**дипломная работа**

на тему

«**Проблемы информационной безопасности банков**»

**Оглавление**

Ââåäåíèå 3

Ãëàâà 1. Îñîáåííîñòè èíôîðìàöèîííîé áåçîïàñíîñòè áàíêîâ. 8

Ãëàâà 2. Âëèÿíèå äîñòèæåíèé â ñôåðå êîìïüþòåðíîé îáðàáîòêè èíôîðìàöèè íà ðàçâèòèå áàíêîâñêèõ òåõíîëîãèé. 12

Ãëàâà 3. ×åëîâå÷åñêèé ôàêòîð â îáåñïå÷åíèè èíôîðìàöèîííîé áåçîïàñíîñòè. 17

Óãðîçû èíôîðìàöèîííîé áåçîïàñíîñòè áàíêà ñî ñòîðîíû ïåðñîíàëà. 17

Êàäðîâàÿ ïîëèòèêà ñ òî÷êè çðåíèÿ èíôîðìàöèîííîé áåçîïàñíîñòè. 21

Ãëàâà 4. Áåçîïàñíîñòü àâòîìàòèçèðîâàííûõ ñèñòåì îáðàáîòêè èíôîðìàöèè â áàíêàõ (ÀÑÎÈÁ). 29

Óãðîçû áåçîïàñíîñòè àâòîìàòèçèðîâàííûõ ñèñòåì. 29

Àíàëèç ñîñòîÿíèÿ áàíêîâñêèõ àâòîìàòèçèðîâàííûõ ñèñòåì ñ òî÷êè çðåíèÿ áåçîïàñíîñòè. 43

Ïîñòðîåíèå çàùèòû áàíêîâñêèõ àâòîìàòèçèðîâàííûõ ñèñòåì. 50

Ãëàâà 5. Áåçîïàñíîñòü êîìïüþòåðíûõ ñåòåé â áàíêå. 77

Êëàññèôèêàöèÿ ñåòåé. 77

Îáåñïå÷åíèå áåçîïàñíîñòè ñåòåé. 81

Ãëàâà 6. Áåçîïàñíîñòü ýëåêòðîííûõ ïëàòåæåé. 88

Ýëåêòðîííûå ïëàòåæè â áàíêå. 88

Âîïðîñû áåçîïàñíîñòè ýëåêòðîííûõ ïëàòåæåé. 94

Ãëàâà 7. Áåçîïàñíîñòü ïåðñîíàëüíûõ ïëàòåæåé ôèçè÷åñêèõ ëèö. 101

Îñíîâíûå ôîðìû óäàëåííîãî áàíêîâñêîãî îáñëóæèâàíèÿ ôèçè÷åñêèõ ëèö. 101

Ïðîáëåìû èäåíòèôèêàöèè êëèåíòà ïðè óäàëåííîì îáñëóæèâàíèè. 103

Áåçîïàñíîñòü ïðè èñïîëüçîâàíèè ïëàñòèêîâûõ êàðò. 105

Çàêëþ÷åíèå. 113

Ñïèñîê ëèòåðàòóðû 115

# Введение

Со времени своего появления банки неизменно вызывали преступный интерес. И этот интерес был связан не только с хранением в кредитных организациях денежных средств, но и с тем, что в банках сосредотачивалась важная и зачастую секретная информация о финансовой и хозяйственной деятельности многих людей, компаний, организаций и даже целых государств. Так, еще в XVIII веке недоброжелатели известного Джакомо Казановы опубликовали закрытые данные о движении средств по его счету в одном из парижских банков. Из этой информации следовало, что организованная Казановой государственная лотерея приносила доход не только казне, но и (в не меньших масштабах) ему лично [1, с.4].

В настоящее время значение информации, хранимой в банках, значительно увеличилось. Так, недавняя утечка данных о ряде счетов в Bank of England в январе 1999 года заставила банк поменять коды всех корреспондентских счетов, часть оборудования и программного обеспечения и обошлась банку в несколько десятков миллионов долларов. [17, сообщ. за 26.02.99г.]

В наши дни в связи со всеобщей информатизацией и компьютеризацией банковской деятельности значение информационной безопасности банков многократно возросло. Еще 30 лет назад объектом информационных атак были данные о клиентах банков или о деятельности самого банка. Такие атаки были редкими, круг их заказчиков был очень узок, а ущерб мог быть значительным лишь в особых случаях. В настоящее время в результате повсеместного распространения электронных платежей, пластиковых карт, компьютерных сетей объектом информационных атак стали непосредственно денежные средства как банков, так и их клиентов. Совершить попытку хищения может любой — необходимо лишь наличие компьютера, подключенного к сети Интернет. Причем для этого не требуется физически проникать в банк, можно «работать» и за тысячи километров от него.

Например, в августе 1995 г. в Великобритании был арестован 24-летний российский математик Владимир Левин, который при помощи своего домашнего компьютера в Петербурге сумел проникнуть в банковскую систему одного из крупнейших американских банков Citibank и похитить $2,8 млн. В 1994 году Владимир Левин вместе с приятелем сумел подобрать ключи к системе банковской защиты Citibank и попытался снять с его счетов крупные суммы. По сведениям московского представительства Citibank, до тех пор подобное никому не удавалось. Служба безопасности Citibank выяснила, что у банка пытались похитить $2,8 млн., но контролирующие системы вовремя это обнаружили и заблокировали счета. Украсть же удалось лишь $400 тысяч. Для получения денег Левин выехал в Англию, где и был арестован [17, сообщ. за 01.10.95г.].

Компьютеризация банковской деятельности позволила значительно повысить производительность труда сотрудников банка, внедрить новые финансовые продукты и технологии. Однако прогресс в технике преступлений шел не менее быстрыми темпами, чем развитие банковских технологий. В настоящее время свыше 90% всех преступлений связана с использованием автоматизированных систем обработки информации банка (АСОИБ) [6, с.17]. Следовательно, при создании и модернизации АСОИБ банкам необходимо уделять пристальное внимание обеспечению ее безопасности. Именно этой проблеме посвящена большая часть дипломной работы.

Именно эта проблема является сейчас наиболее актуальной и наименее исследованной. Если в обеспечении физической и классической информационной[[1]](#footnote-1) безопасности давно уже выработаны устоявшиеся подходы (хотя развитие происходит и здесь), то в связи с частыми радикальными изменениями в компьютерных технологиях методы безопасности АСОИБ требуют постоянного обновления. Как показывает практика, не существует сложных компьютерных систем, не содержащих ошибок. А поскольку идеология построения крупных АСОИБ регулярно меняется, то исправления найденных ошибок и «дыр» в системах безопасности хватает ненадолго, так как новая компьютерная система приносит новые проблемы и новые ошибки, заставляет по-новому перестраивать систему безопасности.

Особенно актуальна данная проблема в России. В западных банках программное обеспечение (ПО) разрабатываются конкретно под каждый банк и устройство АСОИБ во многом является коммерческой тайной. В России получили распространение «стандартные» банковские пакеты, информация о которых широко известна, что облегчает несанкционированный доступ в банковские компьютерные системы. Причем, во-первых, надежность «стандартного» ПО ниже из-за того разработчик не всегда хорошо представляет конкретные условия, в которых этому ПО придется работать, а во-вторых, некоторые российские банковские пакеты не удовлетворяли условиям безопасности. Например, ранние версии (которые и по сей день эксплуатируются в небольших банках) самого популярного российского банковского пакета требовали наличия дисковода у персонального компьютера и использовали ключевую дискету, как инструмент обеспечения безопасности [16]. Такое решение, во-первых, технически ненадежно, а во-вторых, одно из требований безопасности АСОИБ — закрытие дисководов и портов ввода-вывода в компьютерах сотрудников, не работающих с внешними данными.

В связи с вышеизложенным, в настоящей работе основное внимание уделено именно компьютерной безопасности банков, т.е. безопасности автоматизированных систем обработки информации банка (АСОИБ), как наиболее актуальной, сложной и насущной проблеме в сфере банковской информационной безопасности.

В работе рассматриваются особенности информационной безопасности банков, показывается, что именно для банков (в отличие от других предприятий) информационная безопасность имеет решающее значение (глава 1). В главе 2 говорится о развитии банковских информационных технологий, поскольку именно эти технологии во многом определяют систему информационной безопасности банка. Поскольку, по данным статистики [17, сообщ. за 08.12.98г.], наибольшая часть преступлений против банков совершается с использованием инсайдерской информации, то в работе имеется глава 3, посвященная обеспечению информационной безопасности в сфере работы с персоналом.

Остальная часть работы посвящена безопасности АСОИБ и электронных платежей, как ее составной части. В главе 4 анализируются угрозы безопасности АСОИБ и рассматриваются общие принципы построения систем безопасности АСОИБ. В главе 5 описываются специализированные проблемы безопасности банковских компьютерных сетей. Главы 6 и 7 посвящены безопасности электронных платежей.

По мере развития и расширения сферы применения средств вычислительной техники острота проблемы обеспечения безопасности вычислительных систем и защиты хранящейся и обрабатываемой в них информации от различных угроз все более возрастает. Для этого есть целый ряд объективных причин.

Основная из них — возросший уровень доверия к автоматизированным системам обработки информации. Им доверяют самую ответственную работу, от качества которой зависит жизнь и благосостояние многих людей. ЭВМ управляют технологическими процессами на предприятиях и атомных электростанциях, движениями самолетов и поездов, выполняют финансовые операции, обрабатывают секретную информацию.

Сегодня проблема защиты вычислительных систем становится еще более значительной в связи с развитием и распространением сетей ЭВМ. Распределенные системы и системы с удаленным доступом выдвинули на первый план вопрос защиты обрабатываемой и передаваемой информации.

Доступность средств вычислительной техники, и прежде всего персональных ЭВМ, привела к распространению компьютерной грамотности в широких слоях населения. Это, в свою очередь, вызвало многочисленные попытки вмешательства в работу государственных и коммерческих, в частности банковских, систем, как со злым умыслом, так и из чисто «спортивного интереса». Многие из этих попыток имели успех и нанесли значительный урон владельцам информации и вычислительных систем.

В немалой степени это касается разных коммерческих структур и организаций, особенно тех, кто по роду своей деятельности хранит и обрабатывает ценную (в денежном выражении) информацию, затрагивающую к тому же интересы большого количества людей. В банках, когда дело касается электронных платежей и автоматизированного ведения счетов, такая информация в некотором роде и представляет из себя деньги.

Целостную картину всех возможностей защиты создать довольно сложно, поскольку пока еще нет единой теории защиты компьютерных систем. Существует много подходов и точек зрения на методологию ее построения. Тем не менее, в этом направлении прилагаются серьезные усилия, как в практическом, так и в теоретическом плане, используются самые последние достижения науки, привлекаются передовые технологии. Причем занимаются этой проблемой ведущие фирмы по производству компьютеров и программного обеспечения, университеты и институты, а также крупные банки и международные корпорации.

Известны различные варианты защиты информации — от охранника на входе до математически выверенных способов сокрытия данных от ознакомления. Кроме того, можно говорить о глобальной защите и ее отдельных аспектах: защите персональных компьютерах, сетей, баз данных и др.

Необходимо отметить, что абсолютно защищенных систем нет. Можно говорить о надежности системы, во-первых, лишь с определенной вероятностью, а во-вторых, о защите от определенной категории нарушителей. Тем не менее проникновения в компьютерную систему можно предусмотреть. Защита — это своего рода соревнование обороны и нападения: кто больше знает и предусматривает действенные меры — тот и выиграл.

Организация защиты АСОИБ — это единый комплекс мер, которые должны учитывать все особенности процесса обработки информации. Несмотря на неудобства, причиняемые пользователю во время работы, во многих случаях средства защиты могут оказаться совершенно необходимыми для нормального функционирования системы. К основным из упомянутых неудобств следует отнести:

1. Дополнительные трудности работы с большинством защищенных систем.

2. Увеличение стоимости защищенной системы.

3. Дополнительная нагрузка на системные ресурсы, что потребует увеличения рабочего времени для выполнения одного и того же задания в связи с замедлением доступа к данным и выполнения операций в целом.

4. Необходимость привлечения дополнительного персонала, отвечающего за поддержание работоспособности системы защиты.

Что же касается необходимости применения защиты, то здесь принцип «пока гром не грянет, мужик не перекрестится» себя не оправдывает. Информация может иметь слишком большую ценность, чтобы рисковать ею, а непреложная истина: «кто владеет информацией — тот владеет миром», большей частью вполне себя оправдывает.

Современный банк трудно представить себе без автоматизированной информационной системы. Компьютер на столе банковского служащего уже давно превратился в привычный и необходимый инструмент. Связь компьютеров между собой и с более мощными компьютерами, а также с ЭВМ других банков — также необходимое условие успешной деятельности банка — слишком велико количество операций, которые необходимо выполнить в течении короткого периода времени.

В то же время информационные системы становятся одной из наиболее уязвимых сторон современного банка, притягивая к себе злоумышленников как из числа персонала банка, так и со стороны. Оценки потерь от преступлений, связанных с вмешательством в деятельность информационной системы банков, очень сильно разнятся. Сказывается разнообразие методик для их подсчета. Средняя банковская кража с применением электронных средств составляет около $9.000, а один из самых громких скандалов связан с попыткой украсть $700 млн. (Первый национальный банк, Чикаго). [3, с.56]

Причем необходимо учитывать не только суммы прямого ущерба, но и весьма дорогостоящие мероприятия, которые проводятся после успешных попыток взлома компьютерных систем. Так, недавняя пропажа данных о работе с секретными счетами Bank of England в январе 1999 года заставила банк поменять коды всех корреспондентских счетов. В этой связи в Великобритании были подняты по тревоге все имеющиеся силы разведки и контрразведки для того, чтобы не допустить невероятной утечки информации, способной нанести огромный ущерб. Правительством предпринимались крайние меры с тем, чтобы посторонним не стали известны счета и адреса, по которым Bank of England направляет ежедневно сотни миллиардов долларов. Причем в Великобритании больше опасались ситуации, при которой данные могли оказаться в распоряжении иностранных спецслужб. В таком случае была бы вскрыта вся финансовая корреспондентская сеть Bank of England. Возможность ущерба была ликвидирована в течение нескольких недель. [17, сообщ. за 26.02.99г.]

Услуги, предоставляемые банками сегодня, в немалой степени основаны на использовании средств электронного взаимодействия банков между собой, банков и их клиентов и торговых партнеров. В настоящее время доступ к услугам банков стал возможен из различных удаленных точек, включая домашние терминалы и служебные компьютеры. Этот факт заставляет отойти от концепции «запертых дверей», которая была характерна для банков 60-х годов, когда компьютеры использовались в большинстве случаев в пакетном режиме как вспомогательное средство и не имели связи с внешним миром.

Компьютерные системы, без которых не может обойтись ни один современный банк, — источник совершенно новых, ранее неизвестных угроз. Большинство из них обусловлено использованием в банковском деле новых информационных технологий и характерны не только для банков. При этом следует помнить, что во многих странах, несмотря на все увеличивающуюся роль электронных систем обработки, объем операций с бумажными документами в 3-4 раза выше, чем с их электронными аналогами.

Уровень оснащенности средствами автоматизации играет немаловажную роль в деятельности банка и, следовательно, напрямую отражается на его положении и доходах. Усиление конкуренции между банками приводит к необходимости сокращения времени на производство расчетов, увеличения номенклатуры и повышения качества предоставляемых услуг.

Чем меньше времени будут занимать расчеты между банком и клиентами, тем выше станет оборот банка и, следовательно, прибыль. Кроме того, банк более оперативно сможет реагировать на изменение финансовой ситуации. Разнообразие услуг банка (в первую очередь это относится к возможности безналичных расчетов между банком и его клиентами с использованием пластиковых карт) может существенно увеличить число его клиентов и, как следствие, повысить прибыль.

В то же время, АСОИБ банка становится одним из наиболее уязвимых мест во всей организации, притягивающей злоумышленников, как извне, так и из числа сотрудников самого банка. Для подтверждения этого тезиса можно привести несколько фактов:

\* Потери банков и других финансовых организаций от воздействий на их системы обработки информации составляют около $3 млрд. в год.

\* Объем потерь, связанных с использованием пластиковых карточек оценивается в $2 млрд. в год, что составляет 0.03-2% от общего объема платежей в зависимости от используемой системы.

\* Средняя величина ущерба от банковской кражи с применением электронных средств составляет около $9.000. [3, с.60]

\* Один из самых громких скандалов связан с попыткой семерых человек украсть $700 млн. в Первом национальном банке, Чикаго. Она была предотвращена ФБР.

\* 27 млн. фунтов стерлингов были украдены из Лондонского отделения Union Bank of Switzerland;

\* DM 5 млн. украдены из Chase Bank (Франкфурт); служащий перевел деньги в банк Гонконга; они были взяты с большого количества счетов (атака «салями»), кража оказалась успешной;

\* $3 млн. — банк Стокгольма, кража была совершена с использованием привилегированного положения нескольких служащих в информационной системе банка и также оказалась успешной. [10]

Чтобы обезопасить себя и своих клиентов, большинство банков предпринимают необходимые меры защиты, в числе которых защита АСОИБ занимает не последнее место. При этом необходимо учитывать, что защита АСОИБ банка — дорогостоящее и сложное мероприятие. Так, например, Barclays Bank тратит на защиту своей автоматизированной системы около $20 млн. ежегодно. [13]

В первой половине 1994 г. Datapro Information Services Group провела почтовый опрос среди случайно выбранных менеджеров информационных систем. Целью опроса явилось выяснение состояния дел в области защиты. Было получено 1.153 анкеты, на основе которых получены приводимые ниже результаты [2, с.101]:

\* около 25% всех нарушений составляют стихийные бедствия;

\* около половины систем испытывали внезапные перерывы электропитания или связи, причины которых носили искусственный характер;

\* около 3% систем испытывали внешние нарушения (проникновение в систему организации);

\* 70-75% - внутренние нарушения, из них:

- 10% совершены обиженными и недовольными служащими-пользователями АСОИБ банка;

- 10% - совершены из корыстных побуждений персоналом системы;

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

Эти данные свидетельствуют о том, что чаще всего происходят не такие нарушения, как нападения хакеров или кража компьютеров с ценной информацией, а самые обыкновенные, проистекающие из повседневной деятельности. В то же время именно умышленные атаки на компьютерные системы приносят наибольший единовременный ущерб, а меры защиты от них наиболее сложны и дорогостоящи. В этой связи проблема оптимизации защиты АСОИБ является наиболее актуальной в сфере информационной безопасности банков.

# Глава 1. Особенности информационной безопасности банков.

Стратегия информационной безопасности банков весьма сильно отличается от аналогичных стратегий других компаний и организаций. Это обусловлено прежде всего специфическим характером угроз, а также публичной деятельностью банков, которые вынуждены делать доступ к счетам достаточно легким с целью удобства для клиентов.

Обычная компания строит свою информационную безопасность, исходя лишь из узкого круга потенциальных угроз — главным образом защита информации от конкурентов (в российских реалиях основной задачей является защита информации от налоговых органов и преступного сообщества с целью уменьшения вероятности неконтролируемого роста налоговых выплат и рэкета). Такая информация интересна лишь узкому кругу заинтересованных лиц и организаций и редко бывает ликвидна, т.е. обращаема в денежную форму.

Информационная безопасность банка должна учитывать следующие специфические факторы:

1. Хранимая и обрабатываемая в банковских системах информация представляет собой реальные деньги. На основании информации компьютера могут производится выплаты, открываться кредиты, переводиться значительные суммы. Вполне понятно, что незаконное манипулирование с такой информацией может привести к серьезным убыткам. Эта особенность резко расширяет круг преступников, покушающихся именно на банки (в отличие от, например, промышленных компаний, внутренняя информация которых мало кому интересна).

2. Информация в банковских системах затрагивает интересы большого количества людей и организаций — клиентов банка. Как правило, она конфиденциальна, и банк несет ответственность за обеспечение требуемой степени секретности перед своими клиентами. Естественно, клиенты вправе ожидать, что банк должен заботиться об их интересах, в противном случае он рискует своей репутацией со всеми вытекающими отсюда последствиями.

3. Конкурентоспособность банка зависит от того, насколько клиенту удобно работать с банком, а также насколько широк спектр предоставляемых услуг, включая услуги, связанные с удаленным доступом. Поэтому клиент должен иметь возможность быстро и без утомительных процедур распоряжаться своими деньгами. Но такая легкость доступа к деньгам повышает вероятность преступного проникновения в банковские системы.

4. Информационная безопасность банка (в отличие от большинства компаний) должна обеспечивать высокую надежность работы компьютерных систем даже в случае нештатных ситуаций, поскольку банк несет ответственность не только за свои средства, но и за деньги клиентов.

5. Банк хранит важную информацию о своих клиентах, что расширяет круг потенциальных злоумышленников, заинтересованных в краже или порче такой информации.

Преступления в банковской сфере также имеют свои особенности [2, с.16]:

1. Многие преступления, совершенные в финансовой сфере остаются неизвестными для широкой публики в связи с тем, что руководители банков не хотят тревожить своих акционеров, боятся подвергнуть свою организацию новым атакам, опасаются подпортить свою репутацию надежного хранилища средств и, как следствие, потерять клиентов.
2. Как правило, злоумышленники обычно используют свои собственные счета, на который переводятся похищенные суммы. Большинство преступников не знают, как «отмыть» украденные деньги. Умение совершить преступление и умение получить деньги — это не одно и то же.
3. Большинство компьютерных преступлений — мелкие. Ущерб от них лежит в интервале от $10.000 до $50.000.
4. Успешные компьютерные преступления, как правило, требуют большого количества банковских операций (до нескольких сотен). Однако крупные суммы могут пересылаться и всего за несколько транзакций.
5. Большинство злоумышленников — клерки. Хотя высший персонал банка также может совершать преступления и нанести банку гораздо больший ущерб — такого рода случаи единичны.
6. Компьютерные преступления не всегда высокотехнологичны. Достаточно подделки данных, изменения параметров среды АСОИБ и т.д., а эти действия доступны и обслуживающему персоналу.
7. Многие злоумышленники объясняют свои действия тем, что они всего лишь берут в долг у банка с последующим возвратом. Впрочем «возврата», как правило, не происходит.

Специфика защиты автоматизированных систем обработки информации банков (АСОИБ) обусловлена особенностями решаемых ими задач:

1. Как правило АСОИБ обрабатывают большой поток постоянно поступающих запросов в реальном масштабе времени, каждый из которых не требует для обработки многочисленных ресурсов, но все вместе они могут быть обработаны только высокопроизводительной системой;
2. В АСОИБ хранится и обрабатывается конфиденциальная информация, не предназначенная для широкой публики. Ее подделка или утечка могут привести к серьезным (для банка или его клиентов) последствиям. Поэтому АСОИБ обречены оставаться относительно закрытыми, работать под управлением специфического программного обеспечения и уделять большое внимание обеспечению своей безопасности;
3. Другой особенностью АСОИБ является повышенные требования к надежности аппаратного и программного обеспечения. В силу этого многие современные АСОИБ тяготеют к так называемой отказоустойчивой архитектуре компьютеров, позволяющей осуществлять непрерывную обработку информации даже в условиях различных сбоев и отказов.

Можно выделить два типа задач, решаемых АСОИБ:

1. Аналитические. К этому типу относятся задачи планирования, анализа счетов и т.д. Они не являются оперативными и могут требовать для решения длительного времени, а их результаты могут оказать влияние на политику банка в отношении конкретного клиента или проекта. Поэтому подсистема, с помощью которой решаются аналитические задачи, должна быть надежно изолирована от основной системы обработки информации. Для решения такого рода задач обычно не требуется мощных вычислительных ресурсов, обычно достаточно 10-20% мощности всей системы. Однако ввиду возможной ценности результатов их защита должна быть постоянной.

