обследование и описание информационных ресурсов АБС;

определение наиболее критичных, уязвимых мест системы;

вероятностная оценка угроз безопасности информационным ресурсам АБС;

экономическая оценка возможного ущерба;

стоимостной анализ возможных методов и средств защиты информации;

определение рентабельности применения системы защиты информации.

Информационные ресурсы АБС включают:

хранимые или обрабатываемые данные;

аппаратные и программные средства автоматизированной системы;

персонал АБС, которая является системой "человек-машина".

Определение уязвимых мест завершается вероятностной оценкой угроз безопасности информационным ресурсам. Перечисленные действия сопровождаются и завершаются экономическим анализом по критерию эффективность / стоимость. Окончательный вывод о выборе конкретной системы защиты информации также производится по финансовым критериям и возможностям.

Анализ риска делается по эмпирическим моделям, с применением теории математической статистики и экономических методик. Исходные данные часто приводятся или ранжируются в виде таблиц и матриц.

Изложенная последовательность действий ориентирует на планомерное осуществление работ по обеспечению безопасности информации АБС.

3.2. Планирование реализации защиты информации

За рубежом существует практика разработки и реализации планов безопасности, которые определяют цели и правила обеспечения безопасности АБС, ответственность и необходимую

подготовку персонала, которые взаимосвязаны в едином временном процессе. Такой план может включать следующие разделы:

политика безопасности;

текущее состояние автоматизированной системы;

реализация системы безопасности;

организационные положения и мероприятия;

внедрение и сервисное обслуживание средств защиты;

развитие и уточнение плана.

Рассмотрим более детально первый раздел плана, посвященный политике безопасности, которая является документом, вобравшим основные положения, правила и практические рекомендации по распределению и защите критичной информации в системе. Политика безопасности содержит цели системы защиты информации, меры ответственности и санкции, связанные с защитой. В этом документе излагается (для АБС с определенной совокупностью объектов и субъектов, с конкретной технологией обработки информации) набор требований по защите и средств их реализации. Основу политики безопасности составляет способ управления доступом, определяющий порядок доступа субъектов системы к ее объектам. Здесь субъект - активный компонент системы, который может явиться источником потока информации от объекта к субъекту или причиной изменения состояния системы. Объект - пассивный компонент системы, доступ к которому подразумевает доступ к содержащейся в нем информации. Для анализа способа управления доступом строится его математическая модель с перенесением ее на конкретную структуру программных средств, операционную систему, систему управления базами данных или на автоматизированную систему в целом. Модель защиты представляет собой формализованное описание правил взаимодействия ресурсов в программно-аппаратной среде автоматизированной системы. Модель защиты позволяет сконцентрировать внимание на наиболее важных аспектах защиты информации, сравнивать различные системы на общей основе.

Модели защиты информации возникли из работ по теории защиты операционных систем [18]. В настоящее время наибольшее

распространение получили матричные (дискреционные) модели защиты информации вследствие того, что они служат не только для целей анализа логического функционирования системы, но и поддаются практической реализации в конкретных программных системах.

Другим распространенным видом моделей являются многоуровневые модели, в которых рассматривается не только сам факт доступа к информации, но также и потоки информации внутри системы. Наибольшую известность имеет многоуровневая модель защиты, разработанная Бэллом и Ла Падулом в фирме Mitre Corp[9].

В план безопасности может входить отдельным разделом или иметь автономное значение план обеспечения непрерывной работы и восстановления (ОНРВ) функционирования АБС. План ОНРВ предназначен для определения действий в критических ситуациях (см. раздел 2.5) и содержит разделы, которые должны предотвратить кризисные события. В крайнем случае, при возникновении опасной ситуации, в плане предусмотрен раздел восстановления системы. Обычно план ОНРВ содержит следующие пункты:

описание нарушений и кризисных ситуаций;

реакция пользователей и администрации;

оценка ущерба от нарушения;

устранение нарушения и возобновление функционирования;

разбор или расследование нарушений.

Для практической реализации плана ОНРВ предусматриваются различные виды копирования данных и всевозможное резервирование самой АБС.

3.3. Задачи и методы обеспечения безопасности информации

Подводя итог вышеизложенному, можно сформулировать триединую задачу обеспечения безопасности информации в АБС:

1) предотвращение недопустимых рисков для информационных ресурсов;

2) регистрация и анализ нерегламентированных воздействий на систему;

3) компенсация последствий нарушений в системе.

Решение задачи обеспечения безопасности информации в АБС должно приводить к снижению рисков для информационных ресурсов. С учетом положений раздела 2.5 можно сгруппировать угрозы в следующий перечень [18], в котором опасные действия расположены в порядке убывания рисков для банковских автоматизированных систем:

а) подделка или модификация информации - злоумышленные или случайные действия, в результате которых нарушается целостность (точность, достоверность, полнота) информации;

б) утрата или порча информации - умышленные или неосторожные действия, приводящие к полному или частичному уничтожению информации;

в) раскрытие или кража информации - умышленные или неосторожные действия, приводящие к нарушению конфиденциальности информациии ее незаконному тиражированию;

г) нарушение доступности или блокировка информации для законного пользователя в автоматизированной системе ее обработки, что связано с частичным или полным нарушением работы системы.

Решение поставленной задачи достигается путем создания системы комплексной защиты информации, которая реализует ряд методов, средств и мероприятий, направленных на обеспечение безопасности информации [2,15]. Кратко перечислим упомянутые методы.

1. Управление доступом - метод защиты информации регулированием использования всех ресурсов системы, включающий следующие функции:

идентификация ресурсов системы;

установление подлинности (аутентификация) объектов или субъектов системы по идентификатору;

проверка полномочий в соответствии с установленным регламентом;

разрешение и создание условий работы в соответствии с регламентом;

регистрация обращений к защищаемым ресурсам;

реагирование при попытках несанкционированных действий.

2. Препятствие - метод физического преграждения пути нарушителю к защищаемым ресурсам системы.

3. Маскировка - метод защиты информации путем ее криптографического закрытия.

4.Регламентация - метод защиты информации, создающей такие условия автоматизированной обработки, хранения и передачи информации, при которых возможности несанкционированного доступа к ней минимизируются.

5. Принуждение - метод защиты информации, при котором пользователи и персонал системы вынуждены соблюдать регламент под угрозой ответственности.

6. Побуждение - метод защиты информации, который мотивирует пользователей и персонал системы соблюдать сложившиеся морально-этические нормы.

Изложенные методы реализуются в автоматизированных системах посредством технических (аппаратные и физические) и программных средств, которые охвачены и координируются организационными мероприятиями, включающими морально-этические нормы и законодательные акты [19].

3.4. Обобщенная структура систем защиты информации от несанкционированного доступа

В предыдущем разделе среди множества угроз информации электронного банка была выделена проблема несанкцио-

нированного доступа к информационным ресурсам, которая является составной частью обеспечения безопасности информации АБС.

В общем случае система защиты информации от несанкционированного доступа состоит из четырех подсистем [18]:

управления доступом;

регистрации и учета;

криптографической;

обеспечения целостности.

Подсистема управления доступом, как упоминалось в предыдущем разделе, содержит элементы идентификации, проверки подлинности и контроля доступа к ресурсам. При наличии нескольких уровней конфиденциальности информации, она включает средства управления потоками информации.

Подсистема регистрации и учета содержит средства регистрации и учета событий или ресурсов с указанием времени и инициатора. Регистрация осуществляется посредством ведения системного журнала. Данная подсистема также осуществляет очистку (обнуление) накопителей от использованной информации.

Криптографическая подсистема реализуется в виде программно-аппаратных комплексов (ПАК) или программных средств, соответствующих требованиям ГОСТ 28147-89, ГОСТ Р34.10-94 и ГОСТ Р43.11-94.

Подсистема обеспечения целостности является обязательной и включает перечисленные методы и средства защиты, которые обеспечивают:

физическую охрану информационных ресурсов АБС;

контроль целостности программных средств;

периодическое тестирование системы;

функционирование администратора или службы безопасности информации;

применение сертифицированных средств защиты информации;

восстановление системы защиты информации в соответствии с планом ОНВР.

Практика разработки систем защиты информации позволила выделить ряд основных принципов защиты информации в автоматизированных системах.

1. **Комплексность механизма защиты информации.** Надежная защита информации от НСД обеспечивается сочетанием организационных мер, программных, криптографических и аппаратных средств защиты. Существенно важным является то обстоятельство, что ни одно из названных средств не является абсолютным в том смысле, что только с его помощью можно было бы обеспечить требуемую защиту информации в современных АБС. Напротив, на основании опыта проектирования отечественных и зарубежных АБС можно утверждать, что только комбинированным и комплексным использованием всех названных средств может быть обеспечена защита данных. Организационные меры играют ведущую роль в системе защиты от НСД: являются самостоятельным инструментом защиты и одновременно объединяют все средства и методы в целостный механизм защиты информации в АБС.

2. **Принцип персональной ответственности.** Заключается в том, что каждый пользователь должен нести персональную ответственность за свою деятельность в системе, включая любые операции с конфиденциальной информацией и возможные нарушения ее защиты.

3. **Минимизация и разделение полномочий по доступу к обрабатываемой информации и процедурам обработки.** Каждому сотруднику из числа пользователей, обслуживающего и эксплуатирующего персонала должен представляться наименьший набор полномочий по доступу к обрабатываемой конфиденциальной информации и процедурам её обработки. В то же время эти полномочия должны быть достаточными для успешного выполнения сотрудниками своих служебных обязанностей. Положение, при котором одно лицо становится ответственным за полную отработку любой деловой операции, недопустимо.

4. **Полнота контроля и регистрации попыток НСД.**

Доступ абонентов в систему и их действия должны контролироваться и фиксироваться для проведения возможного расследования. Меры и средства защиты должны исключать возможность совершения неавторизируемых операций в среде АБС. Любая операция должна совершаться от имени конкретного пользователя и регистрироваться соответствующим образом до её совершения. Полнота контроля означает, что данные должны быть защищены на любом технологическом участке в каждый момент времени. Анализ зарегистрированных попыток нарушения защиты должен служить основой для выработки рекомендаций по совершенствованию системы защиты.

5. **Несекретность проектирования.** Поскольку задача скрытия деталей реализации системы защиты, предназначенной для эксплуатации в течение продолжительного периода времени, является практически невыполнимой, механизм защиты должен быть эффективен даже в том случае, когда его структура и принципы функционирования становятся известными нарушителям.

6. **Равнопрочность механизма защиты.** Вероятности получения одинакового ущерба в случае обхода средств защиты или их несанкционированного отключения на различных технологических участках должны быть равны. Принцип подразумевает дифференциацию требований к мерам и средствам защиты в зависимости от величины ущерба, который может быть понесён в случае их обхода/отключения. В частности, критические операции в АБС (ущерб от которых в случае их несанкционированного совершения превышает определённый, заранее зафиксированный уровень) должны проходить дополнительную проверку на правомочность их выполнения.

7. **Контроль за функционированием системы защиты.** Данный принцип утверждает, с одной стороны, необходимость создания специальных средств и методов, направленных на предотвращение попыток несанкционированного вмешательства в работу механизмов защиты, и, с другой стороны, необходимость разработки мероприятий по проверке работоспособности и корректности этого механизма. Мероприятия по контролю функционирования системы

защиты могут быть достаточно эффективными только тогда, когда система защиты имеет достаточно простую логическую структуру, и для каждой ее компоненты можно доказать (может быть качественно):

функциональную пригодность;

корректность функционирования, в смысле объявленных функций и спецификаций.

8. **Экономичность механизма защиты.** Стоимость разработки и эксплуатации мер и средств защиты не должна превышать величины возможного ущерба при создании и эксплуатации АБС без соответствующих мер и средств защиты.

9. **Документированность системы защиты.** Атрибуты безопасности должны включаться во все документы по АБС, касающиеся её программных и аппаратных средств, их проектирования, приобретения, эксплуатации и обслуживания.

3.5. Реализация защиты информации в отечественном электронном банке

Перейдем от рассмотрения общих проблем защиты информации от НСД к их реализации в среднем отечественном электронном банке, основные характеристики которого изложены в разделе 2.2.

3.5.1. Организационные меры защиты

Организационные меры определяют порядок:

ведения системы защиты от НСД;

ограничения доступа в помещения и к СВТ АБС;

назначения полномочий по доступу;

контроля и учёта событий;

сопровождения ПО и СВТ;

контроля за системой защиты.

Для обеспечения надёжной защиты от НСД к информации АБС обязательным является разделение функций по ведению СЗИ между несколькими сотрудниками, контролирующими друг друга.

Для предотвращения доступа посторонних лиц в помещения, где расположены СВТ АБС, в рабочее время, могут применяться следующие меры:

контроль со стороны ответственных лиц из числа эксплуатирующего персонала АБС (как дополнительная служебная обязанность);

оснащение входных дверей в помещение кодовыми замками (или другими "захлопывающимися" замками, требующих для открытия ключа, карточки или знания кода);

организация постов охраны.

Дополнительно к общим мерам по ограничению доступа в помещения для предотвращения доступа посторонних лиц к СВТ АБС в рабочее время могут применяться следующие меры:

контроль со стороны ответственных лиц из числа эксплуатирующего персонала АБС;

оснащение СВТ электронными и электронно-механическими замками.

Для предотвращения доступа посторонних лиц в помещения, где расположены СВТ АБС во внерабочее время, могут применяться следующие меры:

оснащение входных дверей замками различной степени надёжности;

организация специальной службы хранения входных ключей;

установка охранной сигнализации;

опечатывание и/или опломбирование входных дверей (как мера контроля);

организация постов охраны.