2. Повседневные. К этому типу относятся задачи, решаемые в повседневной деятельности, в первую очередь выполнение платежей и корректировка счетов. Именно они и определяют размер и мощность основной системы банка; для их решения обычно требуется гораздо больше ресурсов, чем для аналитических задач. В то же время ценность информации, обрабатываемой при решении таких задач, имеет временный характер. Постепенно ценность информации, например, о выполнении какого-либо платежа, становиться не актуальной. Естественно, это зависит от многих факторов, как-то: суммы и времени платежа, номера счета, дополнительных характеристик и т.д. Поэтому, обычно бывает достаточным обеспечить защиту платежа именно в момент его осуществления. При этом защита самого процесса обработки и конечных результатов должна быть постоянной.

Каким же мерам защиты систем обработки информации отдают предпочтение зарубежные специалисты? На этот вопрос можно ответить, используя результаты опроса, проведенного Datapro Information Group в 1994 году среди банков и финансовых организаций [2]:

1. Сформулированную политику информационной безопасности имеют 82% опрошенных. По сравнению с 1991 годом процент организаций, имеющих политику безопасности, увеличился на 13%.
2. Еще 12% опрошенных планируют разработать политику безопасности. Четко выражена следующая тенденция: организации с большим числом персонала предпочитают иметь разработанную политику безопасности в большей степени, чем организации с небольшим количеством персонала. Например, по данным этого опроса, всего лишь 66% организаций, с числом сотрудников менее 100 человек имеют политику безопасности, тогда как для организаций с числом сотрудников более 5000 человек доля таких организаций составляет 99%.
3. В 88% организаций, имеющих политику информационной безопасности, существует специальное подразделение, которое отвечает за ее реализацию. В тех организациях, которые не содержат такое подразделение, эти функции, в основном, возложены на администратора системы (29%), на менеджера информационной системы (27%) или на службу физической безопасности (25%). Это означает, что существует тенденция выделения сотрудников, отвечающих за компьютерную безопасность, в специальное подразделение.
4. В плане защиты особое внимание уделяется защите компьютерных сетей (90%), больших ЭВМ (82%), восстановлению информации после аварий и катастроф (73%), защите от компьютерных вирусов (72%), защите персональных ЭВМ (69%).

Можно сделать следующие выводы об особенностях защиты информации в зарубежных финансовых системах [2, с.21]:

1. Главное в защите финансовых организаций — оперативное и по возможности полное восстановление информации после аварий и сбоев. Около 60% опрошенных финансовых организаций имеют план такого восстановления, который ежегодно пересматривается в более чем 80% из них. В основном, защита информации от разрушения достигается созданием резервных копий и их внешним хранением, использованием средств бесперебойного электропитания и организацией «горячего» резерва аппаратных средств.
2. Следующая по важности для финансовых организаций проблема — это управление доступом пользователей к хранимой и обрабатываемой информации. Здесь широко используются различные программные системы управления доступом, которые иногда могут заменять и антивирусные программные средства. В основном используются приобретенные программные средства управления доступом. Причем в финансовых организациях особое внимание уделяют такому управлению пользователей именно в сети. Однако сертифицированные средства управления доступом встречаются крайне редко (3%). Это можно объяснить тем, что с сертифицированными программными средствами трудно работать и они крайне дороги в эксплуатации. Это объясняется тем, что параметры сертификации разрабатывались с учетом требований, предъявляемым к военным системам.
3. К отличиям организации защиты сетей ЭВМ в финансовых организациях можно отнести широкое использование стандартного (т.е. адаптированного, но не специально разработанного для конкретной организации) коммерческого программного обеспечения для управления доступом к сети (82%), защита точек подключения к системе через коммутируемые линии связи (69%). Скорее всего это связано с большей распространенностью средств телекоммуникаций в финансовых сферах и желание защититься от вмешательства извне. Другие способы защиты, такие как применение антивирусных средств, оконечное и канальное шифрование передаваемых данных, аутентификация сообщений применяются примерно одинаково и, в основном (за исключением антивирусных средств), менее чем в 50% опрошенных организаций.
4. Большое внимание в финансовых организациях уделяется физической защите помещений, в которых расположены компьютеры (около 40%). Это означает, что защита ЭВМ от доступа посторонних лиц решается не только с помощью программных средств, но и организационно-технических (охрана, кодовые замки и т.д.).
5. Шифрование локальной информации применяют чуть более 20% финансовых организаций. Причинами этого являются сложность распространения ключей, жесткие требования к быстродействию системы, а также необходимость оперативного восстановления информации при сбоях и отказах оборудования.
6. Значительно меньшее внимание в финансовых организациях уделяется защите телефонных линий связи (4%) и использованию ЭВМ, разработанных с учетом требования стандарта Tempest (защита от утечки информации по каналам электромагнитных излучений и наводок). В государственных организациях решению проблемы противодействия получению информации с использованием электромагнитных излучений и наводок уделяют гораздо большее внимание.

Анализ статистики позволяет сделать важный вывод: защита финансовых организаций (в том числе и банков) строится несколько иначе, чем обычных коммерческих и государственных организаций. Следовательно для защиты АСОИБ нельзя применять те же самые технические и организационные решения, которые были разработаны для стандартных ситуаций. Нельзя бездумно копировать чужие системы — они разрабатывались для иных условий.

# Глава 2. Влияние достижений в сфере компьютерной обработки информации на развитие банковских технологий.

Мировая банковская индустрия вошла в период перемен. Появление новых информационных технологий начинает оказывать влияние на выработку стратегической политики банка.

Нынешние изменения в банковской сфере связаны с влиянием ряда факторов, в числе которых международная тенденция глобализации рынка банковских услуг, изменение законодательства, а также развитие информационных технологий. Все это заставляет банки изменять способы обслуживания клиента.

Для того, чтобы остаться конкурентоспособными в XXI веке банки должны оценивать внешние факторы и адекватно реагировать на них. К тому же на деятельность банков влияют и внутренние факторы, такие как изменение запросов клиентов, необходимость уменьшения времени обслуживания, расширение использования высоких технологий.

Все это вынуждает банки искать свое место на рынке и разрабатывать свою стратегию действий с учетом новых реальностей. В жестких условиях современного рынка банки должны дать четкий ответ на следующие вопросы:

1. Что оказывает давление на мой бизнес?

2. Что оказывает давление на бизнес моих клиентов?

3. Как я буду конкурировать на рынке?

4. Как я могу увеличить количество моих клиентов?

5. Смогу ли я увеличить поступления с помощью расширенного набора услуг?

6. На каких рынках мне следует быть?

7. Где и как возникают наибольшие затраты и как я могу их уменьшить?

8. Как я могу увеличить количество моих акционеров?

К основным внешним факторам, влияющих на банковскую индустрию в Европе, специалисты фирмы DEC [1, с.42] относят следующие:

\* Общий рынок. Европейское Сообщество приняло решение о создании Общего европейского рынка товаров и услуг. Также как и некоторые положения Программы Общего рынка, некоторые директивы, вытекающие из этого решения окажут воздействие на деятельность банков.

\* Вторая банковская директива. Наиболее значительным актом, оказывающим воздействие на деятельность банков, является Вторая координационная банковская директива [Second Coordination Directive (Banking)], принятая к исполнению всеми членами Сообщества с 1 января 1993 г. Основным содержанием этой директивы являются принципы внутригосударственного управления и всеобщего одобрения членами Сообщества стандартов контроля и регулирования деятельности банков. Это позволяет банкам Сообщества, имеющим лицензии на деятельность в своей стране, выполнять операции в рамках всего Сообщества без получения дополнительных лицензий.

\* Глобализация рынка услуг. С развитием новых технологий исчезают ограничения, связанные с национальными барьерами, и рынок услуг становится доступным 24 часа в сутки.

\* Изменения в законодательстве. Изменения в законодательстве поощряют небанковские организации оказывать финансовые услуги в прямом соперничестве с банками. Многие из таких организаций созданы недавно, их деятельность не регулируется так, как банковская, и они не нуждаются в дорогостоящей инфраструктуре для этой цели. Они используют существующие сети распределения и продаж для оказания услуг, стоимость которых оказывается меньше, чем у банков. Более того, они не наследуют традиционную банковскую инфраструктуру: многие банки считают слишком обременительным для себя ее переориентировать. Небанковские организации используют расширяющуюся сеть клиентов и увеличение продаж в тех областях, которые были исключительной вотчиной банков. Так например, английская фирма Marks & Spencer успешно внедрилась на финансовый рынок с помощью создания собственного инвестиционного фонда и карточек для обслуживания в магазинах.

\* Увеличение требовательности клиентов. Информированность клиентов о доступности услуг банков и их стоимости приводит к увеличению требований к качеству и стоимости предлагаемых услуг. Особенно это касается крупнейших универсальных банков, которые становятся все менее привлекательны для клиентов, объединенных каким-либо одним общим интересом или проживающих в одном регионе. Клиенты также прекрасно осведомлены о риске, связанном с банковской деятельностью, и становятся более осторожными при вкладывании денег в ненадежные банки.

\* Обработка транзакций. Обработка транзакций остается наиболее трудоемким элементом цепи приоритетов банка; она должна быть безошибочной и обеспечивать точную и своевременную информацию. Однако клиенты не желают оплачивать «невидимые» услуги и поэтому не считают обработку транзакций прибыльным элементом для банка. Банки не в состоянии оказывать высококачественные услуги без значительных затрат в этой области. Но они стараются компенсировать их с помощью прогрессивно возрастающих тарифов. Конкуренты стремятся использовать более дешевые технологии, которые дают преимущество в конкурентной борьбе.

\* Технологии. За последнее десятилетие развитие технологий, средств обработки и передачи информации помогли увеличить производительность и уменьшить стоимость банковских операций. Современные технологии позволяют практически моментально получать и использовать информацию о клиентах, продуктах и рисках, что, несомненно, оказывает влияние на конкурентоспособность банков. Однако пока очень немногие банки в полной мере используют эти возможности. Средства телекоммуникаций вместе с новыми информационными технологиями становятся инструментом при разработке новых продуктов и механизмов их распространения, что расширяет сферу деятельности банков. Электронные платежи и средства расчета в точке продажи — примеры использования новых технологий, коренным образом меняющих банковскую индустрию. Тем не менее, информационные технологии и поддерживающие их организационные структуры могут стать барьером на пути развития. Вложив большие средства в определенную технологию, очень сложно переориентироваться на какую-либо другую. Этого недостатка лишены новые конкуренты, которые будут сразу приобретать перспективные технологии.

Выход из этого тупика - разработка эффективных способов обработки данных. В идеале следует заставить клиентов расплачиваться за улучшение параметров обслуживания (например, скорости). Так, скажем, операции передачи денег традиционно имеют большой объем и все больше зависят от применяемых технологий для сокращения расходов. Выполнение этих операций для большого числа клиентов может дать банкам существенную прибыль. Объемы же операций, связанных с обработкой чеков и других бумажных документов будут уменьшаться пропорционально распространению электронных банковских карт.

Современные технологии предлагают альтернативы традиционным банковским продуктам и услугам. Изменения, которые привели к уменьшению объема локальных операций, оказываются в центре внимания.

Так, Deutsche Bank в 1992 г. объявил об убытках, связанных с обслуживанием частных лиц, в сумме DM 200 млн. Тем не менее он продолжал выполнять программу расширения сети самообслуживания путем эмитирования 3-х миллионов электронных карт. [1, с.51]

Использование современных технологий создало новый рынок, где технологии становятся товаром в таких областях как обмен электронными данными, системы электронных платежей в точке продажи и т.д. Прежде всего это касается улучшения обслуживания клиентов и оказания более специфических услуг.

Идя навстречу требованиям клиентов, и в соответствии с другими факторами конкурентной борьбы, банки должны будут выбрать один из следующих путей развития:

1. Оказывать все виды услуг в большинстве своих отделений, включая, возможно, и небанковские услуги — универсальный банк;

2. Предоставлять узкому кругу клиентов небольшой, но специфичный перечень услуг в определенном регионе — специализированный банк.

Существующий круг клиентов — это ключевой ресурс банка, который необходимо сохранить и попытаться увеличить. С этой целью многие банки приспосабливают свои технологии для продажи новой продукции. Более того, они переопределяют назначение традиционных механизмов распределения (единые филиальные и корпоративные банковские сети) и вводят в эксплуатацию новые (телекоммуникационные средства связи с другими банками и корпоративными клиентами).

Растет необходимость жесткого контроля за расходами, особенно в условиях увеличения затрат на регулирование деятельности и появления на рынке новых дешевых товаров и услуг, производимых и оказываемых небанковскими организациями. Такой контроль может быть осуществлен с помощью централизованной обработки информации и совершенствования управлением. Эти меры, безусловно, оказывают воздействие на штат банка.

Возрастает необходимость обработки постоянно растущего потока информации о состоянии рынка для более точного определения места специфической продукции на расширяющемся рынке.

Возможность доступа клиента к банку с помощью существующих филиальных сетей теперь уже не является ключевым фактором успеха. Изменение требований клиентов, новые технологии и фиксированно высокая стоимость содержания таких сетей заставляют искать альтернативные стратегии. Предлагаются следующие подходы:

- мобильные пункты продажи товаров и услуг;

- механизмы прямой продажи товаров и услуг;

- технологии расчета в точке продажи;

- электронное и телефонное банковское обслуживание и др.

Применение новых технологий оказывает влияние на стратегические направления и направления бизнеса в деятельности банка.

Банки издавна внедряют и используют самые современные достижения науки и техники для облегчения ручного труда и ускорения выполняемых операций. Однако сейчас этого уже недостаточно и победителями будут те, кто полностью перестроит свою деятельность в соответствии с современными технологиями.

Развитие современных информационных технологий может осуществляться под воздействием бизнеса и для бизнеса. Особенно важным в этом процессе является то, что информационные технологии развиваются в тесном взаимодействии с экономикой. Информационные технологии влияют на размер получаемых доходов и на то, как они складываются и распределяются.

Информационные технологии пронизывают каждый элемент цепи приоритетов банка, наполняя их новым содержанием и воздействуя на связь элементов между собой. Кроме того, технологии влияют на конкурентоспособность банков, изменяя жизненный цикл продукции, предлагаемой клиентам.

Стратегии применения информационных технологий определяют методы, с помощью которых они изменяют современный бизнес, и пути управления этими переменами.

Важным моментом является разработка архитектуры компьютерной системы банка. Под архитектурой системы понимается совокупность ее функциональных компонентов и их взаимодействие друг с другом. Целью разработки архитектуры компьютерной системы банка является создание внутренне логичной и гибкой системы, которая будет следовать за изменениями стратегии деятельности банка с минимальным разрушающим воздействием на нее. Любая архитектура должна сочетаться с стратегией банка и упрощать проведение ее в жизнь.

Появление каждой новой технологии обязательно влечет за собой отказ от существующих систем обработки данных. Естественно, это является барьером на пути внедрения новых разработок. Неуклонно возрастает в связи с этим интерес к стандартизованным и открытым системам, в которых программы и представления данные совместимы и их работа не зависит от поставщика оборудования и программ.

Это направление особенно важно при выработке взаимных соглашений и между организациями и их слиянии. Например, слияния Dutch Postbank и Naturale Nederlanden, английских Lloyds и Abbey Life, германских - Deutsche Bank и Deutsch Lebensversicherung - привели к возникновению проблем, связанных с информационными технологиями. Задача заключается в том, чтобы разработать такую архитектуру, которая свяжет вместе критичную деятельность клиентов и каналы распределения товаров и услуг банка, не нарушая при этом порядка работы организации. [1, с.60]

Во многом прибыльность банка зависит от обеспечения высшего руководства нужной, своевременной и точной информацией. Системы управления информацией должны быть действительными помощниками в деятельности банка, обеспечивая, например, информацию о положении на рынке, прибыльности банковской продукции, состоянии клиентов и т.д. Получаемая с их помощью информация может использоваться банком для улучшения обслуживания клиентов или для представления им с целью использования в собственных интересах.

Банкам необходима постоянная информация о степени риска их деятельности. Оценка риска — это процесс, который коренным образом может быть изменен с помощью современных технологий. В него могут быть вовлечены более «интеллектуальные» системы, которые способны оценивать процентные ставки, курсы валют, кредитоспособность клиента и т.п., выдавая при этом рекомендации относительно возможных действий и их результатов.

Современные технологии дают банкам огромные преимущества в организации систем доставки товаров и услуг. Использование электронных средств связи позволяет реализовать:

1. электронные платежи и расчеты в точке продажи;
2. клиентские терминалы, осуществляющие прямую связь с банком;
3. домашнее банковское обслуживание с помощью персонального компьютера или телефона;
4. обмен электронными данными в сети с расширенным набором услуг;
5. технологии электронных банковских карт, включая магнитные пластиковые и интеллектуальные карты.

Реализация этих и других методов банковского обслуживания в конкретных системах требует разработки жестких мер защиты для предотвращения случайных и умышленных нарушений их функционирования.

Одна из важных проблем банков сегодня - это управление инвестициями в электронные банковские системы с тем, чтобы последние полностью отражали перемены в банковской индустрии. Успех на новых стратегических направлениях бизнеса во многом зависит от реализации информационных систем.

# Глава 3. Человеческий фактор в обеспечении информационной безопасности.

## Угрозы информационной безопасности банка со стороны персонала.

Преступления, в том числе в информационной сфере, совершаются людьми. Большинство систем не может нормально функционировать без участия человека. Пользователь системы, с одной стороны, — ее необходимый элемент, а с другой — он же является причиной и движущей силой нарушения или преступления. Вопросы безопасности систем (компьютерных в том числе), таким образом, большей частью есть вопросы человеческих отношений и человеческого поведения. Особенно это актуально в сфере информационной безопасности, т.к. утечка информации в подавляющем большинстве случаев происходит по вине сотрудников банков.

Анализ сообщений средств массовой информации и оперативных сводок правоохранительных органов о криминальных и диверсионно-террористических актах про­тив коммерческих структур в Москве и других городах России позволяет сделать однозначный вывод о высо­кой степени осведомленности преступников относите­льно режима дня и динамики деятельности предприни­мателей: жертв, как правило, неизменно встречали в районе проживания или места работы, либо с пред­ельной точностью по времени и месту перехватывали на трассе.

Заблаговременно были изучены основные и запас­ные маршруты перемещения коммерсантов. Преступ­ники располагали подробными сведениями о составе семьи и родственниках будущих жертв, марках и но­мерных знаках личных и служебных автомашин, сосе­дях и т.п.

Неотъемлемым составляющим элементом любой планируемой преступной акции является сбор инфор­мации. Представляется возможным выделить следу­ющие основные методы, которые используются зло­умышленниками в настоящее время для добывания сведений о коммерческих структурах:

1. наблюдение, в том числе с помощью мобильных и стационарных оптико-технических средств, скрытое фотографирование, видеозапись; выведывание информации;
2. проведение опросов, интервьюирования, анкетиро­вания, «направленных» бесед и т.п.;
3. хищение, скрытое копирование, подделка каких-ли­бо внутренних документов лицами, внедренными или приобретенными в коммерческих структурах, которые согласились или оказались вынужденными осуществ­лять указанные действия по корыстным побуждениям, в результате угроз, по физическому принуждению либо иным причинам;
4. перехват информации на различных частотных ка­налах внутренней и внешней радио- и телевизионной связи коммерческих структур;
5. получение информации техническими средствами путем использования различных источников сигналов в помещениях коммерческих структур как связанных с функционирующей аппаратурой (персональные ком­пьютеры), так и через специально внедренную технику негласного съема информации (спецзакладки, в том числе дистанционного управления);
6. добывание информации о коммерческих структурах посредством применения системы аналитических ме­тодов (структурный анализ, финансовый анализ, ана­лиз себестоимости продукции, анализ научно-техничес­ких образцов, оценка квалификационных особенностей рабочих и служащих, изучение основных материаль­ных фондов и т.п.).

При всем многообразии и несомненных достоинст­вах вышеперечисленных методов в настоящее время все же использование сотрудников коммерческих струк­тур в качестве источников внутренней информации рас­сматривается как наиболее надежный, быстрый и эффек­тивных способ получения конфиденциальных данных.

Отметим также, что кроме добывания собственно конфиденциальной информации по различным вопро­сам такой внутренний источник из числа сотрудников коммерческих организаций может быть одновременно использован для получения уточняющих сведений, ко­торые бы дополняли данные, добытые техническими средствами и иными методами.

Помимо этого агентурные информационные источ­ники сегодня все более активно и настойчиво использу­ются для оказания выгодного криминальным структу­рам, а также конкурентам влияния на стратегию и так­тику поведения руководителей соответствующих ком­мерческих предприятий, а также для воздействия на позицию лиц, принимающих ответственные решения в сфере налогообложения, таможенной политики, экс­портно-импортных квот, землеотвода и т.д. [4, с.268]

При анализе нарушений защиты большое внимание следует уделять не только самому факту как таковому (то есть объекту нарушения), но и личности нарушителя, то есть субъекту нарушения. Такое внимание поможет разобраться в побудительных мотивах и, может быть, даст возможность избежать в дальнейшем повторения подобных ситуаций. Ценность такого анализа обуславливается еще и тем, что совершаемые без причины преступления (если речь не идет о халатности) очень и очень редки. Исследовав причину преступлений или нарушений можно либо повлиять на саму причину (если это возможно), либо ориентировать систему защиты именно на такие виды преступлений или нарушений.

Прежде всего, кто бы ни был источником нарушения, какое бы оно не было, все нарушители имеют одну общую черту -доступ к системе. Доступ может быть разным, с разными правами, к разным частям системы, через сеть, но он должен быть.

По данным Datapro Information Services Group [2] 81.7% нарушений совершаются самими служащими организации, имеющими доступ к ее системе, и только 17.3% нарушений совершаются лицами со стороны (1% приходится на случайных лиц). По другим данным, физическое разрушение составляет около 25% нарушений (пожар, наводнение, порча) и только 1-2% составляют нарушения со стороны посторонних лиц. На долю служащих, таким образом, остается 73-74% всех преступлений. Различаясь в цифрах, результаты обоих исследований говорят об одном: главный источник нарушений — внутри самой АСОИБ. И вывод отсюда также однозначен: неважно, есть ли у АСОИБ связи с внешним миром и есть ли внешняя защита, но внутренняя защита должна быть обязательно.

Можно выделять четыре основные причины нарушений: безответственность, самоутверждение, месть и корыстный интерес пользователей (персонала) АСОИБ.

При нарушениях, вызванных безответственностью, пользователь целенаправленно или случайно производит какие-либо разрушающие действия, не связанные тем не менее со злым умыслом. В большинстве случаев это следствие некомпетентности или небрежности. Маловероятно, чтобы разработчики системы защиты могли предусмотреть все такие ситуации. Более того, во многих случаях система в принципе не может предотвратить подобные нарушения (например, случайное уничтожение своего собственного набора данных). Иногда ошибки поддержки адекватной защищенной среды могут поощрять такого рода нарушения. Даже лучшая система защиты будет скомпрометирована, если она неграмотно настроена. Наряду с неподготовленностью пользователей к точному соблюдению мер защиты, это обстоятельство может сделать систему уязвимой к этому виду нарушений.

Некоторые пользователи считают получение доступа к системным наборам данных крупным успехом, затевая своего рода игру «пользователь против системы» ради самоутверждения либо в собственных глазах, либо в глазах коллег. Хотя намерения могут быть и безвредными, эксплуатация ресурсов АСОИБ считается нарушением политики безопасности. Пользователи с более серьезными намерениями могут найти конфиденциальные данные, попытаться испортить или уничтожить их при этом. Такой вид нарушения называется зондированием системы. Большинство систем имеет ряд средств противодействия подобным «шалостям». В случае необходимости администратор защиты использует их временно или постоянно.

Нарушение безопасности АСОИБ может быть вызвано и корыстным интересом пользователя системы. В этом случае он будет целенаправленно пытаться преодолеть систему защиты для доступа к хранимой, передаваемой и обрабатываемой в АСОИБ информации. Даже если АСОИБ имеет средства, делающие такое проникновение чрезвычайно сложным, полностью защитить ее от проникновения практически невозможно. Тот, кому успешно удалось проникновение — очень квалифицирован и опасен. Проникновение — опаснейший вид нарушений, правда, он встречается чрезвычайно редко, так как требуют необычайного мастерства и упорства.

Как показывает практика, ущерб от каждого вида нарушений обратно пропорционален его частоте: чаще всего встречаются нарушения, вызванные халатностью и безответственностью, обычно ущерб от них незначителен и легко восполняется. Например, случайно уничтоженный набор данных можно восстановить, если сразу заметить ошибку. Если информация имеет важное значение, то необходимо хранить регулярно обновляемую резервную копию, тогда ущерб вообще практически незаметен.

Ущерб от зондирования системы может быть гораздо больше, но и вероятность его во много раз ниже. Для таких действий необходима достаточно высокая квалификация, отличное знание системы защиты и определенные психологические особенности. Наиболее характерным результатом зондирования системы является блокировка: пользователь в конце концов вводит АСОИБ в состояние зависания, после чего операторы и системные программисты должны тратить много времени для восстановления работоспособности системы.

Проникновение — наиболее редкий вид нарушений, но и наиболее опасный. Отличительной чертой проникновении обычно является определенная цель: доступ (чтение, модификация, уничтожение) к определенной информации, влияние на работоспособность системы, слежение за действиями других пользователей и др. Для выполнения подобных действий нарушитель должен обладать теми же качествами, что и для зондирования системы, только в усиленном варианте, а также иметь точно сформулированную цель. В силу этих обстоятельств ущерб от проникновении может оказаться в принципе невосполнимым. Например, для банков это может быть полная или частичная модификация счетов с уничтожением журнала транзакций.

Таким образом, для организации надежной защиты необходимо четко отдавать себе отчет, от каких именно нарушений важнее всего избавиться, Для защиты от нарушений, вызванных халатностью нужна минимальная защита, для защиты от зондирования системы — более жесткая и самая жесткая вместе с постоянным контролем — от проникновении. Целью таких действий должно служить одно — обеспечение работоспособности АСОИБ в целом и ее системы защиты в частности.

Причины, побудившие пользователя совершить нарушение или даже преступление, могут быть совершенно различными. Как уже отмечалось, около 86% нарушений составляют неумышленные ошибки, вызванные небрежностью, недостаточной компетентностью, безответственностью и т.д. Но не это составляет основную угрозу для системы. Гораздо более серьезным может быть ущерб, нанесенный в результате умышленного воздействия из-за обиды, неудовлетворенности своим служебным или материальным положением или по указанию других лиц. Причем ущерб этот будет тем больше, чем выше положение пользователя в служебной иерархии. Это только некоторые из возможных причин, побуждающих пользователей идти на нарушение правил работы с системой.

Способы предотвращения нарушений вытекают из природы побудительных мотивов — это соответствующая подготовка пользователей, а также поддержание здорового рабочего климата в коллективе, подбор персонала, своевременное обнаружение потенциальных злоумышленников и принятие соответствующих мер. Первая из них - задача администрации системы, вторая — психолога и всего коллектива в целом. Только в случае сочетания этих мер имеется возможность не исправлять нарушения и не расследовать преступления, а предотвращать саму их причину.

При создании модели нарушителя и оценке риска потерь от действий персонала необходимо дифференцировать всех сотрудников по их возможностям доступа к системе и, следовательно, по потенциальному ущербу от каждой категории пользователей. Например, оператор или программист автоматизированной банковской системы может нанести несравненно больший ущерб, чем обычный пользователь, тем более непрофессионал.

Ниже приводится примерный список персонала типичной АСОИБ и соответствующая степень риска от каждого из них [3].

1. Наибольший риск:

- системный контролер;

- администратор безопасности.

2. Повышенный риск:

- оператор системы;

- оператор ввода и подготовки данных;

- менеджер обработки;

- системный программист.

3. Средний риск:

- инженер системы;

- менеджер программного обеспечения.

4. Ограниченный риск:

- прикладной программист;

- инженер или оператор по связи;

- администратор баз данных;

- инженер по оборудованию;

- оператор периферийного оборудования;

- библиотекарь системных магнитных носителей;

- пользователь-программист;

- пользователь-операционист.

5. Низкий риск:

- инженер по периферийному оборудованию;

- библиотекарь магнитных носителей пользователей;

- пользователь сети.

Каждый из перечисленных выше пользователей в соответствии со своей категорией риска может нанести больший или меньший ущерб системе. Однако пользователи различных категорий различаются не только по степени риска, но и по тому, какому элементу системы они угрожают больше всего. Понятно, что операционист вряд ли сможет вывести из строя АСОИБ, но зато способен послать платеж не по адресу и нанести серьезный финансовый ущерб.

## Кадровая политика с точки зрения информационной безопасности.

Практика последнего времени свидетельствует о том, что различные по масштабам, последствиям и значимости виды преступлений и правонарушений так или иначе связаны с конкретными действиями сотрудников коммерческих структур. В связи с этим представляется целесообразным и необходимым в це­лях повышения экономической безопасности этих объектов уделять больше внимания подбору и изуче­ния кадров, проверке любой информации, указыва­ющей на их сомнительное поведение и компромети­рующие связи. При этом необходимо также в обяза­тельном порядке проводить значительную разъясни­тельно-воспитательную работу, систематические инст­руктажи и учения по правилам и мерам безопасности, регулярные, но неожиданные тестирования различных категорий сотрудников по постоянно обновляемым программам.

В контрактах необходимо четко очерчивать персональ­ные функциональные обязанности всех категорий со­трудников коммерческих предприятий и на основе существующего российского законодательства во внутрен­них приказах и распоряжениях определять их ответст­венность за любые виды нарушений, связанных с раз­глашением или утечкой информации, составляющей коммерческую тайну.

Кроме того, в этой связи целесообразно отметить, что ведущие московские коммерческие банки все шире вводят в своих служебных документах гриф «конфиде­нциально» и распространяют различного рода надбав­ки к окладам для соответствующих категорий своего персонала.

Как свидетельствуют многочисленные опросы и проведённые беседы, в настоящее время многие ру­ководители ведущих московских коммерческих струк­тур все более глубоко осознают роль и место своих сотрудников в создании и поддержании общей систе­мы экономической безопасности. Такое понимание этой проблемы ведет к настойчивому внедрению про­цедур тщательного подбора и расстановки персонала.

Так, постепенно приобретают все большую значи­мость рекомендательные письма, научные методы проверки на профпригодность и различного рода те­стирования, осуществляемые кадровыми подразделе­ниями, сотрудниками служб безопасности и группами психологической поддержки, которые созданы в ряде коммерческих структур либо привлекаются в качестве сторонних экспертов.

Несмотря, однако, на некоторые положительные примеры, в целом приходится, к сожалению, констати­ровать тот факт, что руководители подавляющего бо­льшинства коммерческих организаций все же еще не в полной мере осознали необходимость организации комплексной защиты своих структур от уголовных и экономических преступлений и в этой связи потреб­ность постоянного совершенствования процесса под­бора и расстановки кадров.

Как свидетельствует современный опыт, безопа­сность экономической деятельности любой коммер­ческой структуры во многом зависит от того, в какой степени квалификация ее сотрудников, их морально-нравственные качества соответствуют решаемым задачам.

Если объективно оценивать существующие сегодня процедуры отбора кадров, то окажется, что во многих банках и фирмах акцент, к сожалению, делается пре­жде всего на выяснении лишь уровня профессиональ­ной подготовки кандидатов на работу, который опре­деляется зачастую по традиционно-формальным при­знакам: образование; разряд; стаж работы по специальности.

При таком подходе очевидно, что кадровые подра­зделения исходят из все более устаревающей концеп­ции ограниченной материально-финансовой ответст­венности отдельных работников за конечные резуль­таты своей деятельности и сохранность конфиденци­альной информации.

В современных же коммерческих банках при весьма ограниченной численности сотрудников, все более ча­стом совмещении рядовыми исполнителями различ­ных участков работы и стремительно увеличивающих­ся потоках информации и управленческих команд, каж­дый сотрудник во все возрастающей степени становит­ся носителем конфиденциальных сведений, которые могут представлять интерес как для конкурентов, так и криминальных сообществ.

В таких условиях весьма существенно повышаются и изменяются требования к личным и деловым качест­вам сотрудников и, следовательно, к кандидатам на работу. Данное обстоятельство побуждает руководи­телей коммерческих структур все чаще обращаться к методам и процедурам научной психологии, с помо­щью которых можно достаточно быстро, надежно и всесторонне оценивать возможного кандидата и со­ставлять его психологический портрет.

Конечно, было бы ошибкой полагать, что психоло­гический отбор полностью заменяет прежние, достато­чно надежные кадровые процедуры. В этой связи под­черкнем, что только при умелом сочетании психологи­ческих и традиционных кадровых подходов можно с высокой степенью достоверности прогнозировать по­ведение сотрудников в различных, в том числе экст­ремальных, ситуациях.

В настоящее время ведущие банковские струк­туры имеют, как правило, строго разработанные и ут­вержденные руководством организационные структу­ры и функции управления для каждого подразделения. Наибольшей популярностью пользуются методики со­ставления оргсхем или организационных чертежей, на которых графически изображается каждое рабочее ме­сто, прописываются должностные обязанности и опре­деляются информационные потоки для отдельного ис­полнителя.

При такой схеме управления и контроля предельно ясно, на каком участке (отдел, служба, управление) требуется специалист соответствующей квалификации и какой информацией он должен располагать для вы­полнения функций на своем рабочем месте. Внутрен­ними распоряжениями также определяются требова­ния к деловым и личным качествам сотрудников и обусловливаются режимы сохранения или коммерчес­кой тайны.

Кроме того, для большей конкретизации этих про­цедур на каждое рабочее место рекомендуется состав­лять профессиограмму, т.е. перечень личностных ка­честв, которыми в идеале должен обладать потенциаль­ный сотрудник. Содержательная сторона и глубина проработки профессиограмм могут быть различными. Это зависит в первую очередь от того, на какое рабо­чее место они составляются.

Однако обязательными атрибутами подобных до­кументов являются разделы, отражающие профессио­нально значимые качества (психологические характери­стики, свойства личности, без которых невозможно выполнение основных функциональных обязанностей), а также противопоказания (личностные качества, кото­рые делают невозможным зачисление кандидата на кон­кретную должность). В некоторых случаях необходимо не только указывать профессионально значимые каче­ства, но и оценивать степень их выраженности, т.е. сформированности.

После разработки схем управления и составления профессиограмм можно приступать к собеседованиям и применять разнообразные процедуры отбора кан­дидатов на работу. Как правило, проблема отбора кадров встает перед руководителями банков в двух основных случаях: создание новых подразделений, замещение вакантных должностей. Для первого случая характерно, как правило, изуче­ние значительного числа кандидатур, для которых из набора имеющихся вакансий подбирается соответст­вующая должность. Во втором случае из ограничен­ного числа кандидатов отбирается тот, который по своим личным и профессиональным качествам в на­ибольшей степени соответствует требованиям профессиограммы данного рабочего места.

Проблема состоит в том, что даже весьма опыт­ные работники кадровых подразделений не всегда мо­гут правильно, достоверно и быстро оценить подлин­ное психическое состояние лиц, пришедших на собеседо­вание. Этому способствуют повышенное волнение, склонность отдельных кандидатов к предвзятым оцен­кам характера деятельности некоторых коммерческих структур, но особенно широкое и зачастую бесконт­рольное самолечение различных психосоматических расстройств с использованием в ряде случаев весьма сильных психотропных препаратов. В этой связи веду­щие московские коммерческие банки требуют от кан­дидатов предоставления справок о состоянии здоровья либо сами выдают направления в определенные поликлиники с рекомендацией прохождения полной диспан­серизации (за счет кандидата).

С точки зрения обеспечения страте­гических интересов коммерческой структуры являются обязательными следующие функции службы безопас­ности:

- определение степени вероятности формирования у кандидата преступных наклонностей в случаях воз­никновения в его окружении определенных благопри­ятных обстоятельств (персональное распоряжение кре­дитно-финансовыми ресурсами, возможность контро­ля за движением наличных средств и ценных бумаг, доступ к материально-техническим ценностям, работа с конфиденциальной информацией и пр.);

- выявление имевших место ранее преступных на­клонностей, судимостей, связей с криминальной сре­дой (преступное прошлое, наличие конкретных суди­мостей, случаи афер, махинаций, мошенничества, хи­щений на предыдущем месте работы кандидата и уста­новление либо обоснованное суждение о его возмож­ной причастности к этим преступным деяниям).

Для добывания подобной информации использу­ются возможности различных подразделений банковских структур, в первую очередь службы безопасности, отдела кадров, юридического отдела, под­разделений медицинского обеспечения, а также не­которых сторонних организаций, например, детек­тивных агентств, бюро по занятости населения, диспансеров и пр.

Очевидно также, что представители банковских структур должны быть абсолютно уверены в том, что проводят тесты, собеседования и встречи именно с те­ми лицами, которые выступают в качестве кандидатов на работу. Это подразумевает тщательную проверку паспортных данных, иных документов, а также получе­ние фотографий кандидатов без очков, контактных линз, парика, макияжа.

Рекомендуется настаивать на получении набора цветных фотографий кандидата, которые могут быть использованы в случае необходимости для предъявле­ния жильцам по месту его проживания или коллегам по работе. Использование в кадровой работе цветных фотографий, соответствующих паспортным данным, предпочтительнее также в связи с тем, что они четко и без искажений передают цвет волос, глаз, кожи, возраст и характерные приметы кандидата.

В практике уже известны случаи, когда для допол­нительного анализа анкеты кандидата и его фотогра­фий руководители банковских структур приглашали высокопрофессиональных юристов, графологов, из­вестных психоаналитиков с целью обеспечения максимальной полноты формулировок окончательного заключения и выявления возможных скрытых противоречий в характере проверяемого лица.

В том случае, если результаты указанных проверок, тестов и психологического изучения не противоречат друг другу и не содержат данных, которые бы препят­ствовали приему на работу данного кандидата, с ним заключается трудовое соглашение, в большинстве слу­чаев предусматривающее определенный испытатель­ный срок (1-3 месяца).

Необходимо также подчеркнуть следующее важное обстоятельство - лица, принима­емые на ответственные вакантные должности в ком­мерческих структурах (члены правлений, главные бух­галтеры, консультанты, начальники служб безопасно­сти и охраны, руководители компьютерных центров и цехов, помощники и секретари первых лиц) сегодня подвергаются, как правило, следующей стандартной проверке, включающей:

1. достаточно продолжительные процедуры сбора и верификации установочно-биографических сведений с их последующей аналитической обработкой;
2. предоставление рекомендательных писем от извест­ных предпринимательских структур с их последующей проверкой;
3. проверки по учетам правоохранительных органов; установки по месту жительства и по предыдущим местам работы;
4. серии собеседований и тестов с последующей пси­хоаналитической обработкой результатов.

По мнению экспертов, даже каждый, взятый в от­дельности из упомянутых методов проверки доста­точно эффективен. В совокупности же достигается весьма высокая степень достоверности информации о профессиональной пригодности и надежности ка­ндидата, его способностях к творческой работе на конкретном участке в соответствующем коммерческом предприятии.

Серьезное влияние на вопросы безопасности ком­мерческих предприятий оказывают процедуры уволь­нения сотрудников. К сожалению, отдельных руково­дителей порой мало интересуют чувства и пережива­ния персонала, который по тем или иным причинам попадает под сокращение или самостоятельно изъяв­ляет желание покинуть банк или акционерное обще­ство. Как показывает опыт, такой подход приводит, как правило, к серьезным негативным последствиям.

Современные психологические подходы к процессу увольнения позволяют выработать следующую при­нципиальную рекомендацию: каковы бы ни были причи­ны увольнения сотрудника, он должен покидать коммер­ческую организацию без чувства обиды, раздражения и мести.

Только в этом случае можно надеяться на то, что увольняемый сотрудник не предпримет необдуманных шагов и не проинформирует правоохранительные ор­ганы, налоговую инспекцию, конкурентов, криминаль­ные структуры об известных ему аспектах работы банка. Кроме того, известны случаи мести бывших сотрудников с использованием компьютерного проникновения.

Таким образом, представители кадровых подраз­делений и служб безопасности должны быть четко ориентированы на выяснение истинных мотивов уво­льнения всех категорий сотрудников. Зачастую причи­ны, на которые ссылается сотрудник при увольнении, и подлинные мотивы, побудившие его к такому шагу, существенно отличаются друг от друга. Обычно лож­ный защитный мотив используется потому, что со­трудник в силу прежних привычек и традиций опасает­ся неправильной интерпретации своих действий со сто­роны руководителей и коллег по работе.

Наряду с этим весьма часто имеют место случаи, когда сотрудник внутренне сам уверен в том, что увольняется по откровенно называемой им причине, хотя его решение сформировано и принято под влия­нием совершенно иных, порой скрытых от него обсто­ятельств. Так, в практике уже известны случаи весьма тонких и тайных комбинаций оказания влияния на высококвалифицированных специалистов с целью их переманивания на другое место работы.

В этой связи принципиальная задача состоит в том, чтобы определить истинную причину увольнения со­трудника, попытаться правильно ее оценить и решить, целесообразно ли в данной ситуации предпринимать попытки к искусственному удержанию данного лица в коллективе либо отработать и реализовать процеду­ру его спокойного и бесконфликтного увольнения. Ре­шение рекомендуется принимать на основе строго объективных данных в отношении каждого конкрет­ного сотрудника.

При поступлении устного или письменного заявле­ния об увольнении рекомендуется во всех без исключе­ниях случаях провести с сотрудником беседу с участи­ем представителя кадрового подразделения и кого-ли­бо из руководителей коммерческой структуры. Однако до беседы целесообразно предпринять меры по сбору следующей информации об увольняющемся сотруднике:

- характер его взаимоотношений с коллегами в кол­лективе; отношение к работе; уровень профессиональной подготовки; наличие конфликтов личного или служебного хара­ктера;

- ранее имевшие место высказывания или пожелания перейти на другое место работы;

- доступ к информации, в том числе составляющей коммерческую тайну;

- вероятный период устаревания сведений, составля­ющих коммерческую тайну для данного предприятия; предполагаемое в будущем место работы увольня­ющегося (увольняемого) сотрудника.

Беседа при увольнении проводится лишь только после того, когда собраны все необходимые сведения. Конечно, предварительно руководитель коммерческой структуры отрабатывает принципиальный подход к вопросу о том, целесообразно ли предпринимать попытки склонить сотрудника изменить его первона­чальное решение либо санкционировать оформление его увольнения. В любом случае рекомендуется дать собеседнику высказаться и в развернутой форме объяс­нить мотивы своего решения. При выборе места про­ведения беседы предпочтение отдается, как правило, служебным помещениям.

В зависимости от предполагаемого результата беседа может проводиться в официальном тоне либо иметь форму доверительной беседы, задушевного разговора, обмена мнениями. Однако каковы бы ни были планы в отношении данного сотрудника, раз­говор с ним должен быть построен таким образом, чтобы последний ни в коей мере не испытывал чувства униженности, обиды, оскорбленного достоинства. Для этого следует сохранять тон беседы предельно кор­ректным, тактичным и доброжелательным, даже не­смотря на любые критические и несправедливые заме­чания, которые могут быть высказаны сотрудником в адрес банковской структуры и ее конкретных менеджеров.

Если менеджером банка, отделом кадров и службой безопасности все же принято решение не препятствовать увольнению сотрудника, а по своему служебному положению он располагал доступом к конфиденциальной информации, то в этом случае от­рабатывается несколько вариантов сохранения в тайне коммерческих сведений (оформление официальной подписи о неразглашении данных, составляющих ком­мерческую тайну, либо устная «джентльменская» до­говоренность о сохранении увольняемым сотрудником лояльности к «своему банку или фирме»).

В этой связи необходимо подчеркнуть, что личное обращение к чувству чести и достоинства увольняемых лиц наиболее эффективно в отношении тех индивиду­умов, которые обладают темпераментом сангвиника и флегматика, высоко оценивающих, как правило, до­верие и доброжелательность.

Что касается лиц с темпераментом холерика, то с этой категорией сотрудников рекомендуется завер­шать беседу на официальной ноте. В ряде случаев объявление им принятого решения об увольнении вы­зывает бурную негативную реакцию, связанную с по­пытками спекулировать на своих истинных, а порой и мнимых профессиональных достоинствах. Поэтому с сотрудниками такого темперамента и склада харак­тера целесообразно тщательно оговаривать и обуслов­ливать в документах возможности наступления для них юридических последствий раскрытия коммерчес­кой тайны.

Несколько иначе рекомендуется действовать в тех случаях, когда увольнения сотрудников происходят по инициативе самих коммерческих структур. В этих об­стоятельствах не следует поспешно реализовывать принятое решение. Если увольняемое лицо располага­ет какими-либо сведениями, составляющими коммерческую тайну, то целесообразно предварительно и под соответствующим предлогом перевести его на другой участок работы, например в такое подразделение, в ко­тором отсутствует подобная информация.

Кроме того, таких лиц традиционно стремятся со­хранить в структуре банка или фирмы (их дочерних предприятий, филиалов) до тех пор, пока не будут приняты меры к снижению возможного ущерба от разглашения ими сведений, составляющих коммерчес­кую тайну, либо найдены адекватные средства защиты конфиденциальных данных (технические, администра­тивные, патентные, юридические, финансовые и пр.).

Только лишь после реализации этих мер рекомен­дуется приглашать на собеседование подлежащего уво­льнению сотрудника и объявлять конкретные причи­ны, по которым коммерческая организация отказыва­ется от его услуг. Желательно при этом, чтобы эти причины содержали элементы объективности, достове­рности и проверяемости (перепрофилирование произ­водства, сокращение персонала, ухудшение финансово­го положения, отсутствие заказчиков и пр.). При моти­вации увольнения целесообразно, как правило, воздер­живаться от ссылок на негативные деловые и личные качества данного сотрудника.

После объявления об увольнении рекомендуется внимательно выслушивать контрдоводы, аргументы и замечания сотрудника в отношении характера рабо­ты, стиля руководства компанией и т. п. Обычно уво­льняемый персонал весьма критично, остро и правдиво освещает ситуацию в коммерческих структурах, вскры­вая уязвимые места, серьезные недоработки, кадровые просчеты, финансовые неурядицы и т. п.

Если подходить не предвзято и объективно к подо­бной критике, то эти соображения могут быть исполь­зованы в дальнейшем весьма эффективно в интересах самого банка. В ряде случаев увольняемому со­труднику вполне серьезно предлагают даже изложить письменно свои рекомендации, конечно, за соответст­вующее вознаграждение.

При окончательном расчете обычно рекомендуется независимо от личностных характеристик увольняемых сотрудников брать у них подписку о неразглашении конфиденциальных сведений, ставших известными в процессе работ.

В любом случае после увольнения сотрудников, осведомленных о сведениях, составляющих коммер­ческую тайну, целесообразно через возможности служ­бы безопасности банка или фирмы (частного детектив­ного агентства) проводить оперативную установку по их новому месту работы и моделировать возможности утечки конфиденциальных данных.

Кроме того, в наиболее острых и конфликтных ситуациях увольнения персонала проводятся оператив­ные и профилактические мероприятия по новому месту работы, жительства; также в окружении носителей коммерческих секретов.

Персонал оказывает су­щественное, а в большинстве случаев даже решающее влияние на информационную безопасность банка. В этой связи подбор кадров, их изучение, рас­становка и квалифицированная работа при увольнени­ях в значительной степени повышают устойчивость коммерческих предприятий к возможному стороннему негативному влиянию и агентурному проникновению противоправных элементов.

Регулярное изучение всех категорий персонала, по­нимание объективных потребностей сотрудников, их ведущих интересов, подлинных мотивов поведения и выбор соответствующих методов объединения от­дельных индивидуумов в работоспособный коллек­тив — все это позволяет руководителям в итоге ре­шать сложные производственные и коммерческо-финансовые задачи, в том числе связанные с обеспечением экономической безопасности.