Дополнительно к общим мерам по ограничению доступа в помещения для предотвращения доступа посторонних лиц к СВТ АБС во внерабочее время могут применяться следующие меры:

уборка (если зто технически осуществимо) СВТ в сейфы;

организация специальной службы хранения ключей от сейфов;

оснащение СВТ электронными и электронно-механическими замками;

опечатываение и/или опломбирование корпусов и устройств СВТ;

установка охранной сигнализации.

Для предотвращения несанкционированного назначения полномочий по доступу к ресурсам и/или данным АБС могут применяться следующие меры:

ограничение круга лиц, имеющих право давать распоряжения об изменении полномочий по доступу (включая ввод нового абонента);

контроль со стороны ответственного лица (ответственных лиц) за правильностью ведения системы разграничения доступа на основании данных ведущихся в АБС учётов;

закрытие режима назначения полномочий идентифицирующими признаками нескольких сотрудников, с обязательным комиссионным назначением/изменением полномочий.

Контроль и учёт событий в АБС реализуется посредством создания и ведения систем контроля и учёта.

По своему назначению (реализуемым функциям, организации, ведению и оформлению) в АБС выделяются следующие системы учёта и контроля:

учёт и контроль МН в АБС;

учёт и контроль технологических, ремонтно-профилактических, сопровождающих и других работ, проводимых в АБС;

учёт и контроль обращений пользователей в АБС,

Учёт и контроль МН в АБС предлагается организовать с помощью ручного журнального учёта всех используемых в АБС МН.

Данный учёт предназначен для контроля за перемещением МН в АБС, их централизованного учёта, а также для обеспечения персональной ответственности сотрудников, работающих с МН, за их сохранность.

Учёт и контроль работ, проводимых в АБС, предлагается организовать посредством ведения ручного журнального учёта работ (исключая непосредственную работу абонентов с АБС), проводимых в системе, а также специального Дела, в которое подшиваются все документы, распоряжения, протоколы и акты, касающиеся состояния АБС и работ, проводимых в ней. Фиксирование всех видов работ в АБС и изменений её состояний является обязательным.

Учёт и контроль обращений пользователей в АБС предлагается обеспечить созданием и ведением системы разграничения доступа пользователей, а также соответствующих средств автоматизированного учёта. Система разграничения доступа реализует ограничение возможностей, предоставляемых пользователю, при работе в АБС в соответствии с предоставленными ему полномочиями и обеспечивает предотвращение получения им информации, доступа к которой он не имеет, а также выполнения недоступных процедур обработки. Автоматизированный учёт обращений пользователей в АБС решает задачу определения за заданный промежуток времени всех лиц, работавших с АБС, и характера их действий.

Форма, степень детализации и порядок ведения указанных средств учёта и контроля определяются в ходе разработки системы.

При этом определяются:

реквизиты, накапливаемые в ведущихся ручных учетах;

реквизиты, накапливаемые средствами автоматизированного учета;

процедуры, позволяющие накапливать информацию по данным реквизитам, обрабатывать и выдавать ее;

порядок доступа к данным учетов;

сроки хранения, порядок ведения и уничтожения информации, накапливаемой в учетах АБС.

3.5.2. Программные средства защиты

Программные средства защиты (ПСЗ) включают в себя:

систему разграничения доступа к вычислительным и информационным ресурсам АБС;

средства криптографической защиты информации, хранящейся на магнитных носителях АРМ и файл-сервера АБС;

средства регистрации и учета попыток НСД, событий в системе, документов, выводимых на печать и т.д.;

средства обеспечения и контроля целостности программных файлов АБС, в том числе средства борьбы с программами-вирусами;

средства контроля паузы неактивности пользователя АБС.

ПСЗ реализуют обычно следующие функции:

обеспечение замкнутости программной среды АБС;

идентификация пользователей АБС;

защита парольных наборов ПСЗ;

контроль действий пользователей (разграничение доступа);

контроль паузы неактивности пользователей;

автоматизированный учет обращений к системе и учет выданной пользователям информации;

автоматическая регистрация выходных документов, выдаваемых на печать;

предотвращение и регистрация попыток НСД;

предотвращение проникновения в ПО АБС программ-вирусов;

защита внешних магнитных носителей информации от несанкционированного копирования.

Функция обеспечения замкнутости ПО АБС предназначена для предотвращения обхода нарушителем системы защиты при помощи использования программных средств, что возможно либо при наличии в системном и общем ПО необъявленных входов, либо при загрузке в систему нештатного ПО.

В целом обеспечение замкнутости программной среды осуществляется путем реализации следующих функций и мер защиты:

загрузочные модули ПО АБС хранятся на жестких магнитных дисках АРМ и файл-сервера за исключением страховых копий, хранящихся на ГМД;

специальные программные средства осуществляют загрузку на файл-сервер только необходимых программных средств и их автоматический контроль (включая выявление и удаление "лишних" программ);

специально разработанные средства осуществляют автоматический контроль целостности (неизменности) и самовосстановление программной среды каждого пользователя (путем проверки контрольных сумм файлов, поставленных на учет);

возможности, предоставляемые пользователям, ограничиваются рамками фиксированного набора процедур (меню-система);

из состава ПО АБС исключаются средства формирования пользователями собственных программ (компиляторы, интерпретаторы, отладчики и другие аналогичные средства);

системные программные средства обеспечивают запрет пересылки данных из АРМ в сеть по требованию другого пользователя АБС.

Идентификация пользователей производится в начале и в конце сеанса работы на основе вводимых ими уникальных идентификаторов и соответствующих им тайных паролей. Для контроля со стороны пользователя за работой в АБС от его имени проводится дополнительная идентификация по номеру сеанса работы.

ПСЗ осуществляется автоматическая генерация и смена паролей для пользователей. Автоматическая генерация паролей реализуется

на основе программного датчика псевдослучайных чисел, с соблюдением принятых соглашений о длине и алфавите пароля.

Сменяемость паролей пользователей обеспечивается либо автоматизированно (по установленному регламенту с организационным контролем), либо автоматически (по команде администратора).

ПСЗ при помощи средств криптографической защиты обеспечивают использование паролей пользователей в открытом виде только в момент идентификации пользователя и только в оперативной памяти АРМ. В таблице паролей хранятся образы паролей. В состав ПСЗ входит программная реализация однонаправленной функции преобразования вводимого пароля. Вводимый с клавиатуры пароль преобразуется и полученный результат сравнивается со своим образом, хранимым в памяти ПЭВМ.

Контроль действий пользователей при работе с АБС заключается в обеспечении ПСЗ установленной системы разграничения доступа пользователей и включает в себя:

проверку правомочности работы пользователей с запрашиваемыми ресурсами сети (АРМ, магнитные носители, программы обработки и т.п.);

проверку правомочности доступа пользователя к запрашиваемым режимам работы;

проверку правомочности доступа пользователя к запрашиваемым структурам данных в текущем режиме работы;

проверку на корректность передачи данных по сети (проверка полномочий источника и адресата по доступу к передаваемым данным, проверка их существования, контроль успешности сетевых пересылок, авторизация пересылок и т.п.).

Под контролем паузы неактивности понимается повторение процесса идентификации пользователя, если он не передавал в систему сообщений в течение определенного промежутка времени.

Контроль паузы неактивности осуществляется с момента ввода пользователем своего личного идентификатора в начале сеанса работы на АРМ до его окончания.

В случае истечения паузы неактивности происходит запоминание состояния системы, затирание экрана АРМ и выход в режим ожидания ввода пароля пользователя. Если время работы процедуры обработки данных превышает паузу неактивности, выход в режим запроса пароля происходит после ее окончания. НСД фиксируется, если в течение определенного времени пользователь не проходит повторную идентификацию.

ПСЗ обеспечивают:

выход из сеанса работы только после указания пароля пользователя;

реакцию на окончание работ на АРМ без выхода из сеанса работы как на возможную попытку НСД.

ПСЗ должны обеспечивать предупреждение пользователя перед истечением паузы неактивности с помощью звукового сигнала, включения рамки яркого цвета на экране дисплея в режиме мерцания и т.п.

Учет и контроль санкционированного доступа к информации и операциям над ней обеспечивается созданием и ведением средств автоматизированного учета и долговременного хранения обращений сотрудников в систему, их операций, совершаемых над БД АБС, и результатов этих действий.

Для решения этой задачи в массивах учета накапливаются следующие данные:

идентификатор пользователя;

имя (номер) АРМ сети;

дата и время сеанса работ;

процедура обработки;

результирующие признаки;

специальные признаки о совершении критических действий.

Автоматизированный учет выдаваемой информации предназначен для обеспечения возможности получения сведений о всей выданной конкретному сотруднику информации и о всех

сотрудниках, обращавшихся к конкретной информации, за заданный период времени.

Для решения этих задач в массивах учета накапливаются следующие данные:

идентификатор пользователя;

дата и время сеанса работ;

процедура обработки;

текст запроса;

идентифицирующие признаки объектов учета;

носитель, на который была выдана информация;

ПСЗ должны обеспечивать ведение (создание, получение сводных ведомостей и разовых справок, корректировку и т.п.), защиту от НСД и несанкционированных изменений, а также накопление в течение определенного времени необходимых массивов учета.

Автоматическая регистрация заключается в автоматическом формировании на выходном документе и в массивах учета регистрационной части, которая должна содержать следующие данные:

идентифицирующий признак документа (машинный или регистрационный номер);

дату и время формирования;

гриф конфиденциальности информации;

номера и количество экземпляров;

количество листов.

Кроме того, в массивах учета должны накапливаться данные, позволяющие определить пользователя, выдавшего документ на печать.

ПСЗ должны пресекаться и регистрироваться следующие виды попыток НСД:

трехкратный неверный ввод пароля;

вход в систему с идентификатором пользователя, уже работающего в текущем сеансе с АБС;

попытка нарушения установленной системы разграничения доступа;

перезагрузка системы без нормального выхода пользователя из сеанса работы на АРМ;

превышение пользователем допустимой паузы неактивности при работе на АРМ.

При обнаружении ПСЗ попытки НСД должна происходить автоматическая блокировка АРМ с фиксацией в массивах учета следующих данных:

идентификатора пользователя;

имени АРМ;

даты и времени совершения попытки;

вида попытки НСД.

Под блокировкой понимается отключение клавиатуры (программным способом). Блокировка не должна сниматься в случае перезагрузки системы. Разблокировка ПЭВМ должна производиться путем ввода специального ключа (пароля) разблокировки с АРМ администратора системы.

Для осуществления текущего динамического контроля за работой пользователей АБС может быть предусмотрен режим оперативной выдачи сообщений ПСЗ об обнаруженных попытках НСД на АРМ администратора АБС.

ПО АБС перед установкой в эксплуатацию должно пройти проверку на отсутствие возможно внедренных программ-вирусов, наличие которых может привести как к разрушению БД и потере информации, так и к нарушению функционирования ПСЗ АБС и в конечном итоге к НСД. После проверки все неизменяемые в текущем режиме программные модули системы ставятся под контроль специальных средств проверки целостности ПО. Аналогичные мероприятия должны проводиться при модернизации ПО АБС.

В процессе функционирования АБС специальной программой должен осуществляться контроль системных прерываний и обращений к системному и общему ПО АБС на предмет обнаружения обращений, типичных для известных программ-вирусов.

В АБС на ГМД могут храниться:

страховые копии локальных и сетевых БД АБС (в зашифрованном виде);

страховые копии ПО АБС (в открытом виде);

данные, обеспечивающие информационный обмен между АРМ АБС (в зашифрованном виде);

служебные данные, обеспечивающие эксплуатацию АБС (ключи шифрования и т.п.).

Для защиты перечисленных данных от несанкционированного использования и/или компрометации необходима разработка специальных программных средств, обеспечивающих невозможность их копирования на посторонних, по отношению к АБС, технических и программных средствах, как стандартными, так и нестандартными процедурами.

3.5.3. Аппаратные средства защиты

Аппаратные средства СЗИ АБС обычно выполняют три основные функции:

"прозрачное" шифрование/рашифрование информации АБС;

запрещение загрузки операционных систем и автономных программ с ГМД в процессе начальной загрузки ПЭВМ;

привязка ПО АБС к конкретным АРМ с целью запрещения несанкционированного копирования программ.

В качестве аппаратных средств шифрования используется широкий набор криптоплат, в частности криптоплаты Криптон (Приложение).

Выбор аппаратных средств защиты для АБС определяется их техническими характеристиками, оновными из которых являются:

высокая надежность с целью исключения искажения банковской информации и преодоления рубежей защиты СЗИ нарушителем;

высокая производительность шифрования информации, которая должна обеспечивать время реакции АБС на запрос пользователя не более 3 с.

3.5.4. Криптографические средства защиты информации автоматизированной банковской системы

В настоящее время достаточно серьезное внимание уделяется вопросам безопасности открытых сетей и распределенных систем. В соответствии с принятой для открытых сетей рекомендацией [8] выделяют следующие основные услуги по безопасности, которые могут быть предоставлены пользователю сети.

Контроль доступа. Под контролем доступа понимают защиту средств использования, компонент и ресурсов сети от незаконного, злоумышленного и другого несанкционированного доступа и использования.

Аутентификация обеспечивает проверку подлинности объектов, вступивших в связь для обмена информацией, т.е. служит для предотвращения маскировки одного субъекта под другой субъект.