Обобщая основные рекомендации, представляется, что программа работы с персоналом в коммерческой структуре могла бы быть сформулирована следующим образом:

- добывание в рамках действующего российского за­конодательства максимального объема сведений о ка­ндидатах на работу, тщательная проверка представ­ленных документов как через официальные, так и опе­ративные возможности, в том числе службы безопас­ности банка или частного детективного агент­ства, системность в анализе информации, собранной на соответствующие кандидатуры;

- проведение комплекса проверочных мероприятий в отношении кандидатов на работу, их родственников, бывших сослуживцев, ближайшего окружения в тех случаях, когда рассматривается вопрос об их приеме на руководящие должности или допуске к информа­ции, составляющей коммерческую тайну;

- использование современных методов, в частности собеседований и тестирований, для создания психоло­гического портрета кандидатов на работу, который бы позволял уверенно судить об основных чертах харак­тера и прогнозировать их вероятные действия в раз­личных экстремальных ситуациях;

- оценка с использованием современных психологи­ческих методов разноплановых и разнопорядковых фа­кторов, возможно препятствующих приему кандида­тов на работу или их использованию на конкретных должностях;

- определение для кандидатов на работу в коммер­ческих структурах некоторого испытательного срока с целью дальнейшей проверки и выявления деловых и личных качеств, иных факторов, которые бы могли препятствовать зачислению на должность;

- введение в практику регулярных и неожиданных комплексных проверок персонала, в том числе через возможности служб безопасности;

- обучение сотрудников кадровых подразделений и служб безопасности современным психологическим подходам к работе с персоналом, социальным, психо­аналитическим, этико-моральным методам, навыкам использования современных технических средств для фиксирования результатов интервью и собеседований, приемам проведения целевых бесед «втемную» и про­цедурам информационно-аналитической работы с до­кументами кандидатов;

- выделение из числа первых руководителей ком­мерческих структур куратора кадровой работы для осуществления контроля за деятельностью кадровых подразделений и служб безопасности при работе с пе­рсоналом.

Можно сделать определенный вывод о том, что российские предприниматели во все возрастающей степени меняют свое отношение к «человеческому фак­тору», ставят на вооружение своих кадровых подраз­делений и служб безопасности современные методы работы с персоналом. Очевидно, что дальнейшее раз­витие в этой области связано с активным использова­нием значительного потенциала методов психоанали­за, психологии и этики управления, конфликтологии и ряда других наук и более полного интегрирования соответствующих специалистов в коммерческие пред­приятия.

# Глава 4. Безопасность автоматизированных систем обработки информации в банках (АСОИБ).

## Угрозы безопасности автоматизированных систем.

Не будет преувеличением сказать, что проблема умышленных нарушений функционирования АСОИБ различного назначения в настоящее время является одной из самых актуальных. Наиболее справедливо это утверждение для стран с сильно развитой информационной инфраструктурой, о чем убедительно свидетельствуют приводимые ниже цифры.

По данным, приведенным в [2], в 1992 году ущерб от компьютерных преступлений составил $555 млн., 930 лет рабочего времени и 15.3 года машинного времени. По другим данным ущерб финансовых организаций составляет от $173 млн. до $41 млрд. в год [3].

В настоящей главе приводится классификация умышленных угроз безопасности АСОИБ и их краткое описание. Классификация не является исчерпывающей. Она предназначена для того, чтобы выделить основные типы угроз и методы защиты от них.

Современная АСОИБ — сложный механизм, состоящий из большого количества компонентов различной степени автономности, связанных между собой и обменивающихся данными. Практически каждый из них может выйти из строя или подвергнуться внешнему воздействию.

Под угрозой безопасности понимается потенциально возможное воздействие на АСОИ, которое может прямо или косвенно нанести урон пользователям или владельцам АСОИБ.

Приводимая ниже классификация охватывает только умышленные угрозы безопасности АСОИБ, оставляя в стороне такие воздействия как стихийные бедствия, сбои и отказы оборудования и др. Реализацию угрозы в дальнейшем будем называть атакой.

Угрозы безопасности АСОИБ можно классифицировать по следующим признакам [3]:

1. По цели реализации угрозы. Реализация той или иной угрозы безопасности АСОИБ может преследовать следующие цели:

- нарушение конфиденциальности информации. Информация, хранимая и обрабатываемая в АСОИБ, может иметь большую ценность для ее владельца. Ее использование другими лицами наносит значительный ущерб интересам владельца;

- нарушение целостности информации. Потеря целостности информации (полная или частичная, компрометация, дезинформация) -угроза близкая к ее раскрытию. Ценная информация может быть утрачена или обесценена путем ее несанкционированного удаления или модификации. Ущерб от таких действий может быть много больше, чем при нарушении конфиденциальности,

- нарушение (частичное или полное) работоспособности АСОИБ (нарушение доступности). Вывод из строя или некорректное изменение режимов работы компонентов АСОИБ, их модификация или подмена могут привести к получению неверных результатов, отказу АСОИБ от потока информации или отказам при обслуживании. Отказ от потока информации означает непризнание одной из взаимодействующих сторон факта передачи или приема сообщений. Имея в виду, что такие сообщения могут содержать важные донесения, заказы, финансовые согласования и т.п., ущерб в этом случае может быть весьма значительным. Так как диапазон услуг, предоставляемых современными АСОИБ, весьма широк, отказ в обслуживании может существенно повлиять на работу пользователя.

2. По принципу воздействия на АСОИБ:

- с использованием доступа субъекта системы (пользователя, процесса) к объекту (файлу данных, каналу связи и т.д.);

- с использованием скрытых каналов.

Под доступом понимается взаимодействие между субъектом и объектом (выполнение первым некоторой операции над вторым), приводящее к возникновению информационного потока от второго к первому.

Под скрытым каналом (covert channel) понимается путь передачи информации, позволяющий двум взаимодействующим процессам обмениваться информацией таким способом, который нарушает системную политику безопасности. Скрытые каналы бывают двух видов:

а. Скрытые каналы с памятью (covert storage channel), позволяющие осуществлять чтение или запись информации другого процесса непосредственно или с помощью промежуточных объектов для хранения информации (временной памяти);

б. Скрытые временные каналы (covert timing channel), при которых один процесс может получать информацию о действиях другого, используя интервалы между какими-либо событиями (например, анализ временного интервала между запросом на ввод-вывод и сообщением об окончании операции позволяет судить о размере вводимой или выводимой информации).

Коренное различие в получении информации с помощью доступа и с помощью скрытых каналов заключается в том, что в первом случае осуществляется взаимодействие субъекта и объекта АСОИБ и, следовательно, изменяется ее состояние. Во втором случае используются лишь побочные эффекты от взаимодействия двух субъектов АСОИБ, что не оказывает влияния на состояние системы.

Отсюда следует, что воздействие, основанное на первом принципе, проще, более информативнее, но от него легче защититься. Воздействие на основе второго принципа отличается трудностью организации, меньшей информативностью и сложностью обнаружения и устранения.

3. По характеру воздействия на АСОИБ. По этому критерию различают активное и пассивное воздействие.

Активное воздействие всегда связано с выполнением пользователем каких-либо действий, выходящих за рамки его обязанностей и нарушающих существующую политику безопасности. Это может быть доступ к определенным наборам данных, программам, вскрытие пароля и т.д. Активное воздействие ведет к изменению состояния системы и может осуществляться либо с использованием доступа (например, к наборам данных), либо как с использованием доступа, так и с использованием скрытых каналов.

Пассивное воздействие осуществляется путем наблюдения пользователем каких-либо побочных эффектов (от работы программы, например) и их анализе. На основе такого рода анализа можно иногда получить довольно интересную информацию. Примером пассивного воздействия может служить прослушивание линии связи между двумя узлами сети. Пассивное воздействие всегда связано только с нарушением конфиденциальности информации в АСОИБ, так как при нем никаких действий с объектами и субъектами не производится. Пассивное воздействие не ведет к изменению состояния системы.

4. По причине появления используемой ошибки защиты.

Реализация любой угрозы возможна только в том случае, если в данной конкретной системе есть какая-либо ошибка или брешь защиты.

Такая ошибка может быть обусловлена одной из следующих причин:

а. Неадекватностью политики безопасности реальной АСОИБ. Это означает, что разработанная для данной АСОИБ политика безопасности настолько не отражает реальные аспекты обработки информации, что становится возможным использование этого несоответствия для выполнения несанкционированных действий. Все системы в той или иной степени имеют несоответствия подобного рода (модель никогда не может точно соответствовать реальной системе), но в одних случаях это не может привести к нарушениям, а в других — может. С другой стороны такие действия нельзя назвать несанкционированными, поскольку защита от них не предусмотрена политикой безопасности и система защиты в принципе не способна их предотвратить. Если такое несоответствие является опасным, то необходимо разработать новую политику безопасности, в которой оно будет не столь явным и сменить средства защиты для реализации новой политики безопасности.

б. Ошибками административного управления, под которыми понимается некорректная реализация или поддержка принятой политики безопасности в данной АСОИБ. Например, согласно политике безопасности, в АСОИБ должен быть запрещен доступ пользователей к определенному набору данных, а на самом деле (по невнимательности администратора безопасности) этот набор данных доступен всем пользователям. Обычно на исправление такой ошибки требуется очень мало времени, как и на ее обнаружение, но ущерб от нее может быть огромен.

в. Ошибками в алгоритмах программ, в связях между ними и т.д., которые возникают на этапе проектирования программы или комплекса программ и благодаря которым их можно использовать совсем не так, как описано в документации. Примером такой ошибки может служить ошибка в программе аутентификации пользователя системой VAX/VMS версии 4.4, когда при помощи определенных действий пользователь имел возможность войти в систему без пароля. В последующих версиях ОС VAX/VMS эта ошибка была исправлена. Такие ошибки могут быть очень опасны, но их трудно найти; чтобы их устранить надо менять программу или комплекс программ.

г. Ошибками реализации алгоритмов программ (ошибки кодирования), связей между ними и т.д., которые возникают на этапе реализации или отладки и которые также могут служить источником недокументированных свойств. Подобные ошибки обнаружить труднее всего.

5. По способу воздействия на объект атаки (при активном воздействии):

- непосредственное воздействие на объект атаки (в том числе с использованием привилегий), например, непосредственный доступ к набору данных, программе, службе, каналу связи и т.д., воспользовавшись какой-либо ошибкой. Такие действия обычно легко предотвратить с помощью средств контроля доступа.

- воздействие на систему разрешений (в том числе захват привилегий). При этом способе несанкционированные действия выполняются относительно прав пользователей на объект атаки, а сам доступ к объекту осуществляется потом законным образом. Примером может служить захват привилегий, что позволяет затем беспрепятственно получить доступ к любому набору данных ил и программе.

- опосредованное воздействие (через других пользователей):

- «маскарад». В этом случае пользователь присваивает себе каким-либо образом полномочия другого пользователя выдавая себя за него;

- «использование вслепую». При таком способе воздействия один пользователь заставляет другого выполнить необходимые действия (которые для системы защиты не выглядят несанкционированными, ведь их выполняет пользователь, имеющий на это право), причем последний о них может и не подозревать. Для реализации этой угрозы может использоваться вирус (вирус выполняет необходимые действия и сообщает тому, кто его внедрил о результате).

Два последних способа, особенно «использование вслепую», чрезвычайно опасны. Для предотвращения подобных действий требуется постоянный контроль как со стороны администраторов и операторов за работой АСОИБ в целом, так и со стороны пользователей за своими собственными наборами данных.

6. По способу воздействия на АСОИБ:

- в интерактивном режиме;

- в пакетном режиме.

Работая с системой, пользователь всегда имеет дело с какой-либо ее программой. Но одни программы составлены так, что пользователь может оперативно воздействовать на ход их выполнения, вводя различные команды или данные, а другие так, что всю информацию приходится задавать заранее. К первым (интерактивным) относятся, например, интерпретаторы командных языков, некоторые утилиты, управляющие программы баз данных и др. В основном это программы, ориентированные на работу с пользователем. Ко вторым (пакетным) относятся в основном системные и прикладные программы, ориентированные на выполнение каких-либо строго определенных действий без участия пользователя.

Воздействия различного рода могут производиться с использованием обоих классов программ. При использовании программ первого класса (например, для атаки на систему при помощи командного интерпретатора) воздействие оказывается более длительным по времени и, следовательно, имеет высокую вероятность обнаружения, но более гибким, позволяющим оперативно менять порядок действий. Воздействие с помощью программ второго класса (например, с помощью вирусов) является кратковременным, трудно диагностируемым, гораздо более опасным, но требует большой предварительной подготовки для того, чтобы заранее предусмотреть все возможные последствия вмешательства.

7. По объекту атаки. Одной из самых главных составляющих нарушения функционирования АСОИБ является объект атаки, то есть компонент АСОИБ, который подвергается воздействию со стороны злоумышленника. Определение объекта атаки позволяет принять меры по ликвидации последствий нарушения, восстановлению этого компонента, установку контроля по предупреждению повторных нарушений и т.д.

Воздействию могут подвергаться следующие компоненты АСОИБ:

а. АСОИБ в целом - злоумышленник пытается проникнуть в систему для последующего выполнения каких-либо несанкционированных действий. Для этого обычно используются метод «маскарада», перехват или подделка пароля, взлом или доступ к АСОИБ через сеть.

б. Объекты АСОИБ - данные или программы в оперативной памяти или на внешних носителях, сами устройства системы, как внешние (дисководы, сетевые устройства, терминалы), так и внутренние (оперативная память, процессор), каналы передачи данных. Воздействие на объекты системы обычно имеет целью доступ к их содержимому (нарушение конфиденциальности или целостности обрабатываемой или хранимой информации) или нарушение их функциональности, например, заполнение всей оперативной памяти компьютера бессмысленной информацией или загрузка процессора компьютера задачей с неограниченным временем исполнения (нарушение доступности АСОИБ).

в. Субъекты АСОИБ — процессы и подпроцессы пользователей. Целью таких атак является либо прямое воздействие на работу процесса — его приостановка, изменение привилегий или характеристик (приоритета, например), либо обратное воздействие — использование злоумышленником привилегий, характеристик и т.д. другого процесса в своих целях. Частным случаем такого воздействия является внедрение злоумышленником вируса в среду другого процесса и его выполнение от имени этого процесса. Воздействие может осуществляться на процессы пользователей, системы, сети.

г. Каналы передачи данных — пакеты данных, передаваемые по каналу связи и сами каналы. Воздействие на пакеты данных может рассматриваться как атака на объекты сети, воздействие на каналы — специфический род атак, характерный для сети. К нему относятся: прослушивание канала и анализ трафика (потока сообщений) — нарушение конфиденциальности передаваемой информации; подмена или модификация сообщений в каналах связи и на узлах ретрансляторах — нарушение целостности передаваемой информации; изменение топологии и характеристик сети, правил коммутации и адресации —нарушение доступности сети.

8. По используемым средствам атаки.

Для воздействия на систему злоумышленник может использовать стандартное программное обеспечение или специально разработанные программы. В первом случае результаты воздействия обычно предсказуемы, так как большинство стандартных программ АСОИБ хорошо изучены. Использование специально разработанных программ связано с большими трудностями, но может быть более опасным, поэтому в защищенных системах рекомендуется не допускать добавление программ в АСОИБ без разрешения администратора безопасности системы.

9. По состоянию объекта атаки. Состояние объекта в момент атаки может оказать существенное влияние на результаты атаки и на работу по ликвидации ее последствий. Объект атаки может находиться в одном из трех состояний:

а. Хранения — на диске, магнитной ленте, в оперативной памяти или любом другом месте в пассивном состоянии. При этом воздействие на объект обычно осуществляется с использованием доступа;

б. Передачи — по линии связи между узлами сети или внутри узла. Воздействие предполагает либо доступ к фрагментам передаваемой информации (например, перехват пакетов на ретрансляторе сети), либо просто прослушивание с использованием скрытых каналов;

в. Обработки — в тех ситуациях, когда объектом атаки является процесс пользователя.

Подобная классификация показывает сложность определения возможных угроз и способов их реализации. Это еще раз подтверждает тезис, что определить все множество угроз АСОИБ и способов их реализации не представляется возможным. Не существует универсального способа защиты, который предотвратил бы любую угрозу. Этот факт обуславливает необходимость объединения различных мер защиты для обеспечения безопасности всей АСОИБ в целом.

Выше была рассмотрена классификация возможных угроз безопасности АСОИБ. Конечно, не все приведенные классы угроз являются независимыми от остальных, не для любой угрозы можно определить, к какому виду в каждом из перечисленных классов она принадлежит. Приведенная выше классификация охватывает большинство основных угроз безопасности АСОИБ, которые должны найти свое место в одном или нескольких выделенных классах.

Далее приведено более подробное описание угроз, с которыми наиболее часто приходится сталкиваться администраторам безопасности.

**Несанкционированный доступ** (НСД).

Это наиболее распространенный вид компьютерных нарушений. Он заключается в получении пользователем доступа к объекту, на который у него нет разрешения в соответствии с принятой в организации политикой безопасности. Обычно самая главная проблема определить, кто и к каким наборам данных должен иметь доступ, а кто нет. Другими словами, необходимо определить термин «несанкционированный».

По характеру воздействия НСД является активным воздействием, использующим ошибки системы. НСД обращается обычно непосредственно к требуемому набору данных, либо воздействует на информацию о санкционированном доступе с целью легализации НСД. НСД может быть подвержен любой объект системы. НСД может быть осуществлен как стандартными, так и специально разработанными программными средствами к объектам в любом состоянии.

Методика реализации НСД в значительной мере зависит от организации обработки информации в АСОИБ, разработанной для АСОИБ политики безопасности, возможностей установленных средств защиты, а также добросовестности администратора и оператора. Для реализации НСД существует два способа:

- во-первых, можно преодолеть систему защиты, то есть путем различных воздействий на нее прекратить ее действия в отношении себя или своих программ. Это сложно, трудоемко и не всегда возможно, зато эффективно;

- во-вторых, можно понаблюдать за тем, что «плохо лежит», то есть какие наборы данных, представляющие интерес для злоумышленника, открыты для доступа по недосмотру или умыслу администратора. Такой доступ, хотя и с некоторой натяжкой, тоже можно назвать несанкционированным, его легко осуществить, но от него легко и защититься. К этому же типу относится НСД с подбором пароля, поскольку осуществить такой подбор возможно лишь в случае нарушения правил составления паролей и использования в качестве пароля человеческих имен, повторяющихся символов, наборов типа QWERTY.

В подавляющем большинстве случаев НСД становится возможным из-за непродуманного выбора средств защиты, их некорректной установки и настройки, плохого контроля работы, а также при небрежном отношении к защите своих собственных данных.

**Незаконное использование привилегий.**

Злоумышленники, применяющие данный способ атаки, обычно используют штатное программное обеспечение (системное или прикладное), функционирующее в нештатном режиме. Практически любая защищенная система содержит средства, используемые в чрезвычайных ситуациях, при сбоях оборудования или средства, которые способны функционировать с нарушением существующей политики безопасности. В некоторых случаях пользователь должен иметь возможность доступа ко всем наборам системы (например, при внезапной проверке).

Такие средства необходимы, но они могут быть чрезвычайно опасными. Обычно эти средства используются администраторами, операторами, системными программистами и другими пользователями, выполняющими специальные функции.

Для того, чтобы уменьшить риск от применения таких средств большинство систем защиты реализует такие функции с помощью набора привилегий — для выполнения определенной функции требуется определенная привилегия. В этом случае каждый пользователь получает свой набор привилегий, обычные пользователи — минимальный, администраторы — максимальный (в соответствии с принципом минимума привилегий). Наборы привилегий каждого пользователя являются его атрибутами и охраняются системой защиты. Несанкционированный захват привилегий приведет, таким образом, к возможности несанкционированного выполнения определенной функции. Это может быть НСД (частный случай), запуск определенных программ и даже реконфигурация системы.

Естественно, при таких условиях расширенный набор привилегий -заветная мечта любого злоумышленника. Он позволит ему совершать практически любые действия, причем, возможно, даже в обход всех мер контроля. Нарушения, совершаемые с помощью незаконного использования привилегий, являются активным воздействием, совершаемым с целью доступа к какому-либо объекту или системе в целом.

Незаконный захват привилегий возможен либо при наличии ошибок в самой системе защиты (что, например, оказалось возможным в одной из версий операционной системы UNIX), либо в случае халатности при управлении системой и привилегиями в частности (например, при назначении расширенного набора привилегий всем подряд). Строгое соблюдение правил управления системой защиты, соблюдение принципа минимума привилегий позволят избежать таких нарушений.

**Атаки «салями».**

Атаки «салями» более всего характерны для систем, обрабатывающих денежные счета и, следовательно, для банков особенно актуальны. Принцип атак «салями» построен на том факте, что при обработке счетов используются целые единицы (центы, рубли, копейки), а при исчислении процентов нередко получаются дробные суммы.

Например, 6.5% годовых от $102.87 за 31 день составит $0.5495726. Банковская система может округлить эту сумму до $0.55. Однако если пользователь имеет доступ к банковским счетам или программам их обработки, он может округлить ее в другую сторону — до $0.54, а разницу в 1 цент записать на свой счет. Владелец счета вряд ли ее заметит, а если и обратит внимание, то спишет ее на погрешности обработки и не придаст значения. Злоумышленник же получит прибыль в один цент, при обработке 10.000 счетов в день (а в некоторых банках и больше). Его прибыль таким образом составит $1000, т.е. около $300 000 в год.

Отсюда и происходит название таких атак — как колбаса салями изготавливается из небольших частей разных сортов мяса, так и счет злоумышленника пополняется за счет различных вкладчиков. Естественно, такие атаки имеют смысл лишь в тех организациях, где осуществляется не менее 5.000 - 10.000 транзакций в день, иначе не имеет смысла рисковать, поскольку в случае обнаружения преступника просто определить. Таким образом, атаки «салями» опасны в основном для крупных банков.

Причинами атак «салями» являются, во-первых, погрешности вычислений, позволяющие трактовать правила округления в ту или иную сторону, а во-вторых, огромные объемы вычислений, необходимые для обработки счетов. Успех таких атак зависит не столько от величины обрабатываемых сумм, сколько от количества счетов (для любого счета погрешность обработки одинакова). Атаки «салями» достаточно трудно распознаются, если только злоумышленник не начинает накапливать на одном счете миллионы. Предотвратить такие атаки можно только обеспечением целостности и корректности прикладных программ, обрабатывающих счета, разграничением доступа пользователей АСОИБ к счетам, а также постоянным контролем счетов на предмет утечки сумм.

**«Скрытые каналы»**

«Скрытые каналы» - пути передачи информации между процессами системы, нарушающие системную политику безопасности. В среде с разделением доступа к информации пользователь может не получить разрешение на обработку интересующих его данных, однако может придумать для этого обходные пути. Практически любое действие в системе каким-то образом затрагивает другие ее элементы, которые при этом могут изменять свое состояние. При достаточной наблюдательности и знании этих связей можно получить прямой или опосредованный доступ к данным.

«Скрытые каналы» могут быть реализованы различными путями, в частности при помощи программных закладок («троянских коней»).

Например, программист банка не всегда имеет доступ к именам и балансам депозитных счетов. Программист системы, предназначенной для обработки ценных бумаг, может не иметь доступ к предложениям о покупке или продаже. Однако при создании таких систем он может предусмотреть способ получения интересующих его сведений. В этом случае программа скрытым способом устанавливает канал связи с этим программистом и сообщает ему требуемые сведения.

Атаки с использованием скрытых каналов обычно приводят к нарушениям конфиденциальности информации в АСОИБ, по характеру воздействия являются пассивными: нарушение состоит только в передаче информации. Для организации «скрытых каналов» может использоваться как штатное программное обеспечение, так и специально разработанные «троянские» или вирусные программы. Атака обычно производится программным способом.

Примером передачи информации по «скрытым каналам» может служить, например, итоговый отчет, в котором вместо слова «TOTAL» используется слово «TOTALS» - программист сделал так, что при определенных условиях, которые может распознать его программа, должна происходить замена слов. Подобными «скрытыми каналами» могут стать число пробелов между двумя словами, значение третьей или четвертой цифры после запятой в какой-нибудь дроби (на которые никто не обращает внимания) и т.д. «Скрытым каналом» может явиться и передача информации о наличии или отсутствии какого-либо набора данных, его размере, дате создания или модификации и т.д.

Также существует большое количество способов организации связи между двумя процессами системы. Более того, многие операционные системы имеют в своем распоряжении такие средства, так как они очень облегчают работу программистов и пользователей. Проблема заключается в том, что очень трудно отделить неразрешенные «скрытые каналы» от разрешенных, то есть тех, которые не запрещаются системной политикой безопасности. В конечном счете все определяется ущербом, который может принести организация «скрытых каналов».

Отличительными особенностями «скрытых каналов» является их малая пропускная способность (по ним обычно можно передавать только небольшое количество информации), большие трудности их организации и обычно небольшой наносимый ими ущерб. Более того, он вообще бывает незаметен, поэтому специальные меры защиты против «скрытых каналов» предпринимают довольно редко. Обычно достаточно грамотно разработанной полномочной политики безопасности.

**«Маскарад».**

Под «маскарадом» понимается выполнение каких-либо действий одним пользователем АСОИБ от имени другого пользователя. При этом такие действия другому пользователю могут быть разрешены. Нарушение заключается в присвоении прав и привилегий.

Такие нарушения также называются симуляцией или моделированием. Цель «маскарада» — сокрытие каких-либо действий за именем другого пользователя или присвоение прав и привилегий другого пользователя для доступа к его наборам данных или для использования его привилегий.

«Маскарад» — это способ активного нарушения защиты системы, он является опосредованным воздействием, то есть воздействием, совершенным с использованием возможностей других пользователей.

Примером «маскарада» может служить вход в систему под именем и паролем другого пользователя, при этом система защиты не сможет распознать нарушение. В этом случае «маскараду» обычно предшествует взлом системы или перехват пароля.

Другой пример «маскарада» — присвоение имени другого пользователя в процессе работы. Это может быть сделано с помощью средств операционной системы (некоторые операционные системы позволяют изменять идентификатор пользователя в процессе работы) или с помощью программы, которая в определенном месте может изменить определенные данные, в результате чего пользователь получит другое имя. В этом случае «маскараду» может предшествовать захват привилегий, или он может быть осуществлен с использованием какой-либо ошибки в системе.

«Маскарадом» также называют передачу сообщений в сети от имени другого пользователя. Способы замены идентификатора могут быть разные, обычно они определяются ошибками и особенностями сетевых протоколов. Тем не менее на приемном узле такое сообщение будет воспринято как корректное, что может привести к серьезным нарушениям работы сети. Особенно это касается управляющих сообщений, изменяющих конфигурацию сети, или сообщений, ведущих к выполнению привилегированных операций. [8]

Наиболее опасен «маскарад» в банковских системах электронных платежей, где неправильная идентификация клиента может привести к огромным убыткам. Особенно это касается платежей с помощью электронных банковских карт. Сам по себе метод идентификации с помощью персонального идентификатора (PIN) достаточно надежен, нарушения могут происходить вследствие ошибок его использования. Это произойдет, например, в случае утери кредитной карты, при использовании очевидного идентификатора (своего имени, ключевого слова и т.д.). Поэтому клиентам надо строго соблюдать все рекомендации банка по выполнению такого рода платежей.

«Маскарад» является достаточно серьезным нарушением, которое может привести к тяжелым последствиям, таким как изменение конфигурации системы (сети), утечка информации, нарушения работы АСОИБ. Для предотвращения «маскарада» необходимо использовать надежные методы идентификации и аутентификации, блокировку попыток взлома системы, контроль входов в нее. Также необходимо фиксировать все события, которые могут свидетельствовать о «маскараде», в системном журнале для его последующего анализа.

**«Сборка мусора».**

После окончания работы обрабатываемая информация не всегда полностью удаляется из памяти. Часть данных может оставаться в оперативной памяти, на дисках и лентах, других носителях. Данные хранятся на носителе до перезаписи или уничтожения; при выполнении этих действий на освободившемся пространстве диска находятся их остатки. Хотя прочитать такие данные трудно, однако, используя специальные программы и оборудование, все же возможно. Такой процесс принято называть «сборкой мусора». Он может привести к утечке важной информации.

«Сборка мусора» — активное, непосредственное воздействие на объекты АСОИБ при их хранении с использованием доступа. Это воздействие может привести к нарушению конфиденциальности информации.

Для защиты от «сборки мусора» используются специальные механизмы, которые могут быть реализованы в операционной системе и/или аппаратуре компьютера или в дополнительных программных (аппаратных) средствах. Примерами таких механизмов являются стирающий образец и метка полноты:

- стирающий образец — это некоторая последовательность битов, записываемая на место, освобождаемое файлом. Менеджер или администратор безопасности АСОИБ может автоматически активизировать запись этой последовательности при каждом освобождении участка памяти, при этом стираемые данные уничтожаются физически.

- метка полноты предотвращает чтение участков памяти, отведенных процессу для записи, но не использованных им. Верхняя граница адресов использованной памяти и есть метка полноты. Этот способ используется для защиты последовательных файлов исключительного доступа (результирующие файлы редакторов, компиляторов, компоновщиков т.д.). Для индексных и разделяемых последовательных файлов этот метод называется «стирание при размещении», память очищается при выделении ее процессу.

**«Взлом системы».**

Под «взломом системы» понимают умышленное проникновение в систему с несанкционированными параметрами входа, то есть именем пользователя и его паролем (паролями).

«Взлом системы» — умышленное, активное воздействие на систему в целом. «Взлом системы» обычно происходит в интерактивном режиме.

Поскольку имя пользователя не является секретом, объектом «охоты» обычно становится пароль. Способы вскрытия пароля могут быть различны: перебор возможных паролей, «маскарад» с использованием пароля другого пользователя, захват привилегий. Кроме того, «взлом системы» можно осуществить, используя ошибки программы входа.

Таким образом, основную нагрузку на защиту системы от «взлома» несет программа входа. Алгоритм ввода имени и пароля, их шифрование (при необходимости), правила хранения и смены паролей не должны содержать ошибок. Противостоять «взлому системы» также поможет например, ограничение количества попыток неправильного ввода пароля с последующей блокировкой терминала и уведомлением оператора в случае нарушения.

Кроме того, оператор должен постоянно контролировать активных пользователей системы: их имена, характер работы, время входа и выхода и т.д. Такие действия помогут своевременно установить факт «взлома» и позволят предпринять необходимые действия.

**«Люки».**

«Люк» — это скрытая, недокументированная точка входа в программный модуль. «Люк» вставляется в программу обычно на этапе отладки для облегчения работы: программный модуль можно вызывать в разных местах, что позволяет отлаживать отдельные его части независимо. Но в дальнейшем программист может забыть уничтожить «люк» или некорректно его заблокировать. Кроме того, «люк» может вставляться на этапе разработки для последующей связи данного модуля с другими модулями системы, но затем, в результате изменившихся условий данная точка входа оказывается ненужной.

Наличие «люка» позволяет вызывать программу нестандартным образом, что может серьезно сказаться на состоянии системы защиты (неизвестно, как в таком случае программа будет воспринимать данные, среду системы и т.д.). Кроме того, в таких ситуациях не всегда можно прогнозировать ее поведение.

«Люк» относится к категории угроз, возникающих вследствие ошибок реализации какого-либо проекта (АСОИБ в целом, комплекса программ и т.д.). Поскольку использование «люков» может быть самым разным и зависит от самой программы, классифицировать данную угрозу как-либо еще затруднительно.

«Люки» могут оказаться в программах по следующим причинам:

- их забыли убрать;

- для использования при дальнейшей отладке;

- для обеспечения поддержки готовой программы;

- для реализации тайного контроля доступа к данной программе после ее установки.

Первый из перечисленных случаев — ненамеренный промах, который может привести к бреши в системе защиты. Два следующих случая — серьезные испытания для системы безопасности, с которыми она может и не справиться. Четвертый случай может стать первым шагом преднамеренного проникновения с использованием данной программы.

Отметим, что программная ошибка «люком» не является. «Люк» — это достаточно широко используемый механизм отладки, корректировки и поддержки программ, который создается преднамеренно, хотя чаще всего и без злого умысла. Люк становится опасным, если он не замечен, оставлен и не предпринималось никаких мер по контролю за ним.

Большая опасность «люков», особенно в программах операционной системы, компенсируется высокой сложностью их обнаружения. Если не знать заранее, что данная программа содержит «люк», необходимо обработать килобайты (а иногда и мегабайты) программного кода, чтобы найти его. Понятно, что почти всегда это нереально. Поэтому в большинстве случаев обнаружение «люков» — результат случайного поиска. Защита от них может быть только одна — не допускать появления «люков» в программе, а при приемке программных продуктов, разработанных третьими производителями — проводить анализ исходных текстов программ с целью обнаружения «люков».

**Вредоносные программы.**

В последнее время участились случаи воздействия на вычислительную систему при помощи специально созданных программ. Под вредоносными программами в дальнейшем будем понимать такие программы, которые прямо или косвенно дезорганизуют процесс обработки информации или способствуют утечке или искажению информации.

Ниже рассмотрим некоторые (самые распространенные) виды подобных программ: «троянский конь», вирус, «червь», «жадная» про грамма, «захватчик паролей»:

**«Троянский кoнь»** — программа, выполняющая в дополнение к основным (проектным и документированным) не описанные в документации действия. Аналогия с древнегреческим «троянским конем» таким образом вполне оправдана — в не вызывающей подозрений оболочке таится угроза. Программы такого типа являются серьезной угрозой безопасности АСОИБ.

По характеру угрозы «троянский конь» относится к активным угрозам, реализуемым программными средствами, работающими в пакетном режиме. Он может угрожать любому объекту АСОИБ. Наиболее опасным является опосредованное воздействие, при котором «троянский конь» действует в рамках полномочий одного пользователя, но в интересах другого пользователя, установить личность которого порой невозможно.

Опасность «троянского коня» заключается в дополнительном блоке команд, тем или иным образом вставленном в исходную безвредную программу, которая затем предлагается (дарится, продается, подменяется) пользователям АСОИБ. Этот блок команд может срабатывать при наступлении некоторого условия (даты, времени и т.д., либо по команде извне). Запустивший такую программу подвергает опасности как себя и свой файлы, так и всю АСОИБ в целом.

Наиболее опасные действия «троянский конь» может выполнять, если запустивший ее пользователь обладает расширенным набором привилегий. В этом случае злоумышленник, составивший и внедривший «троянского коня», и сам этими привилегиями не обладающий, может выполнить несанкционированные привилегированные функции чужими руками. Или, например, злоумышленника очень интересуют наборы данных пользователя, запустившего такую программу. Последний может даже не обладать расширенным набором привилегий — это не помешает выполнению несанкционированных действий.

Характерным примером «Троянского коня» является появившийся в Интернете в январе 1999 г. бесплатно распространяемый Screen Saver, который помимо вывода красивых картинок на экране, осуществляет поиск на компьютере программы-шифровальщика алгоритма DEC. В случае обнаружения программы, Screen Saver ставит под контроль обмен ключами шифрования и пересылает ключи по электронной почте на анонимный сервер в Китае. [17]

«Троянский конь» — одна из наиболее опасных угроз безопасности АСОИБ. Радикальным способом защиты от этой угрозы является создание замкнутой среды исполнения программ. В особенности важно разделение внешних сетей (особенно Интернет) и внутренних сетей по крайней мере на уровне протоколов, а еще лучше — на физическом уровне. Желательно также, чтобы привилегированные и непривилегированные пользователи работали с разными экземплярами прикладных программ, которые должны храниться и защищаться индивидуально. При соблюдении этих мер вероятность внедрения программ подобного рода будет достаточно низкой.

**Вирус** — это программа, которая может заражать другие программы путем включения в них своей, возможно модифицированной, копии, причем последняя сохраняет способность к дальнейшему размножению. Вирус может быть охарактеризован двумя основными особенностями :

- способностью к самовоспроизведению. Это свойство означает, что за время своего существования на компьютере вирус должен хотя бы один раз воспроизвести свою копию на долговременном носителе;

- способностью к вмешательству (получению управления) в вычислительный процесс. Это свойство является аналогом «паразитирования» в живой природе, которое свойственно биологическим вирусам.

Как и «троянские кони» вирусы относятся к активным программным средствам. Классификация вирусов, используемые ими методы заражения, способы борьбы с ними достаточно хорошо изучены и описаны. Эта проблема в нашей стране стала особенно актуальной, поэтому очень многие занимаются ею.

Проблема защиты от вирусов может рассматриваться с двух сторон: как самостоятельная проблема и как одна из сторон проблемы общей защиты АСОИБ. И тот, и другой подходы имеют свои отличительные особенности и, соответственно, свои собственные методы решения проблемы.

В последнее время удалось более или менее ограничить масштабы заражений и разрушений. Тут сыграли свою роль и превентивные меры, и новые антивирусные средства, и пропаганда всех этих мер.

Вообще говоря проблема вирусов может стать тем толчком, который приведет к новому осмыслению как концепций защиты, так и принципов автоматизированной обработки информации в целом.

«**Червь**» — программа, распространяющаяся через сеть и (в отличие от вируса) не оставляющая своей копии на магнитном носителе. «Червь» использует механизмы поддержки сети для определения узла, который может быть заражен. Затем с помощью тех же механизмов передает свое тело или его часть на этот узел и либо активизируется, либо ждет для этого подходящих условий.

Наиболее известный представитель этого класса - вирус Морриса (или, вернее, «червь Морриса»), поразивший сеть Internet в 1988 г. Наиболее подходящей средой распространения «червя» является сеть, все пользователи которой считаются дружественными и доверяют друг другу. Отсутствие защитных механизмов как нельзя лучше способствует уязвимости сети.

Самый лучший способ защиты от «червя» — принять меры предосторожности против несанкционированного доступа к сети.

Таким образом, как вирусы, так «троянские кони» и «черви» на сегодняшний день являются одной из самых опасных угроз АСОИБ. Для защиты от этих разновидностей вредоносных программ необходимо создание замкнутой среды исполнения программ, разграничение доступа к исполняемым файлам, контроль целостности исполняемых файлов и системных областей, тестирование приобретаемых программных средств.

«Жадные» программы — это программы, которые при выполнении стремятся монополизировать какой-либо ресурс системы, не давая другим программам возможности использовать его. Доступ таких программ к ресурсам системы обычно приводит к нарушению ее доступности. Естественно, такая атака будет активным вмешательством в работу системы. Непосредственной атаке обычно подвергаются ключевые объекты системы: процессор, оперативная память, устройства ввода-вывода.

Многие компьютеры, особенно в исследовательских центрах, имеют фоновые программы, выполняющиеся с низким приоритетом. Они обычно производят большой объем вычислений, а результаты их работы требуются не так часто. Однако при повышении приоритета такая программа может блокировать все остальные. Такая программа и будет «жадной».

Тупиковая ситуация возникает, когда «жадная» программа бесконечна (например, исполняет заведомо бесконечный цикл). Однако во многих операционных системах существует возможность ограничения времени процессора, используемого задачей. Это не относится к операциям, выполняющимся в зависимости от других программ, например, к операциям ввода-вывода, которые завершаются асинхронно к основной программе; время их выполнения не включается в счет времени программы. Перехватывая асинхронное сообщение о завершении операции ввода-вывода и посылая вновь запрос на новый ввод-вывод, можно добиться по-настоящему бесконечной программы. Такие атаки называют также асинхронными.

Другой пример «жадной» программы — программа, захватывающая слишком большую область оперативной памяти. В оперативной памяти последовательно размещаются данные, например подкачиваемые с внешнего носителя. В конце концов память может оказаться во владении одной программы, и выполнение других окажется невозможным.

Обычно «жадные» программы осуществляют захват одного из трех основных ресурсов системы: времени процессора, оперативной памяти, каналов ввода-вывода. Однако возможен захват и любых других ресурсов системы: блокирование ее работы, или же использование побочного результата деятельности какой-либо программы (например, вируса). Бороться с захватом ресурсов можно путем введения различных ограничений для выполняемых программ (на время процессора, на количество операций ввода-вывода, на разрешенный объем оперативной памяти и т.д.), а также постоянным операторским контролем за их соблюдением.

**Захватчики паролей**. Это программы специально предназначены для воровства паролей. При попытке входа имитируется ввод имени и пароля, которые пересылаются владельцу программы-захватчика, после чего выводится сообщение об ошибке ввода и управление возвращается операционной системе. Пользователь, думающий, что допустил ошибку при наборе пароля, повторяет вход и получает доступ к системе. Однако его имя и пароль уже известны владельцу программы-захватчика. Перехват пароля может осуществляться и другим способом - с помощью воздействия на программу, управляющую входом пользователей в систему и ее наборы данных.

Для предотвращения этой угрозы перед входом в систему необходимо убедиться, что вы вводите имя и пароль именно системной программе входа, а не какой-то другой. Кроме того, необходимо неукоснительно придерживаться правил использования паролей и работы с системой. Большинство нарушений происходят не из-за хитроумных атак, а из-за элементарной небрежности. Не рекомендуется покидать рабочее место, не выйдя из системы. Постоянно проверяйте сообщения о дате и времени последнего входа и количестве ошибочных входов. Эти простые действия помогут избежать захвата пароля.

Кроме описанных выше, существуют и другие возможности компрометации пароля. Не следует записывать команды, содержащие пароль, в командные процедуры, надо избегать явного объявления пароля при запросе доступа по сети: эти ситуации можно отследить и захватить пароль. Не стоит использовать один и тот же пароль для доступа к разным узлам.

Соблюдение правил использования паролей — необходимое условие надежной защиты.

## Анализ состояния банковских автоматизированных систем с точки зрения безопасности.

Под безопасностью АСОИБ будем понимать ее свойство, выражающееся в способности противодействовать попыткам нанесения ущерба владельцам и пользователям системы при различных возмущающих (умышленных и неумышленных) воздействиях на нее. Иными словами под безопасностью системы понимается ее защищенность от случайного или преднамеренного вмешательства в нормальный процесс ее функционирования, а также от попыток хищения, модификации или разрушения ее компонентов. Следует отметить, что природа воздействия может быть самой различной. Это и попытки проникновения злоумышленника, и ошибки персонала, и стихийные бедствия (ураган, пожар), и выход из строя составных частей АСОИБ.

Безопасность АСОИБ достигается обеспечением конфиденциальности обрабатываемой ею информации, а также целостности и доступности компонентов и ресурсов системы.

Конфиденциальность информации — это свойство информации быть известной только допущенным и прошедшим проверку (авторизованным) субъектам системы (пользователям, программам, процессам и т.д.). Для остальных субъектов системы эта информация как бы не существует.

Целостность компонента (ресурса) системы — свойство компонента (ресурса) быть неизменным (в семантическом смысле) при функционировании системы.

Доступность компонента (ресурса) системы — свойство компонента (ресурса) быть доступным для использования авторизованными субъектами системы в любое время. [6, с.57]

Обеспечение безопасности АСОИБ требует применения различных мер защитного характера. Обычно вопрос о необходимости защиты компьютерной системы не вызывает сомнений. Наиболее трудными бывают ответы на вопросы:

1. От чего надо защищать систему?

2. Что надо защищать в самой системе?

3. Как надо защищать систему (при помощи каких методов и средств)?

При выработке подходов к решению проблемы безопасности следует всегда исходить из того, что конечной целью применения любых мер противодействия угрозам является защита владельца и законных пользователей АСОИБ от нанесения им материального или морального ущерба в результате случайных или преднамеренных воздействий на нее.

Обеспечение безопасности АСОИБ в целом предполагает создание препятствий для любого несанкционированного вмешательства в процесс ее функционирования, а также попыток хищения, модификации, выведения из строя или разрушения ее компонентов. То есть защиту всех компонентов системы: оборудования, программного обеспечения, данных и персонала. В этом смысле, защита информации от несанкционированного доступа является только частью общей проблемы обеспечения безопасности АСОИБ, а борьбу следует вести не только с «несанкционированным доступом» (к информации), а шире, — с «несанкционированными действиями».

Обычно различают внешнюю и внутреннюю безопасность АСОИБ [3, с.182]. Внешняя безопасность включает защиту АСОИБ от стихийных бедствий (пожар, наводнение и т.п.) и от проникновения злоумышленников извне с целями хищения, получения доступа к носителям информации или вывода системы из строя. Предметом внутренней безопасности является обеспечение надежной и корректной работы системы, целостности ее программ и данных.

Все усилия по обеспечению внутренней безопасности АСОИБ фокусируются на создании надежных и удобных механизмов регламентации деятельности всех ее пользователей и обслуживающего персонала, соблюдении установленной в организации дисциплины прямого или косвенного доступа к ресурсам системы и к информации.

Учитывая то обстоятельство, что основным предназначением АСОИБ является переработка (сбор, хранение, обработка и выдача) информации, то проблема обеспечения безопасности информации является для АСОИБ центральной в ряду проблем защиты средств вычислительной техники от стихийных бедствий и хищений, проблем подбора и подготовки кадров, организации управления, обеспечения живучести АСОИБ, надежности их технических средств и программного обеспечения и других. Очевидно, что все они тесно связаны с безопасностью информации, поскольку, например, отказ в обслуживании клиента или несвоевременное предоставление пользователю хранящейся в АСОИБ важной информации из-за неработоспособности этой системы по своим последствиям равноценны потере информации (несанкционированному ее уничтожению).

Анализ построения система информационной безопасности следует начинать с анализа рисков возможных угроз.

Риск есть стоимостное выражение вероятностного события, ведущего к потерям. Для оценки степени риска при том или ином варианте действий применяются различные методики. В зарубежной литературе они получили название «анализ риска» (risk analysis). Анализ риска применяется к самым различным операциям. Например, при выдаче кредита специалисты банка оценивают риск его невозврата заемщиком. Оценив величину степени риска можно принять меры, направленные на ее уменьшение (например, опечатав на складе заемщика высоколиквидный товар). [13, с.28]

Перед тем, как выбирать различные средства защиты необходимо четко представлять какие компоненты АСОИБ, от каких посягательств и насколько надежно вы хотите защитить. Безусловно, основой системы защиты АСОИБ должны быть организационные (административные) мероприятия, стержнем которых является разработка и реализация плана защиты. Но организационные меры без повсеместной поддержки их физическими и техническими (программными и аппаратными) средствами будут слабы. Поэтому при выборе средств защиты необходимо обращать внимание не только на их надежность, но и на то, как они будут поддерживать разработанные организационные мероприятия.

Необходимо использовать анализ риска для выбора наиболее реальных угроз АСОИБ и целесообразных способов защиты от них.

Для чего нужен анализ риска в этой области?

1. Для повышения осведомленности персонала. Обсуждение вопросов защиты АСОИБ может поднять уровень интереса к этой проблеме среди сотрудников, что приведет к более точному выполнению требований инструкций.

2. Для определения сильных и слабых сторон существующих и предлагаемых мер защиты. Многие организации не имеют полной информации о своей АСОИБ и ее слабых сторонах. Систематический анализ дает всестороннюю информацию о состоянии аппаратного и программного обеспечения АСОИБ и степени риска потери (искажения, утечки) информации при ее обработке и хранении в электронном виде.

3. Для подготовки и принятия решения по выбору мер и средств защиты. Защита снижает производительность АСОИБ, внося при этом неудобства (иногда существенные) в работу пользователей. Некоторые меры защиты слишком сложны и дороги и их применение не может быть оправдано теми функциями, которые они выполняют. В то же время существуют настолько серьезные виды угроз, что поиск и разработка новых, более эффективных методов и средств защиты от них является просто необходимыми. В обоих случаях степень риска определяет уровень и масштаб применяемых средств защиты.

4. Для определения затрат на защиту. Некоторые механизмы защиты требуют довольно больших ресурсов, и их работа скрыта от пользователей. Анализ риска может помочь определить самые главные требования к системе защиты АСОИБ.

Анализ риска - это процесс получения количественной или качественной оценки ущерба, который может произойти в случае реализации угрозы безопасности АСОИБ.