Конфиденциальность информации, т.е. защита информации от несанкционированного ознакомления. При этом может рассматриваться как задача обеспечения конфиденциальности всей информации, циркулирующей в сети, так и задача защиты отдельных направлений или полей информации. Рассматривают также конфиденциальность траффика, то есть предотвращение возможности извлечения информации из наблюдений за адресацией, частотой и количеством потока сообщений сети.

Целостность. Под целостностью понимают защиту информации и других ресурсов сети от добавления, изменения, уничтожения,

удаления и других действий, производимых неавторизированными пользователями. При этом различают контроль целостности с восстановлением, когда при обнаружении неавторизованных изменений производится попытка восстановления исходной информации, и контроль целостности без восстановления.

Безотказность, то есть невозможность отказа субъекта от ранее производимых им действий. Безотказность может иметь одну или две из следующих форм.

Безотказность с подтверждением источника. В этом случае получателю информации гарантируется, что пославший информацию не может отказаться от факта посылки или содержания сообщения.

Безотказность с подтверждением получения. В этом случае получатель информации не может отказаться от факта получения или содержания сообщения.

Для реализации оказанных услуг служат следующие основные средства обеспечения безопасности информации.

Шифрование информации. Алгоритмы шифрования обычно различаются на две категории:

системы с симметричными или секретными ключами;

системы с несимметричными или открытыми ключами.

В системах с секретным ключом два пользователя, желающие обменяться криптографически защищенной информацией, должны обладать общим секретным ключом. В таких сетях пользователи должны обменяться общим ключом по безопасному каналу до установления связи. Это может быть сделано при помощи механизмов распределения ключей.

В системах с открытым ключом каждый пользователь вырабатывает свой секретный ключ, который хранит у себя, и соответствующий ему открытый ключ, который сообщается возможным партнерам по обычному каналу связи. При необходимости установления связи два пользователя в общем случае обмениваются открытыми ключами и, используя свои секретные ключи, вырабатывают общий ключ, известный только им.

Независимо от типа криптографических систем любая из них должна включать в себя управление крипографическими ключами.

Ключевое управление включает в себя реализацию следующих основных функций:

- генерация ключей: определяет механизм выработки ключей или пар ключей с гарантией их хороших криптографических качеств;

- распределение ключей: определяет механизм, по которому ключи надежно и безопасно доставляются абонентам, которые законно их требуют;

- сохранение ключей: определяет механизм, по которому ключи надежно и безопасно сохраняются для их дальнейшего использования;

- восстановление ключей: определяет механизм восстановления одного из ключей (замена на новый ключ);

- уничтожение ключей: определяет механизм, по которому производится надежное уничтожение вышедших из употребления ключей;

- ключевой архив: механизм, по которому ключи могут надежно сохраняться для их дальнейшего нотаризованного восстановления в конфликтных ситуациях.

Цифровая подпись. Механизм цифровой подписи включает в себя две процедуры:

выработку подписи;

проверку подписанной информации.

Процедура выработки подписи использует информацию, известную только подписывающему сообщение. Сама процедура обычно представляет собой либо шифрование данных, либо выработку проверочной комбинации, либо то и другое вместе. При этом известная только подписывающему информация используется в качестве секретного ключа.

Процедура проверки подписи является общедоступной, при этом процедура проверки не должна позволять найти секретный ключ подписывающего информацию.

Наиболее существенным в механизме цифровой подписи является то свойство, что подписать информацию можно только зная секретный ключ сообщения. Поэтому в спорных ситуациях третьей стороне (арбитру) может быть доказано, что только держатель секретного ключа мог подписать сообщение.

Средства контроля доступа. Контроль доступа обычно классифицируется на дискретный и мандатный. Дискретный контроль состоит в том, что пользователь, обладающий некоторым ресурсом, не только имеет доступ к нему, но и может передать свое право доступа другим пользователям. Мандатный контроль состоит в том, что даже пользователь, обладающий некоторым ресурсом, не может передать право доступа третьим лицам.

Формы контроля доступа довольно многообразны и включают следующие конкретные формы контроля:

- информационные базы, содержащие права авторизированных субъектов по доступу к ресурсам. Эта информация может поддерживаться в центрах доверия или непосредственно на объекте, к которому осуществляется доступ. В наиболее общем виде такая информация представляется в виде матрицы доступа, где каждый столбец соответствует защищаемому объекту и каждая строка отвечает потенциальному субъекту. Элемент матрицы определяет права доступа соответствующего субъекта к соответствующему объекту в терминах способа доступа (т.е. нет доступа, только чтение, чтение и запись, исключение, вызов и т.д.). Кроме матрицы доступа используются также иерархические и распределенные структуры доступа. При этом предполагается, что аутентификация субъектов проведена;

- аутентификационная информация, такая как пароли, представление которой считается достаточной для доступа к ресурсу;

- мандат, владение и представление которого является доказательстом права доступа;

- отметка, связанная с субъектом, разрешающая или отказывающая в доступе;

- фиксация времени, маршрута и продолжительности попытки доступа.

Средства сохранения целостности. Имеется два аспекта целостности: целостность отдельного сообщения или поля информации, и целостность потока сообщений или полей информации. Вообще говоря, разные механизмы используются для реализации этих двух типов целостности, хотя обеспечение второго без первого не имеет практического значения.

Процедура определения целостности отдельного сообщения (информационного поля) включает в себя два процесса: один на передающем конце и другой на приемном конце. На передающем конце к сообщению добавляется проверочная комбинация, которая является функцией от сообщения. Эта проверочная комбинация может быть получена при помощи соответствующих кодов или применением некоторого криптографического алгоритма, причем проверочная комбинация сама может быть зашифрована. На приемном конце, получив сообщение, вырабатывают проверочную комбинацию и сравнивают с полученной комбинацией, чтобы определить, было ли сообщение изменено при передаче. Для контроля целостности потока сообщений (т.е. защиты от переупорядочивания, потери, повторения и дополнения данных) употребляются дополнительные формы, такие как нумерация сообщений, проставление времени передачи и криптографическое связывание.

Средства аутентификации. Для аутентификации могут быть использованы следующие формы:

- аутентификационная информация, такая как пароли;

- криптографические алгоритмы;

- использование характеристик и (или) принадлежностей субъекта.

Большинство существующих компьютерных систем обеспечивают так называемую одностороннюю аутентификацию: пользователь, желающий получить доступ к компьютеру, должен первым доказать свою идентичность компьютеру, который в свою очередь решает, является ли пользователь авторизованным для доступа или нет. В этом случае предполагается, что пользователь знает и доверяет компьютеру (сети) и не требует в свою очередь его идентификации.

Развитие оборудования сети, возрастающее число инсталляций, применений и пользователей требует двухсторонней аутентификации, где обе участвующие стороны должны подтвердить свою идентичность друг для друга.

В дополнение к двухсторонней аутентификации в сетях возникает необходимость аутентификации доверенным третьим лицом, т.е. пользователь сети при обращении к каждому устройству должен каждый раз аутентифицировать их и себя, вместо этого можно использовать процедуру единственной подписи на устройстве аутентификации, обеспечивающую авторизацию пользователя сразу всей сети. В соответствии с этой процедурой, устройство аутентификации вырабатывает сертификат, представляющий всем другим устройствам сети гарантию идентичности пользователя.

На практике могут применяться средства защиты траффика и сетевых маршрутов, направленные соответственно для защиты от анализа траффика и злоумышленного изменения маршрутов в сети.

Средства нотаризации. Нотаризация состоит в регистрации данных (сообщений) на устройстве достоверности, где позже можно проверить соответствие таких характеристик сообщения, как содержание, оригинальность, место назначения, время передачи и др. Безотказность является частным случаем нотаризации, где доверенное устройство доказывает, что данное сообщение было послано (получено) по определенной почте. С возрастающим числом коммерческих и других электронных операций в сетях этот аспект приобретает все большее значение.

3.5.5. Меры по обеспечению безопасности телекоммуникаций

Известны три основных подхода к решению проблемы безопасности связи, отличающиеся не только присущими им характеристиками реализации, но и степенью обеспечиваемой ими безопасности. Эти подходы включают следующие меры:

меры, ориентированные на защиту канала связи;

меры межконцевой защиты связи (на уровне процессов);

меры, ориентированные на защиту соединений между процессами.

Меры, ориентированные на защиту канала связи, обеспечивают защиту всех сообщений, передаваемых по отдельному каналу, соединяющему два узла сети, т.е. в данном случае каждая ассоциация (или каждое соединение) представлена отдельным каналом. Каждый из таких каналов соответствует канальному уровню передачи данных семиуровневой модели взаимодействия открытых систем ISO/OSI. В данном случае нарушитель исходит из того, что легче воздействовать на канал, чем на узел связи.

В вычислительных сетях с защитой каналов связи шифрование информации может выполняться в каждом канале независимо от других каналов. Могут шифроваться протокольная информация управления потоком (например, адреса) и сами данные. При этом в каждом канале используется свой ключ шифрования. Это значит, что если один канал будет раскрыт, то это не ведет с неизбежностью к раскрытию информации, передаваемой по другим каналам. К преимуществам канально-ориентированной защиты можно отнести прозрачность системы защиты для главных ЭВМ, подключенных к сети, т.е. меры по защите информации могут быть реализованы так, что они будут совершенно незаметны для пользователей сети. Но этот подход не свободен и от недостатков. Поскольку информация передается в зашифрованном виде только по каналам , но не в пределах узлов связи, возникает необходимость защиты этих узлов. Должны быть защищены и все промежуточные узлы связи. Нарушение безопасности одного промежуточного узла приведет к раскрытию всех сообщений, проходящих через этот узел, несмотря на то, что физическая безопасность узлов отправителей и получателей остается ненарушенной.

Цель подхода, ориентированного на межконцевую безопасность, состоит в защите сообщений, передаваемых между узлами отправителей и получателей так, что нарушение безопасности одного канала не приведет к общему нарушению безопасности. При этом подходе требуется большая степень стандартизации интерфейсов и протоколов, применяемых пользователями.

Основным преимуществом мер межконцевой безопасности является то, что отдельный пользователь или главная ЭВМ могут применить их, не оказывая влияния на других пользователей и главные ЭВМ. Это значит, что затраты на применение таких мер могут быть распределены более конкретно, чем при подходе, ориентированном на канальную безопасность. Другое преимущество межконцевого подхода заключается в возможности применения этих мер в сетях с коммутацией пакетов. Кроме того, этот подход более соответствует восприятиям пользователями требований к защите информации, поскольку меры защиты при этом подходе реализуются только аппаратными средствами, расположенными у отправителей и получателей сообщений. Пользователь может легко определить в каждом случае, какие меры безопасности следует применить при связи между процессами, в частности, следует ли шифровать только передаваемую информацию или только адрес, или то и другое. В общем, подход, ориентированный на межконцевую безопасность, имеет большие преимущества по сравнению с подходом, ориентированным на канальную безопасность, применительно к открытым системам.

Подход, ориентированный на безопасность соединений (ассоциаций), является дальнейшим развитием подхода, ориентированного на межконцевую безопасность и имеет такие же преимущества. Кроме того, меры защиты при таком подходе допускают большую гибкость при установлении соединений между терминальными устройствами. Можно отметить также и такое преимущество: меры защиты при таком подходе не только защищают канал, соединяющий выбранные терминальные устройства, но и значительно снижают вероятность необнаруживаемых перекрестных (взаимных) помех.

При разработке криптографической защиты для распределенных систем необходимо определить примитивные криптографические функции (примитивы), которые могут быть использованы для создания требуемых служб безопасности, а также систему управления ключами. К криптографическим примитивам относятся, например, шифрование, расшифрование, повторное шифрование, аутентификация, проверка полномочий, проверка кода аутентификации сообщений и др.

Управление ключами основывается на многоуровневой иерархии ключей. Например, в схеме с трехуровневой иерархией имеется секретный главный ключ на каждом узле и в каждом терминале вычислительной сети. Этот ключ используется для шифрования всех ключей более низких уровней, которые могут храниться и передаваться по сети в форме шифртекста (криптограммы). Генерирование ключей может осуществляться с использованием псевдослучайных или чисто случайных процедур.

Применение асимметричных криптоалгоритмов частично решает проблему распределения ключей, так как при этом ключи могут храниться и передаваться в открытой форме, но при этом остается нерешенной проблема аутентичности ключей (отправитель должен быть уверен, что открытый ключ получателя действительно аутентичный).

Ясно, что при любом решении задачи криптографической защиты (на основе симметричной или асимметричной криптосистем) требуется существование контрольных или управляющих центров, в функции которых входят проверка аутентичности ключей и инициирование связи между субъектами распределенной системы. Эти центры должны тесно взаимодействовать с серверами имен субъектов. При любом решении важной задачей является создание безопасных каналов связи между субъектами (и объектами) системы и центрами.

Большое значение для работы сетей связи и распределенных систем имеют применяемые сетевые протоколы. Криптографические средства создают потенциально большое количество безопасных каналов связи. Эти каналы управляются протоколами шифрования. Следовательно, протоколы шифрования оказывают влияние на архитектуру и работу распределенных систем.

3.5.6. Предложения по составу и задачам средств криптографической защиты информации в автоматизированной банковской системе

В соответствии с исходными данными концепция управления обеспечением безопасности информации (ОБИ) банковской системы соответствует международным стандартам в этой области,

то есть предполагает обеспечение описанных ранее услуг по безопасности информации. Реализация указанных услуг требует наличия в АБС определенных средств криптографической защиты (СКЗ).