Ниже рассматриваются основные этапы, проводимые при анализе риска безопасности АСОИБ. Они могут в отдельных случаях корректироваться в зависимости от конкретных условий анализа [13, с.29]:

1. Описание компонентов АСОИБ.

2. Определение уязвимых мест АСОИБ.

3. Оценка вероятностей проявления угроз безопасности АСОИБ.

4. Оценка ожидаемых размеров потерь.

5. Обзор возможных методов защиты и оценка их стоимости.

6. Оценка выгоды от применения предполагаемых мер.

Рассмотрим эти этапы подробнее. Описание компонентов АСОИБ

Все компоненты АСОИБ можно разбить на следующие категории:

- оборудование — ЭВМ и их составные части (процессоры, мониторы, терминалы, рабочие станции), периферийные устройства (дисководы, устройства back-up, порты ввода-вывода, принтеры, кабели, контроллеры, линии связи) и т.д.;

- программное обеспечение — исходные, объектные, загрузочные модули, приобретенные программы, «домашние» разработки, утилиты, операционные системы и системные программы (компиляторы, компоновщики и др.), диагностические программы и т.д.;

- данные — временные, хранимые постоянно, на магнитных носителях, печатные, архивы, системные журналы и т.д.;

- сотрудники — пользователи и обслуживающий персонал.

Кроме компонентов АСОИБ при планировании системы безопасности необходимо четко описать технологию обработки информации в защищаемой АСОИБ. Необходимо зафиксировать состояние АСОИБ как совокупности различных компонентов и технологии обработки информации. Все дальнейшие этапы анализа риска производятся именно с этой, зафиксированной на некоторый момент времени, системой.

Важным моментом является определение уязвимых мест АСОИБ. Для всех категорий, компонентов АСОИБ необходимо определить, какие опасности могут угрожать каждой из них и что может быть их причиной.

Рассмотрим примеры опасных воздействий, которые могут привести к нарушению конфиденциальности, целостности и доступности определенных компонентов и ресурсов АСОИБ:

1. Стихийные бедствия.

2. Внешние воздействия. Подключение к сети, интерактивная работа, воздействие хакеров.

3. Преднамеренные нарушения. Действия обиженных служащих, взяточников, любопытных посетителей, конкурентов и т.д.

4. Неумышленные ошибки. Ввод ошибочной команды, данных, использование неисправных устройств, носителей, а также пренебрежение некоторыми правилами безопасности.

Дальнейший этап анализа риска определяет, как часто может проявиться каждая из угроз безопасности АСОИБ. В некоторых случаях вообще невозможно численно оценить появление той или иной угрозы, однако для большинства случаев такая оценка все же возможна.

Приведем некоторые методы оценки вероятностей проявления угроз.

1. Эмпирическая оценка количества проявлений угрозы за некоторый период времени. Как правило, этот метод применяется для оценки вероятности стихийных бедствий. Невозможно предсказать возникновение, например, пожара в определенном здании, поэтому в таких случаях целесообразно накапливать массив данных об исследуемом событии. Так например, в среднем за год пожар уничтожит некоторое количество зданий; средний ущерб составит $Х. Кроме того, также можно получать данные об обманах со стороны сотрудников, коррупции и т.д. Такой анализ обычно неточен, поскольку использует лишь частичные данные о событии, но тем не менее в некоторых случаях таким путем можно получить приемлемые результаты.

2. Непосредственная регистрация событий. Обычно этот метод применяется для оценки вероятности часто проявляющихся событий (попытки входа в систему, доступ к определенному объекту и т.д.).

3. Оценка частоты проявления угрозы по таблице. Некоторые методы анализа риска позволяют оценить вероятность появления каких либо событий по специальной таблице, выбирая один из коэффициентов. Полнота анализа зависит от качества метода вычисления коэффициентов проявления данного события. Таким образом, оценка вероятности события производится не с помощью безосновательного выбора числа, а на основе системы коэффициентов, которая имеют некоторую методологическую основу.

4. Метод «Дельфийский оракул». С помощью этого метода каждый конкретный коэффициент выводится из частоты появления определенного события. Эти частоты накапливаются и преобразуются в коэффициенты; они могут быть изменены на основе новых данных. После серии испытаний все значения коэффициентов собирают, и если они приемлемы, то одно из них (лучшее в смысле некоторого выбранного критерия) оставляют. В противном случае анализируется методика получения оценок и производится новая серия испытаний.

Определение потерь в результате реализации любой из угроз безопасности — следующий этап анализа риска. Как и оценка частоты реализации различных угроз, определение потерь также трудно поддается расчету. Например, стоимость замены аппаратного или программного обеспечения АСОИБ оценивается достаточно просто. Однако существует много случаев (восстановление данных или программ), когда это сопряжено с большими трудностями.

Многие данные нуждаются в защите по вполне объяснимым причинам. Защищать необходимо личные данные (счета, страховые полисы), коммерческую информацию (технологические, финансовые и другие секреты). Однако при этом трудно оценить величину потерь при искажении, потере этих данных, либо при невозможности получить данные в требуемое время.

Ответы на приведенные ниже вопросы полезно использовать при оценке величины ожидаемых потерь, при анализе различных способов реализации угроз; они, конечно, не дадут полную картину, но могут облегчить оценку возможного ущерба:

1. Каковы Ваши обязательства по сохранению конфиденциальности и целостности тех или иных данных?

2. Может ли компрометация этих данных привести к несчастному случаю? Существует ли реальная возможность такого события?

3. Может ли несанкционированный доступ к этим данным послужить причиной потерь в будущем (упущенная возможность в бизнесе)? Может ли этот случай послужить Вашим соперникам (конкурентам)? Каковы возможные потери от этого?

4. Каков может быть психологический эффект потери? Возможные затруднения? Кредитоспособность? Потеря клиентуры?

5. Каково значение доступа к этим данным? Может ли обработка этих данных быть отложена? Могут ли эти вычислений быть выполнены где-нибудь еще? Сколько Вы можете заплатить за обработку этих данных в другом месте?

6. Каково для Вас значение несанкционированного доступа конкурентов к Вашим данным? Насколько заинтересованы ваши соперники (конкуренты) в этих данных?

7. Какие проблемы могут возникнуть при утере Ваших данных? Могут ли они быть восстановлены? Каков объем работ по восстановлению? Сколько это будет стоить ?

Как уже отмечалось выше, оценка потерь достаточно сложна. Более того, уязвимость вычислительных систем часто оказывается выше ожидаемой. Поэтому реалистичные оценки потенциального ущерба могут послужить основой для разработки системы защиты и определить область наиболее пристального внимания.

Защита от проявления той или иной угрозы может быть реализована различными способами. Например, защитить информацию на жестком диске ПЭВМ от ознакомления можно следующими способами :

- организовать контроль за доступом в помещение, в котором установлена ПЭВМ;

- назначить ответственных за использование ПЭВМ;

- шифровать информацию на диске;

- использовать системы разграничения доступа;

- закрывать доступ или демонтировать дисководы и порты ввода-вывода;

- применять средства оповещения администратора о вскрытии корпуса ПЭВМ.

Для каждого из этих способов определяются такие характеристики, как стоимость и эффективность. Стоимость метода защиты имеет абсолютное значение, выраженное в денежных единицах, затраченных на его реализацию и сопровождение. При оценке стоимости метода необходимо учитывать не только прямые (закупка оборудования, обучение персонала и т.д.), но и косвенные затраты (замедление работы системы, нарушение устоявшейся технологии обработки информации и т.д)

Эффективность метода — это его способность противостоять тем или иным угрозам. Получить реальное значение эффективности очень трудно, и в большинстве случаев эта характеристика определяется эмпирически.

Анализ риска также позволяет экспериментировать с некоторой моделью АСОИБ для того, чтобы выяснить, какие из имеющихся методов защиты наиболее эффективны для сохранения работоспособности системы и конфиденциальности обрабатываемой в ней информации.

Анализ риска — хорошо известный инструмент планирования, широко используемый в практике управления. Тем не менее, иногда выдвигаются аргументы против его использования. Рассмотрим основные из них.

1. Неточность. Многие значения, получаемые в процессе анализа (вероятность появления событий, стоимость ущерба) не отличаются высокой точностью. Однако существуют различные методы для получения приемлемых приближений этих значений.

В то же время, анализ риска — это инструмент планирования. Основная его задача — определить уровень возможных потерь. Например, можно ошибиться в частоте появления некоторого события — один раз в год или один раз в три года, но мы по крайней мере будем уверены, что оно вряд ли будет происходить каждую неделю. Анализ риска определяет эффективный уровень затрат на защиту, особенно в условиях ограниченных финансов.

Кроме того, излишняя точность может оказаться ненужной. Например, совершенно неважно, составят ли ожидаемые потери $150.000 или $100.000, важно, что они будут много больше чем $20.000. Стремление к излишней точности в таких случаях только требует увеличения времени анализа и дополнительных затрат.

2. Быстрая изменяемость. Анализ риска актуален лишь в течение определенного промежутка времени. Потом может изменится состав системы, внешние условия и т.д, и придется проводить новый анализ. В идеале анализ риска для собственной АСОИБ рекомендуется проводить ежегодно.

Важный момент в ежегодном исследовании — учет всех имеющих отношение к делу изменений, происшедших за истекший год. При этом некоторые факторы могли не учитываться в прошлом году, а некоторые могли потерять актуальность.

3. Отсутствие научной базы. Почти все методики проведения анализа риска основывается на положениях теории вероятностей и математической статистики, однако их применение не всегда корректно.

В процессе проведения анализа риска должна быть сформирована основа для определения необходимых мер защиты. В частности, следует определить, что именно относится к АСОИБ (оборудование, программы, данные, персонал и т.д.) и что нуждается в защите.

Далее необходимо составить список возможных на ваш взгляд способов реализации угроз работе системы, роль и место средств защиты для предотвращения кризисных ситуаций,

В этом разделе плана фиксируется порядок формирования и обработки данных в защищаемой АСОИБ. Как отмечалось выше, наиболее сложным этапом анализа риска является определение частоты появления возможных угроз системе. Поскольку использование различных методов оценки может влиять на точность результатов, все они должны быть отражены в данном пункте плана.

Наконец, этот пункт должен содержать сведения о действиях средств защиты в случае возникновения непредусмотренных ситуаций, которые могут возникнуть при вводе в действие новой техники, программ, данных или из-за ошибок в планировании. При этом необходимо также предусмотреть, каким образом существующая система защиты может быть адаптирована к возникающим новым ситуациям.

Таким образом, составление плана защиты — сложный и трудоемкий процесс, требующий значительных исследований и затрат. В то же время чрезмерное увлечение сбором и анализом данных об АСОИБ и ее неформальных спецификаций может чересчур оттянуть и усложнить практическую реализацию мер по защите. Т.е. план должен строится на глубоком анализе ситуации, но в то же время оставаться в рамках здравого смысла, не погружаясь в излишнюю формализацию и бюрократизацию.

## Построение защиты банковских автоматизированных систем.

Каждую систему обработки информации защиты следует разрабатывать индивидуально учитывая следующие особенности:

1. организационную структуру банка;
2. объем и характер информационных потоков (внутри банка в целом, внутри отделов, между отделами, внешних);
3. количество и характер выполняемых операций: аналитических и повседневных (один из ключевых показателей активности банка — число банковских операций в день, является основой для определения параметров системы);
4. количество и функциональные обязанности персонала;
5. количество и характер клиентов;
6. график суточной нагрузки.

Защита АСОИБ должна разрабатываться для каждой системы индивидуально, но в соответствии с общими правилами. Построение защиты предполагает следующие этапы:

- анализ риска, заканчивающийся разработкой проекта системы защиты и планов защиты, непрерывной работы и восстановления;

- реализация системы защиты на основе результатов анализа риска;

- постоянный контроль за работой системы защиты и АСОИБ в целом (программный, системный и административный).

На каждом этапе реализуются определенные требования к защите; их точное соблюдение приводит к созданию безопасной системы.

На сегодняшний день защита АСОИБ — это самостоятельное направление исследований. Поэтому легче и дешевле использовать для выполнения работ по защите специалистов, чем дважды учить своих людей (сначала их будут учить преподаватели, а потом они будут учиться на своих ошибках).

Главное при защите АСОИБ специалистами (естественно после уверенности в их компетенции в данном вопросе) — наличие здравого смысла у администрации системы. Обычно, профессионалы склонны преувеличивать реальность угроз безопасности АСОИБ и не обращать внимания на такие «несущественные детали» как удобство ее эксплуатации, гибкость управления системой защиты и т.д., без чего применение системы защиты становится трудным делом. Построение системы защиты — это процесс поиска компромисса между уровнем защищенности АСОИБ и сохранением возможности работы в ней. Здравый смысл помогает преодолеть большинство препятствий на этом пути.

Для обеспечения непрерывной защиты информации в АСОИБ целесообразно создать из специалистов группу информационной безопасности. На эту группу возлагаются обязанности по сопровождению системы защиты, ведения реквизитов защиты, обнаружения и расследования нарушений политики безопасности и т.д.

Один из самых важных прикладных аспектов теории защиты — защита сети. При этом, с одной стороны, сеть должна восприниматься как единая система и, следовательно, ее защита также должна строиться по единому плану. С другой стороны, каждый узел сети должен быть защищен индивидуально.

Защита конкретной сети должна строиться с учетом конкретных особенностей: назначения, топологии, особенностей конфигурации, потоков информации, количества пользователей, режима работы и т.д.

Кроме того, существуют специфические особенности защиты информации на микрокомпьютерах, в базах данных. Нельзя также упускать из виду такие аспекты, как физическая защита компьютеров, периферийных устройств, дисплейных и машинных залов. Иногда бывает необходим и «экзотический» вид защиты — от электромагнитного излучения или защита каналов связи.

Основные этапы построения системы защиты заключаются в следующем:

Анализ -> Разработка системы защиты (планирование) -> Реализация системы защиты -> Сопровождение системы защиты.

Этап анализа возможных угроз АСОИБ необходим для фиксирования на определенный момент времени состояния АСОИБ (конфигурации аппаратных и программных средств, технологии обработки информации) и определения возможных воздействий на каждый компонент системы. Обеспечить защиту АСОИБ от всех воздействий на нее невозможно, хотя бы потому, что невозможно полностью установить перечень угроз и способов их реализации. Поэтому надо выбрать из всего множества возможных воздействий лишь те, которые могут реально произойти и нанести серьезный ущерб владельцам и пользователям системы.

На этапе планирования формируется система защиты как единая совокупность мер противодействия различной природы.

По способам осуществления все меры обеспечения безопасности компьютерных систем подразделяются на: правовые, морально-этические, административные, физические и технические (аппаратные и программные) [9, с.28].

К правовым мерам защиты относятся действующие законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией ограниченного использования и ответственность за их нарушения. Этим они препятствуют несанкционированному использованию информации и являются сдерживающим фактором для потенциальных нарушителей.

К морально-этическим мерам противодействия относятся всевозможные нормы поведения, которые традиционно сложились или складываются по мере распространения ЭВМ в стране или обществе. Эти нормы большей частью не являются обязательными, как законодательно утвержденные, однако, их несоблюдение ведет обычно к падению авторитета, престижа человека, группы лиц или организации. Морально-этические нормы бывают, как неписанные (например, общепризнанные нормы честности, патриотизма и т.п.), так и оформленные в некий свод (устав) правил или предписаний. Наиболее характерным примером последних является «Кодекс профессионального поведения членов Ассоциации пользователей ЭВМ США» [14]. В частности, считаются неэтичными умышленные или неумышленные действия, которые:

- нарушают нормальную работу компьютерных систем;

- вызывают дополнительные неоправданные затраты ресурсов (машинного времени, памяти, каналов связи и т.п.);

- нарушают целостность хранимой и обрабатываемой информации;

- нарушают интересы других законных пользователей и т.д.

Административные меры защиты — это меры организационного характера, регламентирующие процессы функционирования системы обработки информации, использование ее ресурсов, деятельность персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности. Они включают:

- разработку правил обработки информации в АСОИБ;

- мероприятия, осуществляемые при проектировании, строительстве и оборудовании вычислительных центров и других объектов АСОИБ (учет влияния стихии, пожаров, охрана помещений, организация защиты от установки прослушивающей аппаратуры и т.п.);

- мероприятия, осуществляемые при подборе и подготовке персонала (проверка новых сотрудников, ознакомление их с порядком работы с конфиденциальной информацией, с мерами ответственности за нарушение правил ее обработки; создание условий, при которых персоналу было бы невыгодно допускать злоупотребления и т.д.);

- организацию надежного пропускного режима;

- организацию учета, хранения, использования и уничтожения документов и носителей с конфиденциальной информацией;

- распределение реквизитов разграничения доступа (паролей, профилей полномочий и т.п.);

- организацию скрытого контроля за работой пользователей и персонала АСОИБ;

- мероприятия, осуществляемые при проектировании, разработке, ремонте и модификациях оборудования и программного обеспечения (сертификация используемых технических и программных средств, строгое санкционирование, рассмотрение и утверждение всех изменений, проверка их на удовлетворение требованиям защиты, документальное отражение изменений и т.п.).

Физические меры защиты — это разного рода механические, электро- или электронно-механические устройства и сооружения, специально предназначенные для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации.

Техническими (аппаратно-программными) средствами защиты называются различные электронные устройства и специальные программы, которые выполняют (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическую защиту информации и т.д.).

Наилучшие результаты достигаются при системном подходе к вопросам обеспечения безопасности АСОИБ и комплексном использовании различных мер защиты на всех этапах жизненного цикла системы, начиная с самых ранних стадий ее проектирования.

Очевидно, что в структурах с низким уровнем правопорядка, дисциплины и этики ставить вопрос о защите информации просто бессмысленно. Прежде всего надо решить правовые и организационные вопросы.

Административные меры играют значительную роль в обеспечении безопасности АСОИБ. Эти меры необходимо использовать тогда, когда другие методы и средства защиты просто недоступны (отсутствуют или слишком дороги). Однако это вовсе не означает, что систему защиты необходимо строить исключительно на основе административных методов, как это часто пытаются сделать чиновники, далекие от технического прогресса. Этим мерам присущи серьезные недостатки, такие как:

- низкая их надежность без соответствующей поддержки со стороны физических, технических и программных средств (люди склонны к нарушению любых установленных правил, если только их можно нарушить);

- применение для защиты только административного мер обычно приводит к параличу деятельности АСОИБ и всей организации (совершенно невозможно работать не нарушая инструкций) из-за ряда дополнительных неудобств, связанных с большим объемом рутинной формальной деятельности.

Административные меры надо везде, где только возможно, заменять более надежными современными физическими и техническими средствами. Они должны обеспечивать эффективное применение других, более надежных методов и средств защиты в части касающейся регламентации действий людей.

Известно не так много общих (универсальных) способов защиты АСОИБ от различных воздействий на нее. Ими являются:

- идентификация и аутентификация субъектов (пользователей, процессов и т.д.) АСОИБ;

- контроль доступа к ресурсам АСОИБ;

- регистрация и анализ событий, происходящих в АСОИБ;

- контроль целостности объектов АСОИБ;

- шифрование данных;

- резервирование ресурсов и компонентов АСОИБ.

Эти универсальные способы защиты могут применяться в различных вариациях и совокупностях в конкретных методах и средствах защиты.

Результатом этапа планирования является план защиты — документ, содержащий перечень защищаемых компонентов АСОИБ и возможных воздействий на них, цель защиты информации в АСОИБ, правила обработки информации в АСОИБ, обеспечивающие ее защиту от различных воздействий, а также описание разработанной системы защиты информации.

При необходимости, кроме плана защиты на этапе планирования может быть разработан план обеспечения непрерывной работы и восстановления функционирования АСОИБ, предусматривающий деятельность персонала и пользователей системы по восстановлению процесса обработки информации в случае различных стихийных бедствий и других критических ситуаций.

Сущность этапа реализации системы защиты заключается в установке и настройке средств защиты, необходимых для реализации зафиксированных в плане защиты правил обработки информации. Содержание этого этапа зависит от способа реализации механизмов защиты в средствах защиты.

К настоящему времени сформировались два основных способа реализации механизмов защиты.

При первом из них механизмы защиты не реализованы в программном и аппаратном обеспечении АСОИБ, либо реализована только часть их, необходимая для обеспечения работоспособности всей АСОИБ (например, механизмы защиты памяти в мультипользовательских системах). Защита информации при хранении, обработке или передаче обеспечивается дополнительными программными или аппаратными средствами, не входящими в состав самой АСОИБ. При этом средства защиты поддерживаются внутренними механизмами АСОИБ.

Такой способ получил название «добавленной» (add-on) защиты [6, с.87], поскольку средства защиты являются дополнением к основным программным и аппаратным средствам АСОИБ. Подобного подхода в обеспечении безопасности придерживается, например, фирма IBM, почти все модели ее компьютеров и ОС, от персональных до больших машин, используют добавленную защиту (например пакет RACF).

Другой способ носит название «встроенной» (built-in) защиты. Он заключается в том, что механизмы защиты являются неотъемлемой частью АСОИБ, разработанной и реализованной с учетом определенных требований безопасности. Механизмы защиты могут быть реализованы в виде отдельных компонентов АСОИБ, распределены по другим компонентам системы (то есть в некотором компоненте АСОИБ есть часть, отвечающая за поддержание его защиты). При этом средства защиты составляют единый механизм, который отвечает за обеспечение безопасности всей АСОИБ.

Этот способ использовался компанией DEC при разработке системы VAX/VMS.

Оба способа — добавленной и встроенной защиты — имеют свои преимущества и недостатки. Добавленная защита является более гибкой, ее механизмы можно добавлять или удалять по мере необходимости. Это не составит большого труда, так как они все реализованы отдельно от других процедур системы. Однако в этом случае остро встает вопрос поддержки работы этих механизмов встроенными механизмами ОС, в том числе и аппаратными. В том случае, если добавляемые средства защиты не поддерживаются встроенными механизмами АСОИБ, то они не обеспечат необходимого уровня безопасности.

Проблемой может стать сопряжение встроенных механизмов с добавляемыми программными средствами — довольно сложно разработать конфигурацию механизмов защиты, их интерфейс с добавляемыми программными средствами так, чтобы защита охватывала всю систему целиком.

Другой проблемой является оптимальность защиты. При любой проверке прав, назначении полномочий, разрешений доступа и т.д. необходимо вызывать отдельную процедуру. Естественно, это сказывается на производительности системы. Не менее важна и проблема совместимости защиты с имеющимися программными средствами. Как правило, при добавленной защите вносятся некоторые изменения в логику работы системы. Эти изменения могут оказаться неприемлемыми для некоторых прикладных программ. Такова плата за гибкость и облегчение обслуживания средств защиты.

Основное достоинство встроенной защиты — надежность и оптимальность. Это объясняется тем, что средства защиты и механизмы их поддержки разрабатывались и реализовывались одновременно с самой системой обработки информации, поэтому взаимосвязь средств защиты с различными компонентами системы теснее, чем при добавленной защите. Однако встроенная защита обладает жестко фиксированным набором функций, не позволяя расширять или сокращать их. Некоторые функции можно только отключить.

Справедливости ради стоит отметить, что оба вида защиты в чистом виде встречаются редко. Как правило, используются их комбинации, что позволяет объединять достоинства и компенсировать недостатки каждого из них.

Комплексная защита АСОИБ может быть реализована как с помощью добавленной, так и встроенной защиты.

Этап сопровождения заключается в контроле работы системы, регистрации происходящих в ней событий, их анализе с целью обнаружить нарушения безопасности.

В том случае, когда состав системы претерпел существенные изменения (смена вычислительной техники, переезд в другое здание, добавление новых устройств или программных средств), требуется повторение описанной выше последовательности действий.

Стоить отметить тот немаловажный факт, что обеспечение защиты АСОИБ — это итеративный процесс, завершающийся только с завершением жизненного цикла всей системы.

На последнем этапе анализа риска производится оценка реальных затрат и выигрыша от применения предполагаемых мер защиты. Величина выигрыша может иметь как положительное, так и отрицательное значение. В первом случае это означает, что использование системы защиты приносит очевидный выигрыш, а во втором - лишь дополнительные расходы на обеспечение собственной безопасности.