Средства криптографической защиты можно разделить на СКЗ пользователя (абонента) и СКЗ сети (СКЗ на серверах и ГВМ). Следует отметить, что размещение СКЗ только на абонентском уровне не позволяет в полном объеме выполнить задачу в ОБИ. Размещение СКЗ на серверах (узлах) сети в значительной степени лимитируется необходимостью встраивания криптографических функций в существующие процессы обработки информации. Поэтому представляется целесообразным на СКЗ сети возложить те функции ОБИ, которые не могут быть выполнены на абонентском уровне.

В соответствии с международными стандартами в АБС предполагается предоставление пользователю следующих услуг по обработке и использованию информации:

а) электронная почта;

б) доступ к базам данных, в частности к доскам объявлений;

в) ведение финансовой деятельности.

Для выполнения изложенных выше рекомендаций абонент должен иметь следующие возможности по обеспечению безопасности информации:

шифровать/расшифровывать данные;

проводить взаимную аутентификацию с другим абонентом или устройством (сервером) сети;

подтверждать целостность передаваемой и проверять целостность получаемой информации;

вырабатывать цифровую подпись и проверять идентичность получаемой цифровой подписи;

подтверждать свои права на пользование конкретными ресурсами сети.

Можно отметить, что системы с открытыми ключами на практике обычно не используются непосредственно для

шифрования данных ввиду недостаточной скорости шифрования. Поэтому СКЗ абонента должны включать алгоритм шифрования с симметричными (секретными) ключами, вследствие чего абонент должен дополнительно обладать возможностью вырабатывать или получать из сети секретный ключ для связи с другим абонентом.

Перечисленный набор возможностей абонента можно считать минимально необходимым для ОБИ при функционировании электронной почты.

В принципе возможности абонента по ОБИ могут быть расширены за счет возможностей работы с закрытыми базами данных сети, если такие базы будут созданы, а также за счет дополнительных возможностей по ОБИ на терминале абонента (защита файлов, контроль доступа и т.д.). Подобные задачи могут быть конкретизированы в процессе развития АБС.

Из вышеизложенного следует, что СКЗ абонента должны включать в себя алгоритм шифрования с симметричным ключом и алгоритм цифровой подписи. Как уже отмечалось, пара абонентов для связи между собой должна иметь общий секретный ключ. Выработать такой ключ можно двумя основными способами:

1) ключ вырабатывается сетью и передается абонентам по их запросу;

2) абоненты вырабатывают ключ самостоятельно при помощи алгоритма открытого распределения ключей.

Оба способа могут найти применение в АБС. Первый способ оперативнее, второй обеспечивает больший уровень конфиденциальности абонентам, так как ключ в этом случае не известен сети. Использование второго способа требует наличия у абонента алгоритма открытого распределения ключей.

Таким образом, основу СКЗ абонента должны составлять три алгоритма:

алгоритм открытого распределения ключей;

алгоритм щифрования с симметричным ключом;

алгоритм цифровой подписи.

Для подтверждения целостности обычно используют специальный режим (режим имитозащиты) алгоритма с симметричным ключом, в этих же целях можно применять алгоритм цифровой подписи. Другие задачи ОБИ (аутентификация, выработка сменных ключей, контроль доступа) решаются в виде реализации функций, производных от указанных алгоритмов.

Рассмотрим СКЗ сети. Две задачи ОБИ не могут в полной мере быть решены СКЗ абонента, это - взаимная аутентификация абонентов и распределение ключей. Например, взаимная аутентификация абонентов вообще невозможна, если они заранее не обменялись доверенной информацией. Для аутентификации и распределения ключей в АБС предлагается создать иерархическую систему связанных между собой ключевых серверов. Конкретные предложения по протоколам взаимосвязи абонентов и ключевых серверов, а также ключевых серверов между собой изложены ниже в разделе, касающемся ключевых структур.

В каждом домене сети предполагается наличие одного или нескольких ключевых серверов, которые могут предоставлять связанным с ним абонентам набор услуг, включающих:

взаимную аутентификацию абонентов;

выработку ключей для связи абонентов;

подтверждение доставки сообщения;

шифрование и отправление адресату сообщения, которое абонент при желании может передавать серверу в открытом виде.

Для выполнения указанных функций ключевой сервер необходимо оснастить СКЗ аналогичным СКЗ абонента.

Кроме перечисленного, СКЗ сети могут использоваться для решения следующих задач:

защита траффика;

защита маршрутов;

контроль целостности потока сообщений;

контроль доступа к ресурсам сети.

Для этого может применяться разнообразная криптографическая техника, включающая шифрование адресных частей, однонаправленные функции и т.д. Однако использование подобных средств связано с необходимостью встраивания криптографических функций в процессы обработки информации в сетевых устройствах.

При конкретизации программных средств, которые будут обеспечивать транспортный уровень АБС, могут быть конкретизированы и рекомендации по выбору СКЗ сети, предназначенных для решения указанных выше задач.

4. ОБЕСПЕЧЕНИЕ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ЭЛЕКТРОННОМ БАНКЕ

4.1. Практические рекомендации по созданию систем защиты информации

При конкретной реализации систем защиты информации в современном, отечественном, автоматизированном банке следует применять в соответствии с положениями документов [21,6] сертифицированные средства защиты. Ряд программно-аппаратных комплексов защиты информации, получивших сертификат уполномоченной организации или находящихся в процессе сертификации, представлен в приложении. Любые работы по защите информации должны проводиться предприятием, имеющем лицензию на проведение соответствующих работ.

Другой важный аспект обеспечения безопасности информации электронного банка касается выбранных операционных систем (ОС) автономно функционирующих ЭВМ и их сетей. Характеристики ОС существенно влияют на архитектуру и структуру систем защиты информации. Реализованные в ОС механизмы безопасности могут, например, способствовать решению следующих проблем:

предотвращение возможности несанкционированного использования и модификации (уничтожения) системных ресурсов (областей памяти, программ и т.д.) пользовательскими прикладными программами (в частности, вирусами);

обеспечение корректности выполнения пользовательских программ, параллельно функционирующих на одной ЭВМ и использующих общие ресурсы;

снижение возможности несанкционированного использования прикладными программами одних пользовательских ресурсов, принадлежащих другим.

В зарубежных банках часто используются различные ОС с хорошо отлаженными механизмами безопасности [21]. Например, мультизадачная операционная система AOS / VS фирмы Data General для 32-разрядных ЭВМ; мультизадачная ОС VAX / VMS фирмы DEC для семейства многопользовательских мини-ЭВМ VAX. Наибольшее распространение получила ОС UNIX, созданная фирмой AT&T и представляющая собой многоцелевую мультизадачную операционную систему, предназначенную для использования в пределах широкого спектра типов ЭВМ. ОС UNIX начинает применяться в амтоматизированных банках.

В частности, защита файлов в ОС UNIX организована следующим образом. С каждым файлом связывается множество прав доступа: чтение, обновление и/или выполнение (для исполняемых файлов). Владелец файла, т. е. создавшее его лицо, пользуется по отношению к файлу всеми правами. Часть этих прав он может передать так называемым членам группы - лицам, которым он доверяет сведения, имеющиеся в файле. Все остальные пользователи, не входящие в группу, также могут получить права доступа к файлу с разрешения его владельца. Доступ к ресурсам ОС ограничен средствами защиты по паролям. Пароль может быть использован в качестве ключа для шифрования-расшифрования информации в пользовательских файлах. Сами пароли также хранятся в зашифрованном виде, что затрудняет их выявление и использование злоумышленниками. Пароль может быть изменен пользователем, администратором системы либо самой системой по истечении установленного интервала времени [15].

В целом ОС UNIX традиционно считалась одной из наиболее простых в обращении и надежно защищенных операционных систем, однако известный вирус (репликатор Морриса) разрушил это устоявшееся мнение. Напомним, что подавляющее большинство известных и создаваемых вирусов предназначено для воздействия на MS DOS.

Для замкнутых банковских автоматизированных систем вирусная угроза не представляет большого значения, если соблюдаются организационные меры и определенная технология защиты от вирусов [16]. Например, проведение входного контроля дискет с новыми программным обеспечением, сегментация информации на жестком диске, систематический контроль целостности и архивирование информации.

Проектирование системы защиты, как показал практический опыт, должно быть проведено как можно раньше. Желательно, чтобы оно происходило одновременно с проектированием АБС и в соответствии с ранее описанной методологией. К проектированию системы защиты необходимо привлекать различные категории специалистов: системных аналитиков и программистов, инженеров по оборудованию, программистов. Это позволит повысить устойчивость и экономичность системы защиты в целом.

Системы защиты должна проектироваться комплексно, чтобы осуществлять минимально возможное вмешательство в деятельность пользователей АБС, одновременно обеспечивая всестороннюю защиту обрабатываемых данных. Для реализации этого требования необходимо использовать преимущества различных мер защиты как программно-технических, так и организационных. Крен в какую-либо сторону, отход от положений раздела 3.4, приводит к общему усложнению и ослаблению системы защиты. Часто наблюдается увлечение криптографическими средствами защиты в ущерб другим методам и средствам. При этом надо помнить, что практическая стойкость криптографической подсистемы защиты информации определяется организацией раздачи ключей и уступает теоретической.

Проектирование системы защиты информации и ее введение в работу лучше проводить поэтапно. Можно выделить следующие этапы разработки и внедрения системы защиты информации в АБС:

обследование конкретного электронного банка с целью получения информации, необходимой для разработки системы защиты;

разработка системы защиты информации;

внедрение системы защиты информации;

сопровождение и развитие системы защиты.

Для быстрого реагирования на изменяющиеся потребности в защите система должна иметь гибкое и мощное управление.

С целью контроля за функционированием средств защиты и их настройки, слежения за безопасностью функционирования всей АБС, разработки планов и политики безопасности целесообразно организовать специальное подразделение (в большом банке) или выделить человека, дав ему соответствующие полномочия. В частности, это подразделение до установки средств защиты информации разрабатывает правила, в соответствии с которыми будет регламентирован доступ должностным лицам банка к хранимой, обрабатываемой и передаваемой информации. Эти правила должны получить статус официального документа и их выполнение проверяется указанным подразделением. Одновременно необходимо предусмотреть ответственность персонала за нарушение этих правил.

4.2. Требования к состоянию среды функционирования

В период с 1983 года и по наше время в США выпускается большой комплект документов под общим названием "Радужная серия" (Rainbow Series), посвященных комплексному решению проблем компьютерной безопасности. В нашей стране более известна первая книга этой серии " Критерии оценки безопасности

компьютерных систем" или "Оранжевая книга". Менее известно "Руководство по применению критерия оценки безопасности компьютерных систем в специфических средах" или "Желтая книга", в которой под средой понимаются внешние условия и все то, что влияет на разработку, эксплуатацию и техническое обслуживание вычислительной системы [2]. В "Желтой книге" предлагается адекватная защита от внешних воздействий (среды функционирования вычислительной системы). Кратким аналогом этой книги являются материалы фирмы DEC для автоматизированных банков [12]. Фирма DEC оснастила и обслуживает около 70 % всех электронных банков в мире, предлагая комплексные услуги по разработке, поставке и техническому сопровождению АБС. Обобщая большой и разнообразный опыт создания и эксплуатации АБС, фирма DEC обращает значительное внимание на среду или условия функционирования СВТ, как составной части комплексного обеспечения безопасности информации. В материалах [12], помимо проблем защиты от несанкционированного доступа, упомянуты проблемы внешних воздействий среды функционирования АБС.

Физические факторы среды функционирования включают:

расположение или размещение АБС;

климатические воздействия на систему (температура, влажность и загрязнение воздушной массы);

механические воздействия на технические средства (удары и вибронагрузка).

Электрические факторы среды функционирования включают:

качество и надежность электропитания системы;

заземление оборудования;

электромагнитные помехи.

Целесообразно более подробно остановиться на электрических факторах среды функционирования АБС, т.к. они представляют несомненную угрозу безопасности информации при несоблюдении определенных стандартизированных правил и условий (см. разделы 2.1 и 2.5). Соблюдение этих правил и условий позволяет одновременно решать проблемы раскрытия информации из-за

утечки по каналам электромагнитных излучений и наводок, обеспечивает безотказное функционирование АБС при различных флуктуациях в сети электропитания. Одновременное или совместное решение различных проблем с помощью единых средств существенно снижает затраты по защите информации.

Рассмотрим эти положения на конкретных примерах. С развитием мобильных средств электросвязи (радиотелефон) повсеместно в развитых странах стали отмечаться случаи негативного воздействия мощных электромагнитных полей связных передатчиков на близко расположенную вычислительную технику, которые выражались в сбоях или неустойчивой работе ЭВМ. В результате Международная электротехническая комиссия (МЭК) выпустила стандарт МЭК 801/1000-4, который распространяет свои требования на радиоэлектронные и электронные изделия, которые могут в условиях эксплуатации подвергаться воздействию радиочастотных электромагнитных полей. Отечественным аналогом этого стандарта является ГОСТ Р50008-92 "Совместимость технических средств электромагнитная. Устойчивость к радиочастотным электромагнитным полям в полосе 26-1000 МГц. Технические требования и методы испытаний". Основным средством защиты от подобных воздействий или электромагнитных помех служит электромагнитное экранирование, которое одновременно решает, например, проблемы защиты информации на экране монитора, которая распространяется или - раскрывается за счет электромагнитных излучений.