Сущность этого этапа заключается в анализе различных вариантов построения системы защиты и выборе оптимального из них по некоторому критерию (обычно по наилучшему соотношению «эффективность/стоимость»).

Приведем пример: необходимо оценить выгоду при защите информации от раскрытия или обработки на основе некорректных данных в течении одного года. [2, с.141]

Величину ущерба от реализации этих угроз оценим в $1.000.000. Предположим, предварительный анализ показал, что в среднем эта ситуация встречается один раз в десять лет (Р=0.1).

Тогда стоимость потерь для данной угрозы (СР) составит:

СР = С \* Р = $1.000.000 \* 0.1 = $100.000

Далее зададимся эффективностью методов защиты. Для данного абстрактного случая предположим, что в результате экспертной оценки методов защиты было получено значение 60% (в шести случаях из десяти защита срабатывает), тогда:

ЕМ = 60% \* СР = $60.000

Затраты на реализацию этих методов (закупка средств защиты, обучение персонала, изменение технологии обработки информации, зарплата персоналу и т.д.) составили (СМ) $25.000. Тогда величина выгоды равна:

PR = ЕМ - СМ = $60.000 - $25.000 = $35.000.

В рассмотренном случае величина выгоды имеет положительное значение, что говорит о целесообразности применения выбранных методов защиты.

После того, как были определены угрозы безопасности АСОИБ, от которых будет производится защита и выбраны меры защиты, требуется составить ряд документов, отражающих решение администрации АСОИБ по созданию системы защиты. Это решение конкретизируется в нескольких планах: плане защиты и плане обеспечения непрерывной работы и восстановления функционирования АСОИБ.

План защиты — это документ, определяющий реализацию системы защиты организации и необходимый в повседневной работе. Он необходим:

1. Для определения, общих правил обработки информации в АСОИБ, целей построения и функционирования системы защиты и подготовки сотрудников.

2. Для фиксирования на некоторый момент времени состава АСОИБ, технологии обработки информации, средств защиты информации.

3. Для определения должностных обязанностей сотрудников организации по защите информации и ответственности за их соблюдение.

План представляет собой организационный фундамент, на котором строится все здание системы защиты. Он нуждается в регулярном пересмотре и, если необходимо, изменении.

План защиты обычно содержит следующие группы сведений:

1. Политика безопасности.

2. Текущее состояние системы.

3. Рекомендации по реализации системы защиты.

4. Ответственность персонала.

5. Порядок ввода в действие средств защиты.

6. Порядок пересмотра плана и состава средств защиты.

Рассмотрим подробнее эти группы сведений.

Политика безопасности. В этом разделе должен быть определен набор законов, правил и практических рекомендаций, на основе которых строится управление, защита и распределение критичной информации в АСОИБ. Раздел должен содержать:

1. Цели, преследуемые реализацией системы защиты в вычислительной системе (например, защита данных компании от несанкционированного доступа, защита от утери данных и др.).

2. Меры ответственности средств защиты и нижний уровень гарантированной защиты (например, в работе небольших групп защищенных компьютеров, в обязанностях каждого из служащих и др.).

3. Обязательства и санкции, связанные с защитой (например, штрафы, персональная ответственность и др.).

Рекомендации по реализации системы защиты. Всесторонний анализ риска должен определять размеры наибольших возможных потерь, независимо от вероятности появления соответствующих событий; размеры наибольших ожидаемых потерь; меры, предпринимаемые в случае критических ситуаций, а также стоимость таких мер. Эти результаты используются при определении зон особого контроля и распределении средств для обеспечения защиты. В этом случае план защиты должен содержать рекомендации, какие средства контроля лучше всего использовать в чрезвычайных ситуациях (то есть имеющие наибольшую эффективность) и какие лучше всего соответствовали бы средствам контроля повседневной работы.

Некоторые ситуации могут приводить к слишком большому ущербу (например, крушение системы), а стоимость средств защиты от них может быть слишком высока или эти средства окажутся неэффективны. В этом случае лучше не учитывать такие ситуации при планировании защиты, хотя их и возникающие при этом возможные последствия следует отразить в плане.

Ответственность персонала. Каждый сотрудник обслуживающего персонала вычислительной системы должен хорошо знать свои обязанности и нести ответственность за свои действия. Ниже приводятся некоторые примеры обязанностей сотрудников и групп сотрудников:

1. Пользователь персонального компьютера или терминала несет ответственность за физическую целостность компьютера (терминала) во время сеанса работы с АСОИБ, а также за неразглашение собственного пароля.

2. Администратор баз данных несет ответственность за конфиденциальность информации в базах данных, ее логическую непротиворечивость и целостность.

3. Сотрудник руководства отвечает за разделение обязанностей служащих в сфере безопасности обработки информации, предупреждение возможных угроз и профилактику средств защиты.

Порядок ввода в действие средств защиты. Ввод в работу крупномасштабных и дорогих средств защиты целесообразно проводить постепенно, давая возможность обслуживающему персоналу и пользователям спокойно ознакомиться со своими новыми обязанностями. Для этого необходимо проводить разного рода тренировки, занятия по разъяснению целей защиты и способов ее реализации.

Этот раздел плана содержит расписание такого рода занятий, а также порядок ввода в действие системы защиты.

Порядок модернизации средств защиты. Важной частью плана защиты является порядок пересмотра состава средств защиты. Состав пользователей, данные, обстановка — все изменяется с течением времени, появляются новые программные и аппаратные средства. Многие средства защиты постепенно теряют свою эффективность и становятся ненужными, или подлежат замене по какой-либо иной причине (например, уменьшается ценность информации, для обработки которой достаточно более простых средств защиты). Поэтому список объектов, содержащих ценную информацию, их содержимое и список пользователей должны периодически просматриваться и изменяться в соответствии с текущей ситуацией. Также периодически должен проводиться анализ риска, учитывающий изменения обстановки. Последний пункт плана защиты должен устанавливать сроки и условия такого пересмотра, а также условия, при которых может производиться внеочередной пересмотр (например, качественный скачок в разработке методов преодоления защиты, что может нанести серьезный ущерб пользователям и владельцам АСОИБ).

Каким бы всеобъемлющим не был план, все возможные угрозы и защиту от них он предусмотреть не в состоянии. К тому же многие ситуации он должен только описывать — их контроль может оказаться неэффективным (в силу дороговизны средств защиты или малой вероятности появления угроз). В любом случае владельцы и персонал системы должны быть готовы к различным непредвиденным ситуациям.

Для определения действий персонала системы в критических ситуациях с целью обеспечения непрерывной работы и восстановления функционирования АСОИБ необходимо разрабатывать план обеспечения непрерывной работы и восстановления (план ОНРВ). В некоторых случаях план обеспечения непрерывной работы и план восстановления — разные документы. Первый скорее план, позволяющий избежать опасных ситуаций, второй — план реакции на них.

План ОНРВ можно сравнить с планом противопожарной защиты (обеспечение непрерывной работы) и ликвидации последствий (минимизация ущерба и восстановление функционирования АСОИБ). Про этот план обычно все знают, но никто его не читает, хотя на пепелище об этом обычно сожалеют.

Существует несколько способов смягчения воздействия непредвиденных ситуаций:

1. Избегать их. Это наиболее эффективный, но не всегда осуществимый способ. Избегать непредвиденных ситуаций можно с помощью ограничительных мер, предусмотренных планом защиты, а можно и с помощью устранения самой причины потенциального нарушения. Например, с пожаром можно бороться огнетушителем, а можно соблюдением мер противопожарной защиты. С рассерженными пользователями можно бороться административными мерами (разозлив этим их еще больше), а можно и поддержанием здоровой атмосферы в коллективе.

2. Если избежать какого-либо нарушения невозможно, необходимо уменьшить вероятность его появления или смягчить последствия от него.

3. Если предполагать, что какие-то нарушения все-таки могут произойти, следует предусмотреть меры сохранения контроля над ситуацией. Например, в любой момент может выйти из строя отдельный блок системы — часть компьютера, компьютер целиком, подсеть и т.д., может наступить нарушение энергоснабжения и др. В принципе это может привести к выходу АСОИБ из строя, однако при правильной организации АСОИБ этого можно избежать.

4. Если нарушение произошло, необходимо предусмотреть меры по ликвидации последствий и восстановлению информации. Например, в случае сбоя в компьютере — замену сбойного компонента, в случае уничтожения каких-либо данных — восстановление с резервных копий и т.д.

Все приведенные выше четыре способа должны в той или иной мере присутствовать в плане ОНРВ. Для каждой конкретной АСОИБ эти меры следует планировать в процессе анализа риска с учетом особенностей (специфических видов угроз, вероятностей появления, величин ущерба и т.д.) и на основе критерия «эффективность/стоимость». Хороший план ОНРВ должен отвечать следующим требованиям:

1. Реальность плана ОНРВ.

План должен оказывать реальную помощь в критических ситуациях, а не оставаться пустой формальностью. Необходимо учитывать психологический момент ситуации, при которой персонал находится в состоянии стресса, поэтому сам план и предлагаемые действия должны быть простыми и ясными. План должен учитывать реальное состояние компонентов системы, способов их взаимодействия и т.д. Повышению действенности плана ОНРВ способствуют тренировки в условиях, приближенных к реальным (естественно без реальных потерь).

2.Быстрое восстановление работоспособности системы.

Предлагаемые планом ОНРВ действия должны восстанавливать повседневную деятельность настолько быстро, насколько это возможно. В принципе это главное назначение плана ОНРВ. Расследовать причины и наказать виновных можно потом, главное — продолжить процесс обработки информации.

3. Совместимость с повседневной деятельностью.

Предлагаемые планом ОНРВ действия не должны нарушать привычный режим работы. Если его действия противоречат повседневной деятельности (возможно, возобновленной после аварии), то это приведет к еще большим проблемам.

4. Практическая проверка.

Все положения плана ОНРВ должны быть тщательно проверены, как теоретически, так и практически. Только в этом случае план ОНРВ будет удовлетворять перечисленным выше требованиям.

5. Обеспечение.

Реальная выполнимость плана ОНРВ будет достигнута только в том случае, если предварительно подготовлено, проверено и готово к работе все вспомогательное обеспечение — резервные копии, рабочие места, источники бесперебойного питания и т.д. Персонал должен совершенно точно знать, как и когда пользоваться этим обеспечением.

Наличие любого плана ОНРВ — полного или краткого, но главное —реального, благотворно влияет на моральную обстановку в коллективе. Пользователи должны быть уверены в том, что даже в самых неблагоприятных условиях какая-то часть их труда будет сохранена; руководство должно быть уверено, что не придется начинать все с начала.

План ОНРВ лучше всего строить как описание опасных ситуаций и способов реакции на них в следующем порядке:

- описание нарушения;

- немедленная реакция на нарушение - действия пользователей и администрации в момент обнаружения нарушения (сведение ущерба до минимума, уведомление руководства, останов работы, восстановительные процедуры и т.д.);

- оценка ущерба от нарушения — в чем заключаются потери и какова их стоимость (включая восстановление);

- возобновление обработки информации. После устранения нарушения и первичного восстановления необходимо как можно быстрее возобновить работу, так как машинное время — это деньги;

- полное восстановление функционирования системы - удаление и замена поврежденных компонентов системы, возобновление обработки информации в полном объеме.

В части, посвященной реакции на нарушения, план ОНРВ должен содержать перечень действий, которые выполняются персоналом при наступлении различных ситуаций. Причем действия должны быть реальными, иначе в них нет никакого смысла.

Эта часть плана должна определять:

- что должно быть сделано;

- когда это должно быть сделано;

- кем и как это должно быть сделано;

- что необходимо для того, чтобы это было сделано.

При планировании подобных действий необходимо помнить об их экономической эффективности. Например, всю информацию системы в резервных копиях держать в принципе невозможно — ее слишком много и она слишком часто обновляется. В копиях должна содержаться только самая ценная информация, значимость которой уменьшается не слишком быстро. Вообще определение степени дублирования ресурсов (критичной нагрузки; critical workload) — самостоятельная и достаточно сложная задача. Она должна решаться индивидуально для конкретных условий с учетом стоимости дублирования и загрузки системы, размеров возможного ущерба, имеющихся ресурсов и других факторов.

Для определения конкретных действий по восстановлению и возобновлению процесса обработки, включаемых в план ОНРВ, может быть полезен приводимый ниже список способов организации восстановления программ и данных, а также процесса обработки информации (первый способ для восстановления программ и данных, остальные — для возобновления самого процесса обработки информации).

Способы организации восстановления работы:

Резервное копирование и внешнее хранение программ и данных. Это основной и наиболее действенный способ сохранения программного обеспечения и данных. Резервные копии делаются с наборов данных, потеря или модификация которых могут нанести значительный ущерб. Обычно в таких копиях хранятся системное программное обеспечение и наборы данных, наиболее важное прикладное программное обеспечение, а также наборы данных, являющиеся основными в данной системе (например, база данных счетов в банке).

Резервное копирование может быть полным (копии делаются со всех наборов данных), возобновляемым (копии некоторых наборов данных периодически обновляются) и выборочным (копии делаются только с некоторых наборов данных, но потом не обновляются). Способы резервного копирования определяются для каждой конкретной АСОИБ индивидуально с точки зрения критерия экономической эффективности.

Резервное копирование не имеет никакого, смысла, если копии могут быть уничтожены вместе с оригиналами. Поэтому копии должны храниться в надежном месте, исключающем возможность уничтожения. В тоже время, должны существовать возможность их оперативного использования. Иногда хранят две и более копий каждого набора данных. Например, одна копия может храниться в сейфе, находящемся в границах доступа персонала системы, а другая — в другом здании. В случае сбоя оборудования в системе используется первая копия (оперативно!), а в случае ее уничтожения (например, при пожаре) — вторая.

Взаимодействие служб. Услуги по возобновлению процесса обработки предоставляются по взаимной договоренности другими службами или организациями, обычно безвозмездно. Взаимопомощь бывает двух видов:

1. Внешняя — другая организация предоставляет свою АСОИБ, возможно программное обеспечение для временной обработки информации пострадавшей стороной. Такой способ возобновления процесса обработки информации может использоваться для обработки небольших объемов некритичной информации. При этом желательно, чтобы две организации были примерно одного типа и работали в одной области.

2. Внутренняя — возможность обработки информации предоставляется другими подразделениями одной и той же организации (департаментами, отделами, группами). Такой способ обычно не требует больших затрат и легко доступен, если дублирующая АСОИБ позволяет проводить такого рода обработку.

Любой план хорош в том случае, если он выполним. Для обеспечения выполнимости планов необходимо чтобы работу по их составлению выполняла группа квалифицированных специалистов, размеры которой зависят от характера организации и масштабов предполагаемых мер защиты. Оптимальная численность группы 5-7 человек. Можно привлечь дополнительных сотрудников для обработки и анализа выводов и рекомендаций основной группы, или, в случае больших объемов работы, каждая группа должна составлять один план или один из пунктов плана.

Специализация сотрудников, входящих в группу разработки планов, зависит от конкретных условий. Использование защищенных протоколов, механизмов защиты операционных систем и сетей требует привлечения системных программистов. Применение средств защиты, встраиваемых в прикладное программное обеспечение делает необходимым участие в группе проблемных программистов. Необходимость организации защиты физических устройств, организации резервных рабочих мест также требует присутствия в рабочей группе соответствующих специалистов. И, наконец, поскольку АСОИБ функционирует для пользователя, то целесообразно присутствие пользователей различных категорий - для учета взгляда со стороны на удобство и эффективность предлагаемых методов и средств защиты. В большинстве случаев целесообразно, чтобы в эту группу входили следующие специалисты, каждый из которых должен отвечать за свой участок работы:

- специалисты по техническим средствам;

- системные программисты;

- проблемные программисты;

- сотрудники, отвечающие за подготовку, ввод и обработку данных;

- специалисты по защите физических устройств;

- представители пользователей.

После подготовки плана необходимо его принять и реализовать, что напрямую зависит от его четкости, корректности и ясности для сотрудников организации.

Понимание необходимости мер защиты и контроля - непременное условие нормальной работы. Известен случай о том, как пользователь менял каждый раз 24 пароля и возвращался к первоначальному, так как система была защищена от повторного использования предыдущих 23 паролей. Если сотрудники не понимают или не согласны с предлагаемыми мерами, то они будут стараться обойти их, так как любые меры контроля предполагают увеличение сложности работы.

Другой ключевой момент — управление средствами защиты и восстановления. Надежное управление осуществимо лишь в случае понимания обслуживающим персоналом размеров возможных убытков, ясного изложения планов и выполнения персоналом своих обязанностей. Многие сотрудники, обслуживающие АСОИБ, не всегда осознают риск, связанный с обработкой информации в АСОИБ. Только специальная предварительная подготовка персонала способствует правильной и эффективной работе средств защиты и восстановления; она может проводиться с привлечением сторонних специалистов. Описание различных способов преодоления и нарушения защиты в повседневной деятельности в сфере бизнеса (как, например, утечка информации к конкуренту) поможет обслуживающему персоналу понять необходимость точного выполнения требований защиты (например, своевременной смены паролей).

Важнейшим понятием, которое должно быть оформлено документально, является политика безопасности.

Политика безопасности — набор законов, правил и практических рекомендаций, на основе которых строится управление, защита и распределение критичной информации в системе. Она должна охватывать все особенности процесса обработки информации, определяя поведение системы в различных ситуациях.

Политика безопасности представляет собой некоторый набор требований, прошедших соответствующую проверку, реализуемых при помощи организационных мер и программно-технических средств и определяющих архитектуру системы защиты. Ее реализация для конкретной АСОИБ осуществляется при помощи средств управления механизмами защиты.

Для конкретной организации политика безопасности должна быть индивидуальной, зависимой от конкретной технологии обработки информации, используемых программных и технических средств, расположения организации т.д.

Перед тем, как приступит к изложению материала введем некоторые определения.

Субъект - активный компонент системы, который может явиться причиной потока информации от объекта к субъекту или изменения состояния системы.

Объект - пассивный компонент системы, хранящий, принимающий или передающий информацию. Доступ к объекту подразумевает доступ к содержащейся в нем информации.

Основу политики безопасности составляет способ управления доступом, определяющий порядок доступа субъектов системы к объектам системы. Название этого способа, как правило, определяет название политики безопасности.

Для изучения свойств способа управления доступом создается его формальное описание — математическая модель. При этом модель должна отражать состояния всей системы, ее переходы из одного состояния в другое, а также учитывать, какие состояния и переходы можно считать безопасными в смысле данного управления. Без этого говорить о каких-либо свойствах системы, и тем более гарантировать их, по меньшей мере некорректно. Отметим лишь, что для разработки моделей применяется широкий спектр математических методов (моделирования, теории информации, графов, автоматов и другие).

В настоящее время лучше всего изучены два вида политики безопасности: избирательная и полномочная, основанные, соответственно на избирательном и полномочном способах управления доступом.

Кроме того, существует набор требований, усиливающий действие этих политик и предназначенный для управления информационными потоками в системе.

Следует отметить, что средства защиты, предназначенные для реализации какого-либо из названных выше способа управления доступом, только предоставляют возможности надежного управления доступом или информационными потоками. Определение прав доступа субъектов к объектам и/или информационным потокам (полномочий субъектов и атрибутов объектов, присвоение меток критичности и т д.) входит в компетенцию администрации системы.

Для того, чтобы корректно воплотить в жизнь разработанную политику безопасности необходимо иметь надежные механизмы ее реализации. Естественно предположить, что все средства, отвечающие за реализацию политики безопасности, сами должны быть защищены от любого вмешательства в их работу. В противном случае говорить о надежности защиты будет трудно. Можно изменять их параметры, но в своей основе они должны оставаться в неприкосновенности.

Поэтому все средства защиты и управления должны быть объединены в так называемую достоверную вычислительную базу.

Достоверная вычислительная база (ДВБ) — это абстрактное понятие, обозначающее полностью защищенный механизм вычислительной системы (включая аппаратные и программные средства), отвечающий за поддержку реализации политики безопасности.

Средства защиты должны создавать ДВБ для обеспечения надежной защиты АСОИБ. В различных средствах защиты ДВБ может быть реализована по-разному. Способность реализации ДВБ к безотказной работе зависит от ее устройства и корректного управления, а ее надежность является залогом соблюдения политики безопасности в защищаемой системе.

Таким образом, ДВБ выполняет двойную задачу — поддерживает реализацию политики безопасности и является гарантом целостности механизмов защиты, то есть самой себя. ДВБ совместно используется всеми пользователями АСОИБ, однако ее модификация разрешена только пользователям со специальными полномочиями. К ним относятся администраторы системы и другие привилегированные сотрудники организации.

Процесс, функционирующий от имени ДВБ, является достоверным. Это означает, что система защиты безоговорочно доверяет этому процессу и все его действия санкционированы политикой безопасности. Именно поэтому задача номер один защиты ДВБ — поддержание собственной целостности; все программы и наборы данных ДВБ, должны быть надежно защищены от несанкционированных изменений.

Для поддержки политики безопасности и собственной защиты ДВБ должна обеспечить защиту субъектов (процессов) системы и защиту объектов системы в оперативной памяти и на внешних носителях.

Защита ДВБ строится на основе концепции иерархической декомпозиции системы. Сущность концепции заключается в том, что реальная система представляется как совокупность иерархически упорядоченных абстрактных уровней; при этом функции каждого уровня реализуются компонентами более низкого уровня. Компоненты определенного уровня зависят только от компонентов более низких уровней и их внутренняя структура полагается недоступной с более высоких уровней. Связь уровней организуется через межуровневый интерфейс.

Структура компонентов системы и связи между ними являются жестко фиксированными; их изменение, дублирование, уничтожение невозможны. Компоненты более высоких уровней привязаны к компонентам более низких уровней, те, в свою очередь, к элементам физической реализации (устройствам ввода-вывода, процессору и др.). Связи между различными компонентами определяются спецификациями межуровневого интерфейса и также не могут изменяться. Это является дополнительной мерой обеспечения целостности ДВБ.

Компоненты верхних уровней обычно описывают интерфейс пользователя. Сюда входят различные редакторы, компиляторы, интерпретаторы командных языков, утилиты и т.д. Средние уровни обычно реализуют ввод-вывод на уровне записей, работу с файлами и виртуальной памятью. Компоненты нижних уровней реализуют планирование и диспетчеризацию процессов, распределение ресурсов, ввод-вывод на физическом уровне, обработку прерываний и т.д. Компонентами нулевого уровня можно считать элементы физической реализации: особенности архитектуры процессора, состав и назначение регистров (общих и привилегированных), физическую реализацию некоторых функций и т.д. Множество компонентов всех уровней, кроме верхнего, а также средства управления ими и составляют ДВБ.

Пользователь, находясь на самом высоком уровне, может только послать запрос на выполнение какой-либо операции. Этот запрос будет разрешен к выполнению компонентами более низких уровней только в том случае, если, пройдя обработку корректности на всех промежуточных уровнях, он не был отвергнут, то есть не сможет нарушить существующую политику безопасности. При этом каждая функция может быть выполнена только определенными компонентами на определенном уровне, что определяется архитектурой системы в целом.

Например, пользователь из командного интерпретатора послал запрос на выполнение операции ввода-вывода (для редактирования файла, размещающегося на диске). Этот запрос будет обработан интерпретатором и передан на более низкий уровень — в подсистему ввода-вывода. Та проверит корректность запроса (разрешен ли доступ к этому файлу?), обработает его и передаст дальше — механизмам ввода-вывода, которые выполнят операцию и сообщат о результатах. При этом спецификации межуровневого интерфейса гарантируют, что прямой вызов примитивов ввода-вывода пользователю недоступен. Он еще может иногда обращаться непосредственно к подсистеме ввода-вывода (из программы), но не на более низкий уровень. Таким образом гарантируется невозможность доступа субъекта к объекту в обход средств контроля.

Необходимость защиты внутри отдельных компонентов системы очевидна: каждый из них должен проверять корректность обращения к реализуемой им функции.