Знание требований документа РД 50 714-92 "Уровни электромагнитной совместимости в низковольтных системах электроснабжения общего назначения в части низкочастотных кондуктивных помех и сигналов, передаваемых по силовым линиям" позволяет квалифицированно заказывать СВТ электронного банка, устойчиво работающее при электропитании от отечественных силовых электросетей. Исследование нескольких отечественных питающих сетей показали, что относительное время аварийной работы сетей электропитания составляет до 10 %. По видам нарушений картина следующая: падение напряжения за пределы допустимых значений - 50 %, повышение напряжения - 10 %, отключение питания - 20 %, броски напряжения - 5 %. Самыми

опасными являются кратковременные высоковольтные броски напряжения, обычно возникающие из-за отключения индуктивной нагрузки.

Учитывая указанные обстоятельства, для всех отечественных АБС целесообразно использовать источники бесперебойного питания или Uninterruptable power supply (UPS), которые обеспечивают защиту от данных нарушений. Следует учесть, что при авариях в электросетях UPS обеспечивают качественное электропитания в течение нескольких минут, необходимых для успешного завершения вычислительного процесса и создания условий для его последующего восстановления. Для компенсации более длительных аварий необходимо применять более радикальные средства, например, дизель-генераторы.

Обычно не вызывает сомнений необходимость качественного заземления технических средств АБС, что является не простой проблемой.

В материалах фирмы DEC также уделено внимание правильной установке и обслуживанию СВТ системы, хранению и использованию носителей информации. Также рассматриваются меры по защите АБС от стихийных бедствий и мероприятия по физической безопасности системы.

4.3. Пластиковые идентификационные карточки в автоматизированных банковских системах

В последнее время в различных отечественных банках стали применяться системы электронных платежей на основе пластиковых идентификационных карточек (ИК). Следует отметить, что они в большинстве случаев упоминаются под различными названиями: кредитные карточки, смарт-карты или "пластиковые деньги" и т.п. Название ИК более всего сооответствует международным стандартам и основной их функции.

Сами по себе ИК не функционируют и являются составной частью различных АСОД. ИК предназначены для осуществления взаимодействия человека с АСОД. ИК могут быть определены как аппаратное средство АСОД в виде прямоугольной пластиковой карточки, предназначенное для идентификации субъекта системы и являющееся носителем идентификационной и другой информации. Такое определение подчеркивает основные свойства ИК, характерные для всех их разновидностей.

Идентификация - это процесс распознавания определенных компонентов системы (субъектов и объектов) с помощью уникальных, воспринимаемых системой имен (идентификаторов). Практическая идентификация пользователей заключается в установлении и закреплении за каждым пользователем АСОД уникального идентификатора (признака) в виде номера, шифра, кода и т.д. Это связано с тем, что традиционный идентификатор вида ФАМИЛИЯ-ИМЯ-ОТЧЕСТВО не всегда приемлем для применения в АСОД. Поэтому в различных автоматизированных системах широко применяется персональный идентификационный номер (ПИН) или в английской транскрипции personal identification number (PIN).

ПИН обычно состоит из 4 - 12 цифр и вводится идентифицируемым пользователем с клавиатуры. На практике встречаются назначаемые или выбираемые ПИН [2]. Последний устанавливается пользователем самостоятельно. Назначаемый ПИН устанавливается уполномоченным органом АСОД. Выбор типа ПИН и порядка его использования определяется важностью его применения для обеспечения безопасности информации в АСОД посредством проверки подлинности (аутентификации) пользователей по предъявляемому идентификатору, например, при входе в систему.

Отсутствие надежных средств проверки пользователей может существенно затруднить определение персональной ответственности за нарушение безопасности информации в системе. Идентификация и проверка подлинности являются важными составными частями подсистемы управления доступом в АСОД.

На практике существуют два основных способа проверки ПИН: алгоритмический и неалгоритмический. Алгоритмический способ проверки заключается в том, что у пользователя запрашивается ПИН, который преобразуется по определенному алгоритму с использованием секретного ключа и затем сравнивается со значением ПИН, хранящимся на карточке с соблюдением необходимых мер защиты. Главным достоинством этого метода проверки является отсутствие необходимости интерактивного (режим on-line) обмена информацией в системе. Неалгоритмический способ проверки ПИН не требует применения специальных алгоритмов. Проверка ПИН осуществляется путем прямого сравнения ПИН на карте со значением, хранимым в базе данных, что реализуется в режиме on-line. Это обязывает использовать средства связи, работающие в реальном масштабе времени, и предусматривать средства защиты информации в базе данных и линиях телекоммуникаций. Идентификатор используется при построении различных подсистем разграничения доступа.

ИК применяется для обеспечения безопасности информации в АСОД посредством проверки подлинности (аутентификации) пользователей по предъявляемому идентификатору, например, при входе в автоматизированную систему. Отсутствие надежных средств проверки подлинности пользователей может существенно затруднить определение персональной ответственности за нарушение безопасности ценной информации в АСОД.

Любая ИК является в качестве носителя информации, необходимой для идентификации, и информации, используемой в других целях. Эта информация представляется в различных формах: графической, символьной, алфавитно-цифровой, кодированной, двоичной. Множество форм представления информации на ИК объясняется тем, что карточка служит своеобразным связующим звеном между человеком (пользователем) и машинной системой, для которых характерны различные формы представления информации.

Например, на карточку графически наносят специальный логотип, рисунок, фотографию, фамилию владельца, серийный номер, срок годности, штрих-код и т.п.

Логотип - графический символ организации, выпускающей карточку. Логотип служит своеобразным знаком обслуживания, т.е. обозначением, дающим возможность отличать услуги одной организации от однородных услуг другой организации. Очевидно, что логотип должен обладать различительной способностью и не повторять общеупотребительные обозначения (гербы, флаги и т.п.). Эта информация способствует правильной идентификации и проверке подлинности ИК и ее владельца. Для обеспечения безопасности изображение, в том числе голографическое или видимое только в инфракрасных лучах, наносят на специальном оборудовании, что существенно затрудняет подделку карточки.

Другим средством повышения безопасности визуальной информации служит тиснение или выдавливание (эмбоссирование) некоторых идентификационных характеристик пользователя на поверхности ИК. Эти характеристики с помощью специального устройства (импринтера) могут отпечатываться и дублироваться на бумажном носителе (слипе) для дальнейшего учета. Упомянутая идентификационная информация в двоичной форме заносится в носитель цифровой информации ИК. Способ технической реализации носителя информации в цифровой форме является важнейшим критерием систематизации ИК.

В настоящее время нашли широкое применение магнитные, полупроводниковые и оптические карточки, перечисленные в порядке снижения распространенности.

Последние выделяются большой информационной емкостью от 4 Мб до 200 Мб. При их производстве используется WORM - технология (write once read more), подобная той, что применяется в лазерных дисках. Карточки устойчивы к внешним воздействиям: например, карточку DREXON(R) Laser Card(R) можно "варить" в кипящей воде до 1000 часов без потери хранящейся на ней информации. Они обладают также высокой степенью защищенности от подделки, обусловленной сложной технологией производства. Информация на эти ИК заносится при изготовлении и может только считываться. Указанные свойства оптических карточек позволяют их использовать, например, в качестве ключа доступа к данным в АСОД. Это самые дорогие и малораспространенные карточки среди рассматриваемых.

Наиболее распространенными в мире (около миллиарда штук) являются магнитные идентификационные карты (МИК), в которых магнитная полоса служит в качестве носителя информации в цифровой форме. Согласно стандарту международной организации по стандартизации ISO 7811-1/5:1985 на магнитной полосе выделяются три дорожки, одна из которых (третья) предназначена для перезаписи данных, а остальные две используются преимущественно для идентификационных целей. На практике третья дорожка мало используется для перезаписи информации, т.к. данный процесс малонадежен и дорог. Вместо этого прибегают к элементам бумажной технологии, используя ранее отмеченные эмбоссирование и слипы.

Особенно это касается МИК, изготовленных из поливинилхлорида, механические характеристики которого оставляют желать лучшего. Кроме того, под действием ультрафиолетовых лучей эта пластмасса старится и начинает крошиться, магнитный слой с карточки легко осыпается.

В настоящее время динамично развиваются полупроводниковые идентификационные карточки (ПИК) с интегральной схемой и металлическими контактами, в которых полупроводниковый кристалл (чип) используется в качестве носителя цифровой информации или элемента памяти, а также может выполнять сложные логические функции.

В ПИК, в соответствии со стандартом ISO 7816-1:1988, заложено восемь металлических контактов с золотым покрытием для обеспечения надежности контактирования с аппаратурой сопряжения АСОД. В настоящее время используется 4 - 6 контактов.

Остальные являются запасными. Карточки с полупроводниковым кристаллом бывают различных типов: с незащищенной и с защищенной памятью. Карточки второго типа содержат микроконтроллер, предотвращающий несанкционированный доступ к данным на карте. В карточках с защищенной памятью используется специальный механизм разрешения операций чтения/записи или стирания информации. Чтобы провести эти операции, надо предъявить для карточки секретный ключ. Чтение

записанных в память карточки ключей защиты или копирование памяти карточки невозможно без знания специального ключа.

Рис. 1. Структурная схема карточки с защищенной полупроводниковой памятью

В областях памяти, позволяющих перезаписывать информацию, используется электрически стираемое программируемое постоянное запоминающее устройство (ЭСППЗУ), записываемое в английской транскрипции как EEPROM. Структурная схема карточки с защищенной полупроводниковой памятью приведена на рис. 1. Карточки с простой незащищенной памятью используются в различных системах с малоценной информацией (система оплаты за проезд на городском транспорте, пользование телефоном и т.д.) не требующей серьезной защищенности. Данный тип карточек применяется для такого типа операций, когда требуется дискретное снижение ранее заданной в памяти величины. Их часто называют карточками-счетчиками.

Встречаются ПИК неполностью отвечающие всем требованиям указанных международных стандартов. Например, ПИК (семейство приборов DS 199X Touch Memory) американской фирмы Dallas Semiconductor имеют нестандартную толщину 5,8 мм (корпус F5) или 3,2 мм (корпус F3) толщину и оригинальные электрические параметры двухпроводного интерфейса.

Приборы Touch Memory представляют собой энергонезависимую статическую память с многократной записью/чтением, которая размещается внутри металлического корпуса. В отличие от обычной памяти с параллельным портом адреса/данных, память приборов Touch Memory имеет последовательный интерфейс. Данные записываются/читаются в память по одной двунаправленной сигнальной линии. По этой линии в прибор передаются команды и данные, считываются данные. При этом используется широтно-импульсный метод кодирования. Логические сигналы "1" и "0" с уровнем от +5 В до 0 В передаются импульсами различной длительности. Такой цифровой интерфейс позволяет подключать приборы Touch Memory непосредственно к персональным ЭВМ или через микропроцессорный контроллер.

Важной особенностью приборов является низкая потребляемая мощность, что позволяет использовать встроенную в корпусе прибора миниатюрную литиевую батарейку для сохранения информации в памяти в течение 10 лет.

Каждый прибор семейства является уникальным, так как имеет свой собственный серийный номер, который записывается в прибор с помощью лазерной установки во время его изготовления и не может быть изменен в течение всего срока службы прибора.

Одним из основных отличий приборов Touch Memory от других компактных носителей информации является конструкция корпуса. Помимо защиты стальной корпус выполняет также роль электрических контактов. Он аналогичен по конструкции корпусу стандартной батарейки - состоит из ободка с донышком и электрически изолированной крышки. В отличие от обычных микросхем доступ к прибору осуществляется только через две линии: земляную и двунаправленную сигнальную. Ободок и

донышко представляют собой земляной контакт, а крышечка выполняет функцию сигнального контакта. В семейство Touch Memory входят 5 приборов идентичных по конструкции корпуса, интерфейсу, но отличающихся типом и объемом памяти, а также методом доступа к ней.

В табл. 1 приведены некоторые данные по типам и объемам памяти приборов DS 199X, а также информация о ее защищенности и методам доступа к ней.

Таблица 1

Тип прибора	Объем блокнотной памяти, байт	Объем основной памяти, байт	Наличие защиты памяти по ключу	Команды оперативной памяти		Команды установки паролей
				чтение	запись	запись
DS1991	64	192	+	+	+	+
DS1992	32	128	-	+	-	-
DS1993	32	512	-	+	-	-
DA1994	32	512	-	+	-	-

Все приборы семейства имеют в своем составе постоянную память объемом 64 бита для хранения серийного номера. Эта память содержит 8-битный код типа прибора, 48-битный серийный номер и 8-битный код контроля с циклической избыточностью (CRC).

Прибор DS1990 содержит только постоянную память. Все остальные приборы семейства дополнительно к постоянной памяти имеют в своем составе энергонезависимую перезаписываемую память объемом от 1K до 4K бит. Память разделена на отдельные страницы по 256 бит для DS1992, DS1993, DS1994 и 384 бита - для DS1991.

Для повышения надежности записи в приборах Touch Memory используется дополнительная блокнотная память.

Память приборов DS1992, DS1993 и DS1994 доступна как по чтению, так и по записи. Приборы DS1991 имеют защищенную память с более сложной архитектурой.

DS1991 содержит три независимых страницы памяти. Они защищены по чтению и записи с помощью механизма паролей, который обеспечивает надежную защиту памяти от несанкционированного изменения ее содержимого, что в ряде применений крайне важно.

Следует отметить, что в последнее время в компактной электронной аппаратуре стали часто использовать карточки памяти (memory card) PCMCIA-типа по одноименному названию Международной ассоциации производителей плат памяти персональных компьютеров. Эти карточки используются для наращивания памяти запоминающих устройств, имеют разъемные соединения и не соответствуют полностью требованиям международных стандартов по ИК . Их внешние размеры 85,8 x 54 x 5,5 мм близки к габаритам ИК, что иногда способствует путанице.

Последнее достижение в области ИК с полупроводниковой интегральной схемой представляет собой карточка с микропроцессором, которая обладает следующими основными характеристиками: тактовая частота до 5 Мгц; емкость ОЗУ до 256 байт; емкость ПЗУ до 10 Кбайт; емкость перезаписываемой энергонезависимой памяти до 8 Кбайт.

Перечисленные характеристики напоминают соответствующие показатели первых персональных компьютеров. Учитывая, что современная микроэлектроника еще не достигла фундаментальных ограничений в области интегральной полупроводниковой технологии, можно предвидеть дальнейшее развитие ИК с интегральной микросхемой и металлическими контактами.

Появление идентификационных карточек с микропроцессором (ИКМ) позволило сделать рывок в совершенствовании автоматизированных систем обработки данных. Возникла возможность работы АСОД и ИКМ в режиме пакетной передачи данных off-line, наряду с интерактивным режимом on-line, что

позволяет существенно улучшить показатели безопасности информации подсистемы передачи данных.

Значительно возросла безопасность информации самой карточки. В микропроцессор встраивается специализированная операционная система, обеспечивающая большой набор сервисных операций и средств безопасности. Например, специальная операционная система ИКМ поддерживает файловую систему, предусматривающую разграничение доступа к информации. Для информации, хранимой в любой записи (файл, каталог), могут быть установлены следующие режимы доступа:

1) всегда доступна по чтению/записи;

2) доступна по чтению, но требует специальных полномочий для записи в виде предъявления специального секретного кода;

3) специальные полномочия по чтению/записи в виде предъявления специальных секретных кодов;

4) недоступна. Этот режим не разрешает читать или записывать информацию, которая доступна только внутренним программам карточки для записей, содержащих криптографические ключи.

В ИКМ могут встраиваться криптографические средства, обеспечивающие шифрование информации и выработку "цифровой подписи". Кроме того, могут применяться средства ведения ключевой системы.

В литературе часто встречается нестандартный термин “интеллектуальная” или “разумная” (smart) карта, который подразумевает ИК с интегральной схемой, содержащей микроконтроллер (защищенная память) или микропроцессор .

В табл. 2 приведены некоторые данные по защищенности смарт-карт различных типов с микропроцессором и памятью (ИКП). В столбце "Разграничение доступа" указывается количество зон на карточке, доступ к которым может быть разграничен на основе ключей.

Таблица 2

Фирма-изготовитель	Название карты	Тип карты	ПИН	Спец. набор команд
GEMPLUS CARD INTERNATIONAL	GPM103	ИКП	Нет	Нет
-"-	GPM416	-"-	Есть	-"-
-"-	COS16K	ИКМ	-"-	Да
-"-	PCOS	-"-	-"-	-"-
SOLAIC	E3744	ИКП	-"-	Нет
SCHLUMBERGER TECHNOLOGIES	M16E	ИКМ	-"-	-"-
-"-	ME2000	-"-	-"-	Да

Рассматриваемые карточки отвечают требованиям физической безопасности, изложенным в международном стандарте. Например, требования касаются устойчивости к воздействию ультрафиолетового и рентгеновского облучения, механических нагрузок, электромагнитных полей и статического электричества. Последнее требование весьма важно, учитывая условия хранения и эксплуатации ИК, а также техническую сложность его реализации.

Целесообразно также перечислить оригинальные ИК, которые не получили широкого распространения из-за сравнительно высокой стоимости или не полного соответствия международным стандартам. К ним можно отнести следующие ИК: с перфорацией для оптического считывания информации, штрих-кодовые, на полупроводниковых элементах фирмы DS (рассмотренные ранее), суперинтеллектуальные и карточки с радиоканалом обмена данными. Две последние являются оригинальными смарт-картами. В суперинтеллектуальные ИК встроены клавиатура и жидкокристаллический дисплей. ИК с радиоканалом осуществляют обмен данными в АСОД по радио, без электрических контактов, на расстоянии до нескольких метров.

Встречаются также ИК, совмещающие различные носители данных. В частности, нашли практическое применение ИК, совмещающие магнитную полосу и интегральную схему с

металлическими контактами, что позволяет решить проблему функциональной совместимости карточек различных типов.

ИК нашли широкое применение в различных АСОД обороны и народного хозяйства. Самое большое распространение карточек наблюдается в финансовой сфере.

Можно условно выделить три переплетающиеся области применения ИК:

1) электронные документы;

2) контрольно-регистрационные системы;

3) системы электронных платежей.

Карточки как средство контроля, разграничения и регистрации доступа к объектам, устройствам, информационным ресурсам АСОД используются при создании контрольно-регистрационных охранных систем. Например, известны разнообразные электронные замки к помещениям и аппаратуре. Разграничение доступа к данным ПЭВМ реализовано на уровне предъявления ключ-карты, содержащей идентификационные данные пользователя и его электронный ключ.

ИК являются ключевым элементом различных систем электронных платежей, в которых применяется около 1 миллиарда карточек.

4.4. Нормативные материалы и стандарты

С созданием современных электронных банков резко возросла роль унификации и стандартизации элементов и алгоритмов функционирования АБС. Особую роль стандартизация играет при обеспечении безопасности информации электронных банков, чему способствует деятельность международных организаций МОС (ISO) и МККТТ (CCITT).

В Международной организации стандартов МОС выработкой единой идеологии в сложном комплексе вопросов обеспечения информационной безопасности занимается Подкомитет ПК27 "Информационные технологии. Методы и средства защиты информации".

В частности, в 1987 году был принят стандарт ISO/IEC8372:1987 "Режимы работы 64-битного блочного алгоритма шифрования", основные положения которого были учтены при разработке отечественного стандарта ГОСТ 28147-89 "Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования". Другой стандарт ISO/IEC9797:1989 "Криптографические методы защиты. Механизм удостоверения целостности данных, использующий криптографическую проверочную функцию на базе блочного алгоритма шифрования" определяет механизмы, позволяющие удостовериться в том, что в процессе хранения или пространственной транспортировки произвольного информационного объекта, в нем не возникло каких-либо искажений случайного характера, или искажений (нарушений целостности) информации, вызванных преднамеренными действиями злоумышленников. Вторая цель достигается за счет применения (при формировании проверочной величины - "контрольной суммы" информационного объекта) алгоритма шифрования с секретным ключом, неизвестным потенциальному нарушителю.

Перечень основных финансовых стандартов ISO приведен в работе [22].

Необходимо отметить, что международная стандартизация финансовых документов была начата еще в 70-е годы в рамках двух организаций [22]:

ANSI (American National Standarts Institute);

SWIFT (Society for Worldwide Interbank Financial Telecommunication).

В настоящее время вопросы защиты информации непосредственно затрагиваются в упомянутом техническом подкомитете ПК27 и ряде других подразделений ISO:

ОТК1/ПК6 "Телекоммуникация и обмен информацией между системами";

ОТК1/ПК17 "Идентификационные и кредитные карточки";

ОТК1/ПК18 "Учрежденческие автоматизированные системы и обработка текстов";

ОТК1/ПК21 "Поиск, передача и управление информацией в открытых системах";

ТК68/ПК2 "Банковские операции и прцедуры";

ТК68/ПК6 "Автоматизированные системы денежных расчетов на базе электронных карточек".

Например, по рекомендациям МККТТ X800 [8] был выпущен стандарт ISO 7498-2 "Принципы защиты информации в открытых системах по модели OSI".

Примеры других отечественных стандартов, касающихся рассматриваемой темы, были приведены в предыдущих разделах.

Отечественные нормативные документы, касающиеся защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники стали выпускаться в начале 90-х годов [3-7]. Их основные организующие положения подкреплены Указом Президента Российской Федерации [21]. Эти вопросы отмечались фрагментарно в некоторых ранее выпущенных стандартах:

ГОСТ 24.104-85 "Единая система стандартов автоматизированных систем управления. Автоматизированные системы управления. Общие требования";

ГОСТ 34.601-90 "Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы.Стадии создания.";

ГОСТ 34.601-89 "Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы.".

5. ЗАКЛЮЧЕНИЕ

Данный материал не претендует на полное изложение всех вопросов рассматриваемой темы и является краткой систематизацией положений проблемы обеспечения комплексной безопасности информации в современных, отечественных автоматизированных системах. В основе решения обозначенной задачи должен находиться системный подход, который использует весь жизненный цикл подсистем бозопасности информации. Главными критериями выбора тех или иных решений по защите информации является их техническая эффективность и стоимость.

Выше изложенное базировалось на следующих позициях, позволяющих существенно уменьшить стоимость и сроки создания подсистем обеспечения комплексной безопасности информации АБС:

максимальное использование имеющегося научно-технического задела и опыта специалистов, работающих в данной прикладной области техники в государственной сфере;

улучшение показателей надежности и безотказности функционирования электронного банка;

обеспечение высококачественного аудита автоматизированного банка.

Необходимо отметить отечественную специфику решения проблемы обеспечения комплексной безопасности информации электронного банка, которая заключается в двух противоречивых и взаимозависимых факторах. Во-первых, острой юридической проблемой является отсутствие в настоящее время достаточной правовой базы. Во-вторых, обострение криминогенной обстановки в стране. По мнению Алена Доскара, представителя регионального отделения американской корпорации "VISA CARD" в Европе, уровень мошенничества в России с расчетно-кредитными пластиковыми карточками "VISA" в 4-5 раз превышает среднемировой.

Последние государственные документы в области защиты информации [6,21] способствуют решению указанных проблем, устанавливая основные принципы и организационную структуру в области защиты информации. Они предназначены для государственных органов власти, организаций, предприятий, банков и иных учреждений, расположенных на территории Российской Федерации, независимо от их ведомственной принадлежности и форм собственности.

ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА

1. Коффей Маргарет. Банки в поисках способов борьбы с электронными мошенниками. Финансовые известия N 4, 19 ноября 1992г., стр. 8.

2. В.Гайкович, А.Першин. Безопасность электронных банковских систем. Изд. Единая Европа, М.: 1994.

3. Гостехкомиссия России. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированногодоступа к информации. М.; 1992.

4. Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. М., 1992.

5. Гостехкомиссия России. Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники. М., 1992.

6. Положение о государственном лицензировании деятельности в области защиты информации. Решение N 70 Гостехкомиссии и ФАПСИ от 27.04.94, М., 1994.

7. Гостехкомиссия России. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. М., 1992.

8. Security Architecture for open Systems Interconnection. Recommendation X800, ICCTT, 1991.

9. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. М.: Энергоатомиздат, 1994, 400стр.

10. Устинов Г.М. Обеспечение безопасности информации при ее передаче в телематических службах. Технология электронных коммуникаций. ЭКОТРЕНДЗ, т.33, М., 1993.

11. К.Н.Маркелов. Автоматизированные банковские системы в России. Банковские системы и оборудование. N 1 1994г., стр. 7-16.

12. Digital и банки. Материалы для руководства банков. 1994, 12 с.

13. Закон Российской Федерации от 2 декабря 1990 г. "О банках и банковской деятельности".

14. Ю.А.Стрельченко. Обеспечение информационной безопасности банков. Методическое пособие. М.: ИПКИР, 1994, 120с.

15. Барсуков В.С., Дворянкин С.И., Шеремет И.А. Безопасность связи в каналах телекоммуникаций. Технологии электронных коммуникаций. ЭКОТРЕНДЗ, т20, М., 1992.

16. Защита информации в компьютерных системах. Теоретические аспекты защиты от вирусов/ Под. ред. профессора Э.М.Шмакова. С.-Птб, 1993, 101 с.

17. Викторов А.Д. и др. Аппаратно-программная реализация комплекса для перехвата и защиты электромагнитных излучений технических средств персонального компьютера. Безопасность информационных технологий. N 1, 1994, стр. 75-79.

18. Петров А.В., Пискарев А.С.,Шеин А.В. Информационная безопасность. Защита информации от несанкционированного доступа в автоматизированных системах. Уч. пособие/ Под. ред. А.А.Малюка. М.: МИФИ, 1993, 80 с.

19. Горбатов В.С., Кондратьева Т.А. Информационная безопасность. Основы правовой защиты. Уч. пособие. М.: МИФИ, 1995, 52 с.

20. Новые пластиковые деньги/ Под. ред. А.В.Спесивцева. М., 1994, с.126.

21. Указ Президента Российской Федерации от 3 апреля 1995 года, N 334 "О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации".

22. Автоматизация расчетных операций банков и фондовых бирж. Церих-ПЭЛ., М., 1992, 206 с.

23. Электронный обмен коммерческими и финансовыми данными. Технологии электронных коммуникаций. ЭКОТРЕНДЗ, т15, М., 1991.

СИСТЕМА ЗАЩИТЫ ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ НА ОСНОВЕ ОС Novell NetWare

"Secret NET"

Назначение системы защиты

Система защиты "Secret Net" (далее по тексту Система защиты) предназначена для обеспечения защиты хранимой и обрабатываемой в локальной вычислительной сети (ЛВС) информации от несанкционированного доступа (ознакомления, искажения, разрушения) и противодействия попыткам нарушения нормального функционирования ЛВС и прикладных систем на ее основе.

В качестве защищаемого объекта выступает ЛВС персональных ЭВМ типа IBM PC/AT и старше, работающих под управлением операционной системы MS DOS версий 3.30-6.2 (рабочие станции) и сетевой операционной системы Novell Netware 3.1x (файловые серверы), объединенных при помощи сетевого оборудования Ethernet, Arcnet или Token-Ring.

Максимальное количество защищенных рабочих станций 256

Максимальное количество защищенных файловых серверов 8

Максимальное количество уникально идентифицируемых пользователей сети..... 255

Состав и функции системы защиты

Основные задачи, решаемые Системой защиты

Система защиты позволяет решать следующие задачи:

защита от лиц, не допущенных к работе с системой обработки информации;

регламентация (разграничение) доступа законных пользователей и программ к информационным, программным и аппаратным ресурсам системы в строгом соответствии с принятой в организации политикой безопасности;

защита ЭВМ сети от внедрения вредоностных программ (закладок), а также инструментальных и технологических средств проникновения;

обеспечение целостности критических ресурсов Системы защиты и среды исполнения прикладных программ;

регистрация, сбор, хранение и выдача сведений обо всех событиях, происходящих в сети и имеющих отношение к ее безопасности;

централизованное управление средстванми Системы защиты.

Функциональный состав Системы защиты

Для решения перечисленных выше задач Система защиты включает следующие подсистемы (ПС):

идентификации и аутентификации пользователей;

разграничения доступа к ресурсам;

контроля целостности;

регистрации;

управления средствами защиты (администрирования).

ПС идентификации и аутентификации пользователей предназначена для установления достоверного соответствия между пользователем, пытающимся войти в систему и конкретным зарегистрированным в системе и имеющим определенные права субъектом доступа.

ПС разграничения доступа предназначена для управления доступом поименованных субъектов к поименованным объектам системы (разрешения в случае наличия соответствующих полномочий и отказа в доступе к объекту в случае отсутствия таковых).

ПС контроля целостности предназначена для контроля целостности программ и данных самой Системы защиты, а также среды исполнения прикладных программ.

ПС регистрации предназначена для сбора и хранения необходимых данных обо всех событиях, происходящих на ЭВМ сети и имеющих отношение к ее безопасности.

ПС управления средствами защиты предназначена для обеспечения работы администратора по управлению всеми подсистемами Системы защиты, назначению и изменению полномочий пользователей и меток безопасности объектов, анализу журналов регистрации событий безопасности.

По требованию заказчика в состав Системы защиты может быть включена криптографическая подсистема, предоставляющая услуги по шифрованию конфиденциальной информации в соответствии с ГОСТ 28147-89.

Функции подсистем Системы защиты

Подсистема идентификации и аутентификации

Подсистема выполняет функцию идентификации/аутентификации (проверки подлинности) пользователя при каждом его входе в Систему, а также после каждой приостановки его работы

(специальной временной блокировки работы ПЭВМ по инициативе пользователя). Для идентификации в Системе каждому пользователю присваивается уникальное имя. Обеспечивается работа с именами длиной до 12 символов (символов латинского алфавита и специальных символов). Вводимое имя отображается на экране рабочей станции.

Проверка подлинности пользователя осуществляется после его идентификации для подтверждения того, что пользователь действительно является тем, кем представился. Она не является обязательной (пользователь может не иметь пароля, если это определено для него администратором). Проверка подлинности пользователя осуществляется путем проверки правильности введенного пароля. Поддерживается работа с паролями длиной до 16 символов. Вводимый пароль не отображается на экране рабочей станции.

При неправильно введенном пароле на экран выдается сообщение об ошибке и подается звуковой сигнал. При трехкратном неверном вводе пароля блокируется клавиатура, выдается сообщение о попытке НСД на сервер управления доступом и осуществляется оперативное оповещение администратора безопасности, регистрируется попытка НСД в системном журнале и выдается звуковой сигнал.

Пароли администратора и всех пользователей системы хранятся в зашифрованном виде, и могут быть изменены как администратором безопасности, так и конкретным пользователем (изменение только своего пароля) при помощи специальных программых средств. В том случае, если пользователю разрешено работать на любой из группы рабочих сети (заданных администратором), его имя и пароль на всех этих станциях всегда одинаковы.

Предусмотрен вариант входа пользователя в систему с рабочих станций под специальным именем (предлагаемом ему по умолчанию) без необходимости предъявления пароля. В этом случае пользователь получает соответствующие данному пользователю полномочия.

Для повышения защищенности идентификация/аутентификация пользователя может проводиться до загрузки операционной системы. Это обеспечивается специальным техническим устройством (микросхемой ПЗУ или платой Secret Net Card).

Подсистема разграничения доступа

ПС разграничения доступа реализует концепцию диспетчера доступа, при которой ПС является посредником при всех обращениях субъектов к объектам доступа (попытки обращения к объекту в обход ПС приводят к отказу в доступе). Подсистема разграничения доступа может работать в одном из двух режимах функционирования: основном и технологическом.

Технологический режим предназначен для точного определения объектов, к которым должен иметь доступ пользователь, и прав доступа к ним. При работе в технологическом режиме Система защиты только регистрирует все попыткм доступа к защищаемым ресурсам в системном журнале и выдает предупреждающие сообщения на экран.

В основном режиме Система защиты не только регистрирует попытки доступа к защищаемым ресурсам, но и блокирует их.

Перечень контролируемях объектов доступа

Подсистеиа обеспечивает контроль доступа субъектов к следующим объектам:

физическим и логическим устройствам (дискам, принтерам);

каталогам дисков;

файлам;

физическим и логическим секторам дисков.

В подсистеме реализована сквозная иерархическая схема действия прав доступа к локальным объектам рабочей станции, при

которой объект нижнего уровня наследует права доступа объектов доступа верхних уровней (диск-каталог-файл).

Любой объект на рабочей станции может обладать меткой безопасности. Метка безопасности указывает, какие операции может произвести субъект над данным объектом, кто является его владельцем, а также признак, разрешающий программе (если данный объект-программа) работу с физическими секторами дисков. Метка безопасности заполняется при создании объекта и может корректироваться как пользователем-владельцем объекта, так и администратором.

Каждый пользователь обладает индивидуальными правами доступа к ресурсам компьютера-меткой безопасности, устанавливаемой по умолчанию на все создаваемые им новые объекты.

Права доступа пользсвателя к объектам системы хранятся в его "паспорте". Паспорт пользователя представляет собой некую структуру, недоступную самому пользователю и корректируемую только администратором.

Права доступа пользователя к объектам системы могут принимать следующие значения:

запрет доступа. При таком уровне доступа к объекту пользователь не имеет возможности выполнять с объектом какие-либо действия;

наличие доступа. В этом случае уровень доступа может быть одним из следующих:

доступ на чтение. При таком уровне доступа субъект доступа может лишь читать содержимое объекта;

доступ на запись. В этом случае возможно изменение содержимого объекта или удаление объекта.

доступ на исполнение. В этом случае субъект может только запустить объект на исполнение. Запрещается как запись в объект, удаление, переименование объекта, так и чтение содержимого объекта.

Обеспечивается возможность совмещения приведенных выше прав доступа.

Управление доступом

Управление доступом к локальным логическим и физическим дискам осуществляется при помощи информации о доступе, помещаемой в паспорт пользователя при его создании администратором. Управление доступом к удаленным дискам, каталогам и файлам осуществляется администратором системы при помощи утилит системы разграничения доступа сетевой ОС Novell NetWare v3.1x.

Управление доступом к локальным каталогам и файлам осуществляется путем сравнения меток безопасности субъекта и объекта доступа.

По умолчанию доступ на уровне физических (логических) секторов запрещен. В этом случае, когда программе необходим для работы доступ к диску на уровне логических (физических) секторов администратор должен специально вносить соответствующий признак в метку безопасности данной программы.

Пользователь не имеет возможности изменять собственные права доступа, атребуты доступа и владения объектами, владельцем которых он не является. Пользователь не имеет возможности расширять права доступа других пользователей к ресурсам системы, а также менять имена, права доступа и владельцев тех объектов, к которым он не допущен.

Пользователю предоставлена только возможность назначения прав доступа других пользователей к принадлежащим ему (созданным им) объектам.

Для реализации избирательного управления доступом подсистема поддерживает замкнутую среду доверенного программного обеспечения (при помощи индивидуальных для каждого пользователя списков программ, разрешенных для запуска). Создание и ведение списков программ возложено на администратора. Для этого в его распоряжении имеется специальные программные средства.

Для совместного использования программ и данных Система защиты предусматривает возможность объединения пользователей в группы. Права доступа группы наследуются всеми пользователями этой группы.

Максимальное количество групп - 255.

Максимальное количество пользователей в одной группе - 255.

Каждый пользователь одновременно может входить в 32 группы.

Подсистема разграничения доступа обеспечивает регистрацию в системном журнале обращений к ресурсам системы и всех попыток нарушения установленных правил доступа.

Подсистема контроля целостности

В системе контролируется целостность следующих объектов: операционные системы локальных рабочих станций, программ Системы защиты, файлов паспортов пользователей и системных областей локальных дисков рабочих станций, а также файлов пользователей (по требованию пользователей).

Контроль целостности файлов осуществляется методом контрольного суммирования с использованием специального алгоритма. Для контроля целостности и восстановления системных областей жесткого диска в защищенной области хранятся их копии.

Контроль целостности программ Системы защиты производится периодически администратором. Для этого ему предоставлены соответствующие программные средства.

В случае обнаружения нарушения целостности контролируемых объектов производится регистрация этого события в системном журнале и оперативное оповещение администратора. В случае нарушения целостности системных областей диска, кроме того, производится их восстановление с использованием резервных копий.

Подсистема регистрации событий безопасности

При функционировании Системы защиты все ее подсистемы для регистрации событий безопасности, входящих в область их компетенции, используют возможности единой подсистемы регистрации.

Подсистема регистрации обеспечивает:

ведение и анализ журналов регистрации событий безопасности (системных журналов). Журнал регистрации ведется для каждой рабочей станции сети;

оперативное ознакомление администратора с системным журналом любой станции и с журналом событий об НСД;

получение твердой копии системного журнала;

преобразование содержимого системных журналов в формат DBF для их дальнейшего анализа;

объединение системных журналов и их архивирование;

оперативное оповещение администратора о нарушениях безопасности.

Регистрация событий осуществляется как при наличии сервера управления доступа, так и при его отсутствии, а оповещение производится независимо от того, работает ли пользователь в сети.

Регистрация событий безопасности

Регистрация событий производится путем записи необходимой информации в системный журнал. Системный журнал доступен для чтения только администратору. Разграничение доступа к системным журналам обеспечивается подсистемой управления доступом.

В целях обеспечения единого отсчета времени на всех рабочих станциях сети осуществляется синхронизация времени при обращении станций к серверу доступа при их начальной загрузке.

Инфорамация о событиях безопасности

При регистрации событий безопасности в системном журнале фиксируется следующая информация:

дата и время события;

идентификатор субъекта (пользователя, программы), осуществляющего регистрируемое действие;

действие (если регистрируется запрос на доступ, то отмечается объект и тип доступа).

В системный журнал заносятся сведения более чем о 50 событиях, происшедших как с локальными, так и сетевыми объектами. Подсистема поддерживает четыре уровня регистрации.

Системные журналы формируются на локальных дисках рабочих станций. Перенос их на файловый сервер осуществляется при начальной загрузке этих рабочих станций, либо при подключении пользователя к сети, или оперативно по требованию администратора.

Подсистема управления средствами защиты

Подсистема управления позволяет администрации безопасности осуществлять:

централизованное (с АРМ администратора) создание и удаление пользователей, изменение их полномочий и паролей;

установку атрибутов доступа пользователей к ресурсам;

централизованное создание, удаление и изменение состава групп пользователей, а также их прав доступа;

централизованное управление группами компьютеров;

централизованное управление оперативным оповещением о НСД;

централизованное управление регистрацией событий и просмотр системных журналов.

Подсистема обеспечивает возможность как локального (непосредственно с рабочей станции), так и удаленного (с АРМ администратора) управления средствами защиты, установленными на рабочих станциях.

Состав документации

В комплект документации на Систему защиты входят:

общее описание Системы защиты;

руководство по установке Системы защиты;

руководство администратора безопасности;

руководство пользователя.

Требования к условиям эксплуатации

Предполагается, что для эффективного применения Системы защиты и поддержания необходимого уровня защищенности ЛВС специальной службой (администрацией безопасности системы) осуществляется непрерывное управление и организационно-административная поддержка ее функционирования по реализации принятой в организации политики безопасности.

Система функционирует на ПЭВМ, совместимых с IBM PC/AT/386/486. В состав ПЭВМ каждой рабочей станции должен входить накопитель на жестком диске и сетевая плата ЛВС.

Затраты ресурсов

Объем занимаемой оперативной памяти под резидентные части Системы защиты:

на рабочей станции - до 19-25 К байт (в зависимости от используемого драйвера);

на файловом сервере - до 500 К байт.

Относительные затраты производительности процессора:

на рабочей станции - до 2 %;

на файловом сервере - до 3 %.

Объем дисковой памяти для программ и данных:

на рабочей станции - до 500 К байт;

на файловом сервере - до 10 М байт.

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА QP DOS

Система разграничения доступа

Система разграничения доступа QP DOS является функциональным расширением MS DOS и предназначена для использования в составе АРМ на базе ПЭВМ IBM PC/AT. QP DOS полностью контролирует и управляет доступом всех пользователей к ресурсам и данным АРМ и обладает следующими возможностями:

идентификация пользователя по индивидуальному паролю, вводимому с электронного ключа Touch Memory, и запрет работы с ПЭВМ незарегистрированным пользователям;

разграничение доступа к ресурсам MS DOS для работающего в данный момент зарегистрированного пользователя, т.е. разрешение или запрещение операций чтения, записи или выполнения для каждого файла, а также работы с драйверами устройств и т.д. Разграничение доступа может устанавливаться для любого файла или драйвера MS DOS по отношению как к отдельным пользователям, так и по отношению к любым группам пользователей;

автоматическая регистрация действий пользователя;

автоматический запрос подтверждения личности пользователя по истечении заданной паузы его неактивности;

контроль за возможными попытками НСД;

интегрированная диалоговая оболочка администратора, осуществляющая функции ведения списка пользователей и групп пользователей, определения и изменения полномочий пользователей;

контроль целостности и защита от копирования программного обеспечения.

В качестве функциональных частей системы разграничения доступа могут быть включены следующие подсистемы:

подсистема регистрации и учета, предназначенная для протоколирования событий, происходящих в системе, контроля за возможными попытками НСД, учета сеансов пользователей и генерации отчетов;

подсистема оперативного контроля, позволяющая оперативно наблюдать с АРМ администратора системы за событиями и действиями пользователей, которые происходят на любом АРМ в составе ЛВС;

подсистема контроля целостности и защиты от копирования программного обеспечения;

плата запрещения начальной загрузки с гибкого магнитного диска, предотвращающая возможность обхода системы защиты нарушителем с помощью загрузки АРМ со своей системной дискеты.

Системы разграничения доступа предназначена для защиты информации от НСД и компьютерных преступлений в случае ошибочных или преднамеренных действий пользователей.

При ее использовании достигаются следующие цели:

реализация различных уровней полномочий и прав пользователей при работе в системе;

отсутствие возможностей несанкционированного изменения программного обеспечения АРМ;

отсутствие возможности несанкционированного запуска посторонних программ, в т.ч. находящихся на дискете, что гарантирует антивирусную защиту программного обеспечения;

отсутствие возможности несанкционированного копирования конфиденциальной информации (например, ключей шифрования) или программного обеспечения с целью его анализа;

запрет на работу с АРМ для незарегистрированных пользователей, даже имеющих физический доступ к компьютеру;

эффективная организация многопользовательского использования одного компьютера;

анализ и статистика работы пользователей в системе.

Система криптографической защиты информации на АРМ

Система криптографической защиты информации представляет собой драйвер MS DOS, осуществляющий зашифрование информации на отдельных логических дисках АРМ в прозрачном для прикладных программ режиме. Кроме этого, система включает средства для генерации ключей шифрования и перешифрования информации на новом ключе, и ввода ключей шифрования в систему с электронных ключей Touch Memory.

Система криптографической защиты может использоваться как в чисто программном варианте, так и с аппаратной поддержкой в виде криптоплаты "Криптон-3", что повышает производительность системы.

Криптографическая система предназначена для эффективной защиты информации на АРМ в следующих обстоятельствах:

в случае кражи, утери компьютера или магнитного носителя с информацией;

при выполнении ремонтных или сервисных работ посторонними лицами или обслуживающим персоналом, не допущенным к конфиденциальной информации;

при передаче информации в виде зашифрованных файлов по незащищенным каналам связи;

при использовании компъютера несколькими пользователями криптографическая система представляет собой дополнительный рубеж разграничения доступа к данным.

Сетевой режим системы QP DOS

Возможен сетевой режим системы защиты информации QP DOS, ориентированный на сетевую операционную систему Novell Netware. Количество обслуживаемых рабочих станций достигает 250 штук при одном файловом сервере.

Отличительной особенностью сетевого режима работы является использование для управления и настройки системы защиты информации единой для всех АРМ учетной базы, расположенной на файл-сервере ЛВС.

Сертификация изделия

Система защиты информации QP DOS прошла испытания и сертификацию в Федеральном Агенстве Правительственной Связи и Информации при Президенте РФ.

Состав базового комплекта

ПО системы разграничения доступа QP DOS, компл. 1

ПО системы криптографической защиты информации, компл. 1

Плата адаптера Touch Memory SDC100, шт. 1

Автоматические идентификаторы DS1992, шт. 3

Плата запрещения загрузки с НГМД SDC002, шт. 1

Рабочая документация, компл. 1

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА СНЕГ 2.0 (ВТГА, 07106-01ТУ)

Реализованные нормативные требования по защите от НСД к информации

Подсистема управления доступом осуществляет следующие функции:

идентификацию и проверку подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю временного действия длиной до восьми буквенно-цифровых символов;

идентификацию внешних устройств ПЭВМ по физическим адресам (номерам);

идентификацию программ, томов, каталогов, файлов по именам;

контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа;

управление потоками информации с помощью меток конфиденциальности.

При этом уровень конфиденциальности накопителей должен быть не ниже уровня конфиденциальности записываемой на него информации.

Подсистема регистрации и учета осуществляют следующие функции:

а) регистрацию входа субъектов доступа в систему.

В параметрах регистрации указываются:

время и дата входа субъекта доступа в систему;

результат попытки входа: успешная или неуспешная несанкционированная;

идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;

б) регистрацию выдачи печатных (графических) документов на "твердую" копию.

Выдача сопровождается автоматической маркировкой каждого листа (страницы) документа порядковым номером и учетными реквизитами АБС с указанием на последнем листе документа общего количества листов (страниц).

Вместе с выдачей документа автоматически оформляется учетная карточка документа с указанием даты выдачи документа, учетных реквизитов документа, краткого содержания (наименования, вида, шифра, кода) и уровня конфиденциальности документа, фамилии лица, выдавшего документ, колиства страниц и копий документа.

В параметрах регистрации указывается:

время и дата выдачи (обращения к подсистеме вывода);

идентификатор субъекта доступа, запросившего выдачу;

краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа;

объем фактически выданного документа (количество страниц, листов, копий) и результат выдачи: успешный (весь объем), неуспешный;

в) регистрацию запуска всех программ и процессов (заданий, задач) в АБС.

В параметрах регистрации указывается:

дата и время запуска;

имя (идентификатор) программы (процесса, задания);

идентификатор субъекта доступа, запросившего программу (процесс, задание);

результат запуска: успешный, неуспешный - несанкционированный;

г) регистрацию попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам.

В параметрах регистрации указывается:

дата и время попытки доступа к защищаемому файлу с указанием ее результата: успешная, неуспешная - несанкционированная;

идентификатор субъекта доступа;

спецификация защищаемого файла;

имя программы (процесса, задания, задачи), осуществляющей доступ к файлу;

вид запрашиваемой операции (чтение, запись, удаление, выполнение, расширение и т.п.);

д) регистрацию попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: внешним устройствам ПЭВМ, программам, томам, каталогам, файлам.

В параметрах регистрации указывается:

дата и время попытки доступа к защищаемому объекту с указанием ее результата: успешная, неуспешная - несанкционированная;

идентификатор субъекта доступа;

спецификация защищаемого объекта (логическое имя/номер);

имя программы (процесса, задания, задачи), осуществляющей доступ к защищаемому объекту;

вид запрашиваемой операции (чтение, запись, монтирование, захват и т.п.);

е) автоматический учет создаваемых защищаемых файлов, инициируемых защищаемых томов, каталогов, выделяемых для обработки защищаемых файлов, внешних устройств ПЭВМ;

ж) очистку (обнуление, обезличивание) освобождаемых областей оперативной памяти ПЭВМ;

з) сигнализацию попыток нарушения защиты.

Криптографическая подсистема обеспечивает:

шифрование всей конфиденциальной информации, записываемой на совместно используемые различными субъектами доступа (разделяемые) носители данных.

При этом выполняется автоматическая очистка областей внешней памяти, содержавших ранее незашифрованную информацию;

возможность использования разных криптографических ключей, для шифрования информации, принадлежащей различным субъектам доступа (группе субъектов).

Владельцем ПЭВМ (АРМ, АБС) должна осуществляться периодическая замена всех криптографических ключей, используемых для шифрования информации (перешифрования).

Используемые средства криптографической защиты должны быть сертифицированы специальными сертификационными центрами, имеющими лицензию на проведение сертификации криптографических средств защиты.

В системе "Снег 2.0" предусмотрены средства обеспечения целостности программных средств защиты и неизменности программной среды. При этом:

целостность программных средств системы "Снег 2.0" проверяется по контрольным суммам в с е х компонент СЗИ НСД;

целостность программной среды должна обеспечиваться пользователем (владельцем) ПЭВМ качеством приемки программных средств, предназначенных для применения в ПЭВМ при обработке защищенных файлов.

Общие положения по применению системы "Снег 2.0"

Система защиты информации от несанкционированного доступа "Снег 2.0" (ВТГА.07106-01) предназначена для применения в ПЭВМ типа IBM PC/AT с операционной системой MS DOS версий 5.0 или 6.xx с выполнением требований по защите от НСД к информации.

Система "Снег 2.0" обеспечивает конфиденциальность и защиту от НСД к информации в ПЭВМ до уровня "сов.секретно". Документацией на систему "Снег 2.0" предусмотрены меры организационной поддержки класса защищенности информации от НСД. В частности, предприятие (фирма, владелец ПЭВМ) обязано обеспечить реализацию следующих организационно-распорядительных защитных мер:

введение и организация работы службы безопасности информации (службы БИ);

ведение журнала учета работы ПЭВМ;

организация учета носителей информации;

обеспечение ***физической*** сохранности оборудования;

исключение возможности загрузки ОС с дискет ***пользователя*** при помощи применения специальной платы КРИПТОН-3, опечатывание корпуса ПЭВМ и контроль сохранности печатей;

запрещение доступа пользователям к программам-отладчикам, имеющим непосредственный доступ к оперативной или дисковой памяти,

а также к средствам построения и запуска задач пользователя;

обеспечение уникальности ключевых дискет (по группам пользователей, пользователям, ценности информации, принадлежности информации,...);

ведение журнала учета работы ПЭВМ (так называемый "ручной журнал") при обработке секретной информации.

Рекомендуется хранение и использование главного ключа шифрования, узла замены на одной дискете, применяемой

администратором, а рабочих ключей пользователей на других дискетах, устанавливаемых на дисковод при запросах программ шифрования.

ОДНОПЛАТНЫЕ УСТРОЙСТВА ШИФРОВАНИЯ РЯДА "КРИПТОН"

КРИПТОН - это программно-аппаратные комплексы, использование которых обеспечивает защиту информационных и финансовых, биржевых и банковских коммуникаций, баз данных и других массивов компьютерной информации.

Одноплатные устройства содержат высококачественные датчики случайных чисел для генерации ключей и узлы шифрования, аппаратно-реализованные в специализированных однокристальных микро-ЭВМ. Открытый интерфейс комплексов позволяет внедрять устройства КРИПТОН в Ваши системы, а также разрабатывать дополнительное программное обеспечение специального назначения.

Устройства КРИПТОН программно совместимы "снизу вверх". Дополнительное и базовое ПО, основываясь на уникальных возможностях изделий, позволяет осуществлять:

шифрование файлов, групп файлов и разделов дисков;

защиту информации, передаваемой по открытым каналам связи и сетям межмашинного обмена;

разграничение и контроль доступа к компьютеру;

электронную подпись юридических и финансовых документов;

прозрачное шифрование жестких и гибких дисков.

Основные характеристики устройств ряда КРИПТОН

	КРИПТОН-3	КРИПТОН-ЕС	КРИПТОН-4
Тип компьютера	IBM PC XT/AT 286..486 Pentium	ЕС 1841.. ЕС 1845	IBM PC XT/AT 286..486 Pentium
Тип шины	ISA	ЕС	ISA
Скорость шифрования, К байт/с	20-150	20-150	100-300
Габариты			
Контроллер с шиной микро-ЭВМ	Дискретные элементы	Дискретные элементы	Вентильные матрицы
Примечание	Проведены спец. исследования в ФАПСИ. Рекомендован ФАПСИ для примечания	Доп. порты 2-RS232 1-PRN	Буфер в/вывода на 8 байт. Проведены спец. исследования в ФАПСИ

Тип продукта	Аппаратно-программный на базе специализированных заказных СБИС
Операционная система	MS DOS, версия 3.0 и выше
Используемый алгоритм	ГОСТ 28147-89
Управление ключами	Управляются пользователем или системным администратором
Изготовление ключей	Изготавливаются самостоятельно, системным администратором или заказываются
Длина ключа, бит	256

Ключевая система	7 типов, выбирается пользователем
Использование пароля	Если необходим
Длина пароля, символ	От 3 до 37
Гарантия, год	1

На базе устройств КРИПТОН разработана и выпускается система КРИПТОН-ИК, в том числе обеспечивающая чтение/запись и защиту данных, хранящихся на Smart Card (интеллектуальных идентификационных карточках), широко применяемых как в виде дебетно/кредитных карточек при безналичных расчетах, так и в виде средства хранения прав доступа, ключей шифрования, а также конфиденциальной информации.

Информационная безопасность

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ЭЛЕКТРОННЫХ БАНКОВ

Редактор Н.В. Шумакова

Техн. редактор Е.Н. Кочубей

Лицензия ЛР № 020676 от 09.12.1992 г.

Подписано в печать 14.06.95. Формат 60x84 1/16

Печ.л. 6,5 Уч.-изд.л. 6,5 Тираж 500 экз. Изд.№018-3 Заказ 647

Московский государственный инженерно-физический институт (технический университет) Типография МИФИ.

115409, Москва, Каширское шоссе, 31

30 p. 0.02