Особенность применения концепции иерархической декомпозиции заключается в следующем:

1. Каждый компонент должен выполнять строго определенную функцию;

2. Каждая функция с помощью операции декомпозиции может быть разбита на ряд подфункций, которые реализуются и защищаются отдельно. Этот процесс может насчитывать несколько этапов;

3. Основная «тяжесть» защиты приходится на межуровневый интерфейс, связывающий декомпозированные подфункции в единое целое; горизонтальные ссылки должны быть сведены до минимума. Помимо защиты самой себя ДВБ также должна обеспечить надежную защиту пользователей системы (в частности, друг от друга). Для защиты пользователей используются те же самые механизмы, что и для защиты ДВБ. Теми же остаются и цели защиты: субъектов и объектов пользователей, в оперативной памяти и на внешних носителях. Рассмотрим подробнее принципы такой защиты.

Защита субъектов осуществляется с помощью межуровневого интерфейса: в зависимости от выполняемой им функции система переводит его на соответствующий уровень. Уровень, в свою очередь, определяет и степень управляемости процесса пользователем, который находится на самом верхнем уровне - чем ниже уровень процесса, тем меньше он управляем с более верхних уровней и тем больше он зависит от ОС.

Любые попытки защиты оперативной памяти приводят к необходимости создания виртуальной памяти в том или ином виде. Здесь используется та же концепция иерархической декомпозиции, чтобы отделить реальную память, содержащую информацию, от той, которая доступна пользователям. Соответствие между виртуальной и физической памятью обеспечивается диспетчером памяти. При этом различные области памяти могут являться компонентами разных уровней — это зависит от уровня программ, которые могут обращаться к этим областям.

Пользователи и их программы могут работать только с виртуальной памятью. Доступ к любому участку физической оперативной памяти (в том числе и принадлежащему ДВБ), контролируется диспетчером памяти. При трансляции виртуального адреса в физический проверяются права доступа к указанному участку. Надежность разделения оперативной памяти во многом обеспечивается за счет надежности функции, отображающей виртуальные адреса в физические: адресные пространства различных пользователей и системы не должны перекрываться в физической памяти.

Доступ к информации на внешних носителях осуществляется с помощью подсистемы ввода-вывода; программы этой подсистемы являются компонентами нижних и средних уровней ДВБ. При получении имени файла (адреса записи) в первую очередь проверяются полномочия пользователя на доступ к запрашиваемым данным. Принятие решение на осуществление доступа осуществляется на основе информации, хранящейся в базе данных защиты. Сама база данных является частью ДВБ, доступ к ней также контролируется.

ДВБ должна быть организована таким образом, чтобы только ее компоненты могли выполнить запрос, причем только тот, который содержит корректные параметры.

Одним из необходимых условий реализации ДВБ в средствах защиты является наличие мультирежимного процессора (то есть процессора, имеющего привилегированный и обычный режим работы) о аппаратной поддержкой механизма переключения режимов, и различных способов реализации виртуальной памяти.

Достоверная вычислительная база состоит из ряда механизмов защиты, позволяющих ей обеспечивать поддержку реализации политики безопасности.

Основой ДВБ является ядро безопасности — элементы аппаратного и программного обеспечения, защищенные от модификации и проверенные на корректность, которые разделяют все попытки доступа субъектов к объектам.

Ядро безопасности является реализацией концепции монитора ссылок (reference monitor) - абстрактной концепции механизма защиты.

Помимо ядра безопасности ДВБ содержит другие механизмы, отвечающие за жизнедеятельность системы. К ним относятся планировщики процессов, диспетчеры памяти, программы обработки прерываний, примитивы ввода-вывода и др. программно-аппаратные средства, а также системные наборы данных.

Под монитором ссылок понимают концепцию контроля доступа субъектов к объектам в абстрактной машине. Под базой данных защиты понимают базу данных, хранящую информацию о правах доступа субъектов системы к объектам. Основу базы данных защиты составляет матрица доступа или ее представления, которая служит основой избирательной политики безопасности.

Важным понятием является понятие профиля. Профилем называется список защищаемых объектов системы и прав доступа к ним, ассоциированный с каждым субъектом. При обращении к объекту профиль субъекта проверяется на наличие соответствующих прав доступа.

В системах с большим количеством объектов профили могут иметь большие размеры и, вследствие этого, ими трудно управлять; изменение профилей нескольких субъектов может потребовать большого количества операции и привести к трудностям в работе системы. Поэтому профили обычно используются лишь администраторами безопасности для контроля работы субъектов, и даже такое их применение весьма ограничено.

При реализации полномочной политики безопасности база данных защиты также содержит метки критичности всех объектов и уровни прозрачности субъектов системы.

Монитор ссылок должен выполнять следующие функции:

1. Проверять права доступа каждого субъекта к любому объекту на основании информации, содержащейся в базе данных защиты и положений политики безопасности (избирательной или полномочной);

2. При необходимости регистрировать факт доступа и его параметры в системном журнале.

Реализующее монитор ссылок ядро безопасности должно обладать следующими свойствами:

- контролировать все попытки доступа субъектов к объектам;

- иметь защиту от модификации, подделки, навязывания;

- быть протестировано и верифицировано для получения гарантий надежности;

- иметь небольшой размер и компактную структуру.

В терминах модели Белла-Лападулла (избирательной и полномочной политик безопасности) монитор ссылок должен контролировать состояния системы и переходы из одного в другое. Основными функциями, которые должно выполнять ядро безопасности совместно с другими службами ОС, являются [2, с.193]:

1. Идентификация, аутентификация и авторизация субъектов и объектов системы.

Эти функции необходимы для подтверждения подлинности субъекта, законности его прав на данный объект или на определенные действия, а также для обеспечения работы субъекта в системе.

- Идентификация - процесс распознавания элемента системы, обычно с помощью заранее определенного идентификатора или другой априорной информации; каждый субъект или объект должен быть однозначно идентифицируем.

- Аутентификация - проверка идентификации пользователя, процесса, устройства или другого компонента системы (обычно осуществляется перед разрешением доступа); а также проверка целостности данных при их хранении или передаче для предотвращения несанкционированной модификации.

- Авторизация - предоставление субъекту прав на доступ к объекту.

Эти функции необходимы для поддержания разрешительного порядка доступа к системе и соблюдения политики безопасности: авторизованный (разрешенный) доступ имеет только тот субъект, чей идентификатор удовлетворяет результатам аутентификации. Они выполняются как в процессе работы (при обращении к наборам данных, устройствам, ресурсам), так и при входе в систему.

2. Контроль входа пользователя в систему и управление паролями. Эти функции являются частным случаем перечисленных выше: при входе в систему и вводе имени пользователя осуществляется идентификация, при вводе пароля — аутентификация и, если пользователь с данными именем и паролем зарегистрирован в системе, ему разрешается доступ к определенным объектам и ресурсам (авторизация). Однако при входе в систему существуют отличия при выполнении этих функций. Они обусловлены тем, что в процессе работы система уже имеет информацию о том, кто работает, какие у него полномочия (на основе информации в базе данных защиты) и т.д. и поэтому может адекватно реагировать на запросы субъекта. При входе в систему это все только предстоит определить. В данном случае возникает необходимость организации «достоверного маршрута» — пути передачи идентифицирующей информации от пользователя к ядру безопасности для подтверждения подлинности. Как показывает практика, вход пользователя в систему - одно из наиболее уязвимых мест защиты; известно множество случаев взлома пароля, входа без пароля, перехвата пароля и т.д. Поэтому при выполнении входа и пользователь, и система должны быть уверены, что они работают непосредственно друг с другом, между ними нет других программ и вводимая информация истинна.

Достоверный маршрут реализуется привилегированными процедурами ядра безопасности, чья работа обеспечивается механизмами ДВБ, а также некоторыми другими механизмами, выполняющими вспомогательные функции. Они проверяют, например, что терминал, с которого осуществляется вход в систему, не занят никаким другим пользователем, который имитировал окончание работы.

3. Регистрация и протоколирование. Аудит.

Эти функции обеспечивают получение и анализ информации о состоянии ресурсов системы с помощью специальных средств контроля, а также регистрацию действий, признанных администрацией потенциально опасными для безопасности системы. Такими средствами могут быть различные системные утилиты или прикладные программы, выводящие информацию непосредственно на системную консоль или другое определенное для этой цели устройство, а также системный журнал. Кроме того, почти все эти средства контроля могут не только обнаружить какое-либо событие, но и фиксировать его. Например, большинство систем имеет средства протоколирования сеансов работы отдельных пользователей (всего сеанса или его отдельных параметров).

Большинство систем защиты имеют в своем распоряжении средства управления системным журналом. Системный журнал является составной частью монитора ссылок и служит для контроля соблюдения политики безопасности. Он является одним из основных средств контроля, помогающим администратору предотвращать возможные нарушения в связи с тем, что:

- способен оперативно фиксировать происходящие в системе события;

- может помочь выявить средства и априорную информацию, использованные злоумышленником для нарушения;

- может помочь определить, как далеко зашло нарушение, подсказать метод его расследования и способы исправления ситуации.

Содержимое системного журнала и других наборов данных, хранящих информацию о результатах контроля, должны подвергаться периодическому просмотру и анализу (аудит) с целью проверки соблюдения политики безопасности.

4. Противодействие «сборке мусора».

После окончания работы программы обрабатываемая информация не всегда полностью удаляется из памяти. Части данных могут оставаться в оперативной памяти, на дисках и лентах, других носителях. Они хранятся на диске до перезаписи или уничтожения. При выполнении этих действий на освободившемся пространстве диска находятся их остатки.

Хотя при искажении заголовка файла эти остатки прочитать трудно, однако, используя специальные программы и оборудование, такая возможность все-таки имеется. Этот процесс называется «сборкой мусора». Он может привести к утечке важной информации.

Для защиты от «сборки мусора» используются специальные средства, которые могут входить в ядро безопасности ОС или устанавливаться дополнительно.

5. Контроль целостности субъектов.

Согласно модели Белла-Лападулла [2, с.196] множество субъектов системы есть подмножество множества объектов, то есть каждый субъект одновременно является объектом. При этом под содержимым субъекта обычно понимают содержимое контекста процесса, куда входит содержимое общих и специальных регистров (контекст процесса постоянно изменяется). Кроме содержимого или значения субъект имеет ряд специфических атрибутов: приоритет, список привилегий, набор идентификаторов и др. характеристики. В этом смысле поддержание целостности субъекта, то есть предотвращение его несанкционированной модификации, можно рассматривать как частный случай этой задачи для объектов вообще.

В то же время субъект отличается от объекта тем, что является, согласно определению, активным компонентом системы. В связи с этим для защиты целостности субъекта, в качестве представителя которого выступает процесс, вводится такое понятие как рабочая среда или область исполнения процесса. Эта область является логически защищенной подсистемой, которой доступны все ресурсы системы, относящиеся к соответствующему процессу. Другими словами, область исполнения процесса является виртуальной машиной. В рамках этой области процесс может выполнять любые санкционированные действия без опасения нарушения целостности. Таким образом, реализуется концепция защищенной области для отдельного процесса.

Контроль целостности обеспечивается процедурами ядра безопасности, контролируемыми механизмами поддержки ДВБ. Основную роль играют такие механизмы, как поддержка виртуальной памяти (для создания области данного процесса) и режим исполнения процесса (определяет его возможности в рамках данной области и вне ее).

Область исполнения процесса может содержать или вкладываться в другие подобласти, которые составляют единую иерархическую структуру системы. Процесс может менять области: это действие называется переключением области процесса. Оно всегда связано с переходом центрального процессора в привилегированный режим работы.

Механизмы поддержки областей исполнения процесса обеспечивают контроль их целостности достаточно надежно. Однако даже разделенные процессы должны иметь возможность обмениваться информацией. Для этого разработаны несколько специальных механизмов, чтобы можно было осуществлять обмен информацией между процессами без ущерба безопасности или целостности каждого из них. К таким механизмам относятся, например, кластеры флагов событий, почтовые ящики и другие системные структуры данных. Следует однако учитывать, что с их помощью может осуществляться утечка информации, поэтому если использование таких механизмов разрешено, их обязательно следует контролировать.

6. Контроль доступа.

Под контролем доступа будем понимать ограничение возможностей использования ресурсов системы программами, процессами или другими системами (для сети) в соответствии с политикой безопасности. Под доступом понимается выполнение субъектом некоторой операции над объектом из множества разрешенных для данного типа. Примерами таких операций являются чтение, открытие, запись набора данных, обращение к устройству и т.д.

Контроль должен осуществляться при доступе к:

- оперативной памяти;

- разделяемым устройствам прямого доступа;

- разделяемым устройствам последовательного доступа;

- разделяемым программам и подпрограммам;

- разделяемым наборам данных.

Основным объектом внимания средств контроля доступа являются совместно используемые наборы данных и ресурсы системы. Совместное использование объектов порождает ситуацию «взаимного недоверия», при которой разные пользователи одного объекта не могут до конца доверять друг другу. Тогда, если с этим объектом что-нибудь случиться, все они попадают в круг подозреваемых.

Существует четыре основных способа разделения субъектов к совместно используемым объектам:

1. Физическое - субъекты обращаются к физически различным объектам (однотипным устройствам, наборам данных на разных носителях и т.д.).

2. Временное - субъекты с различными правами доступа к объекту получают его в различные промежутки времени.

3. Логическое - субъекты получают доступ к совместно используемому объекту в рамках единой операционной среды, но под контролем средств разграничения доступа, которые моделируют виртуальную операционную среду «один субъект - все объекты»; в этом случае разделение может быть реализовано различными способами разделение оригинала объекта, разделение с копированием объекта и т.д.

4. Криптографическое - все объекты хранятся в зашифрованном виде, права доступа определяются наличием ключа для расшифрования объекта.

Существует множество различных вариантов одних и тех же способов разделения субъектов, они могут иметь разную реализацию в различных средствах защиты.

Контроль доступа субъектов системы к объектам (не только к совместно используемым, но и к индивидуальным) реализуется с помощью тех же механизмов, которые реализуют ДВБ и осуществляется процедурами ядра безопасности.

Как уже отмечалось выше, настройка механизмов защиты — дело сугубо индивидуальное для каждой системы и даже для каждой задачи. Поэтому дать ее подробное описание довольно трудно. Однако существуют общие принципы, которых следует придерживаться, чтобы облегчить себе работу, так как они проверены практикой. Рассмотрим их:

1.Группирование.

Это объединение множества субъектов под одним групповым именем; всем субъектам, принадлежащим одной группе, предоставляются равные права. Принципы объединения пользователей в группы могут быть самые разные: одинаковый характер вычислений, работа над совместным проектом и т.д. При этом один и тот же субъект может входить в несколько различных групп, и, соответственно, иметь различные права по отношению к одному и тому же объекту. Механизм группирования может быть иерархическим. Это означает, что каждый субъект является членом нескольких групп, упорядоченных по отношению «быть подмножеством». Контроль за состоянием групп очень важен, поскольку члены одной группы имеют доступ к большому числу объектов, что не способствует их безопасности. Создание групп и присвоение групповых привилегий должно производиться администратором безопасности, руководителем группы или каким-либо другим лицом, несущим ответственность за сохранность групповых объектов.

2. Правила умолчания.

Большое внимание при назначении привилегий следует уделять правилам умолчания, принятым в данных средствах защиты; это необходимо для соблюдения политики безопасности. Во многих системах, например, субъект, создавший объект и являющийся его владельцем, по умолчанию получает все права на него. Кроме того, он может эти права передавать кому-либо. В различных средствах защиты используются свои правила умолчания, однако принципы назначения привилегий по умолчанию в большинстве систем одни и те же. Если в системе используется древовидная файловая структура, то необходимо принимать во внимание правила умолчания для каталогов. Корректное использование правил умолчания способствуют поддержанию целостности политики безопасности.

3. Минимум привилегий.

Это один из основополагающих принципов реализации любой политики безопасности, используемый повсеместно. Каждый пользователь и процесс должен иметь минимальное число привилегий, необходимых для работы. Определение числа привилегий для всех пользователей, с одной стороны, позволяющих осуществлять быстрый доступ ко всем необходимым для работы объектам, а, с другой, — запрещающих доступ к чужим объектам — проблема достаточно сложная. От ее решения во многом зависит корректность реализации политики безопасности.

4. Принцип «надо знать».

Этот принцип во многом схож с предыдущим. Согласно ему, полномочия пользователей назначаются согласно их обязанностям. Доступ разрешен только к той информации, которая необходима им для работы. Согласно принципу, пользователь должен знать обо всех доступных ему ресурсах. В том случае, если пользователь не знает о них, такие ресурсы должны быть отключены.

5. Объединение критичной информации.

Во многих системах сбор, хранение и обработка информации одного уровня производится в одном месте (узле сети, устройстве, каталоге). Это связано с тем, что проще защитить одним и тем же способом большой массив информации, чем организовать индивидуальную защиту для каждого набора данных. Для реализации этого принципа могут быть разработаны специальные программы, управляющие обработкой таких наборов данных. Это будет простейший способ построения защищенных областей.

6. Иерархия привилегий.

Контроль объектов системы может иметь иерархическую организацию. Такая организация принята в большинстве коммерческих систем.

При этом схема контроля имеет вид дерева, в котором узлы — субъекты системы, ребра — право контроля привилегий согласно иерархии, корень — администратор системы, имеющий право изменять привилегии любого пользователя.

Узлами нижележащих уровней являются администраторы подсистем, имеющие права изменять привилегии пользователей этих подсистем (в их роли могут выступать руководители организаций, отделов). Листьями дерева являются все пользователи системы. Вообще говоря, субъект, стоящий в корне любого поддерева, имеет право изменять защиту любого субъекта, принадлежащего этому поддереву.

Достоинство такой структуры — точное копирование схемы организации, которую обслуживает АСОИБ. Поэтому легко составить множество субъектов, имеющих право контролировать данный объект. Недостаток иерархии привилегий — сложность управления доступом при большом количестве субъектов и объектов, а также возможность получения доступа администратора системы (как высшего по иерархии) к любому набору данных.

7. Привилегии владельца.

При таком контроле каждому объекту соответствует единственный субъект с исключительным правом контроля объекта — владелец. Как правило, это его создатель. Владелец обладает всеми разрешенными для этого типа данных правами на объект, может разрешать доступ любому другому субъекту, но не имеет права никому передать привилегию на корректировку защиты. Однако такое ограничение не касается администраторов системы — они имеют право изменять защиту любых объектов.

Главным недостатком принципа привилегий владельца является то, что при обращении к объекту, пользователь должен предварительно получить разрешение у владельца (или администратора). Это может приводить к сложностям в работе (например; при отсутствии владельца или просто нежелании его разрешить доступ). Поэтому такой принцип обычно используется при защите личных объектов пользователей.

8. Свободная передача привилегий.

При такой схеме субъект, создавший объект, может передать любые права на него любому другому субъекту. Тот, в свою очередь, может передать все эти права другому субъекту.

Естественно, при этом возникают большие трудности в определении круга субъектов, имеющих в данный момент доступ к объекту (права на объект могут распространяться очень быстро и так же быстро исчезать), и поэтому такой объект легко подвергнуть несанкционированной обработке. В силу этих обстоятельств подобная схема применяется достаточно редко — в основном в исследовательских группах, работающих над одним проектом (когда все имеющие доступ к объекту заинтересованы в его содержимом).

В чистом виде рассмотренные принципы реализации политики безопасности применяются редко. Обычно используются их различные комбинации. Ограничение доступа к объектам в ОС включает в себя ограничение доступа к некоторым системным возможностям, например, ряду команд, программам и т.д., если при использовании их нарушается .политика безопасности. Вообще набор полномочий каждого пользователя должен быть тщательно продуман, исключены возможные противоречия и дублирования, поскольку большое количество нарушений происходит именно из-за этого. Может произойти утечка информации без нарушения защиты, если плохо была спроектирована или реализована политика безопасности.

Политика безопасности и механизмы поддержки ее реализации образуют единую защищенную среду обработки информации. Эта среда имеет иерархическую структуру, где верхние уровни представлены требованиями политики безопасности, далее следует интерфейс пользователя, затем идут несколько программных уровней защиты (включая уровни ОС) и. наконец, нижний уровень этой структуры представлен аппаратными средствами защиты. На всех уровнях, кроме верхнего, должны реализовываться требования политики безопасности, за что, собственно, и отвечают механизмы защиты.

В различных системах механизмы защиты могут быть реализованы по-разному; их конструкция определяется общей концепцией системы. Однако одно требование должно выполняться неукоснительно: эти механизмы должны адекватно реализовывать требования политики безопасности.

Имеется два подхода к обеспечению безопасности АСОИБ.

«Фрагментарный» подход ориентируется на противодействие строго определенным угрозам при определенных условиях. Примерами реализации такого подхода являются, например, специализированные антивирусные средства, отдельные средства регистрации и управления, автономные средства шифрования и т.д. Главная отличительная особенность «фрагментарного» подхода — отсутствие единой защищенной среды обработки информации.

Главным достоинством «фрагментарного» подхода является его высокая избирательность относительно конкретной угрозы, обуславливающая и основной его недостаток — локальность действия. Другими словами, фрагментарные меры защиты обеспечивают эффективную защиту конкретных объектов АСОИБ от конкретной угрозы, но не более того. Даже небольшое видоизменение угрозы ведет к потере эффективности защиты; распространить действие таких мер на всю АСОИБ практически невозможно.

Особенностью комплексного подхода является создание защищенной среды обработки информации в АСОИБ, объединяющей разнородные меры противодействия угрозам (правовые, организационные, программно-технические). Защищенная среда обработки информации строится на основе разработанных для конкретной АСОИБ правил обработки критической информации.

Организация защищенной среды обработки информации позволяет гарантировать (в рамках разработанной политики безопасности) уровень безопасности АСОИБ. Недостатками подхода являются высокая чувствительность к ошибкам установки и настройки средств защиты, сложность управления, ограничения на свободу действий пользователей АСОИБ.

Комплексный подход применяют для защиты крупных АСОИБ, или небольших АСОИБ, обрабатывающих дорогостоящую информацию или выполняющих ответственные задачи. При этом способ реализации комплексной защиты определяется спецификой АСОИБ, другими объективными и субъективными факторами.

Для всех крупных организаций характерно то, что нарушение безопасности информации в их АСОИБ может нанести огромный материальный ущерб как самим организациям, так и их клиентам. Поэтому эти организации вынуждены особое внимание уделять гарантиям безопасности, что ведет к необходимости реализации комплексной защиты.

Комплексного подхода придерживаются большинство государственных и крупных коммерческих предприятий и учреждений, он нашел свое отражение в различных стандартах и целенаправленно проводится в жизнь, например, Министерством обороны США в лице Национального Центра Компьютерной Безопасности (NCSC). [2, с.201]

Важным компонентом защиты является «горячий резерв».

«Горячий резерв» используется для возобновления процесса обработки после событий, вызвавших полный или частичный отказ основной системы — в результате отключения энергоснабжения, неисправности оборудовании или программного обеспечения, злого умысла («вирусная атака») и т.д.

«Горячий резерв» — это готовая к работе дублирующая система, в которой полностью сгенерирована операционная система, размещены прикладное программное обеспечение и наборы данных. Кроме того, резервная система должна иметь работоспособные периферийные устройства, подключенные каналы связи, источники энергоснабжения и даже персонал. Время на подготовку определяется временем загрузки резервных копий и системы.

Содержание «горячего резерва» обходится очень дорого. Однако в некоторых случаях — для обработки информации, требующей полного контроля со стороны ее владельца, «горячий резерв» необходим. Кроме того, можно содержать и использовать «горячий резерв» на кооперативных началах — вместе с другими организациями.

«Расщепленный резерв» представляет собой способ не столько восстановления, сколько организации АСОИБ. В этом смысле о нем можно говорить, как о способе организации системы с высокой степенью распределенности и взаимодублирующими составными частями. При таком подходе критичные элементы системы (аппаратура, программы, данные) разнесены по отдельным ее частям (узлам распределенной системы) и функционируют в какой-то мере независимо, обмениваясь между собой информацией по каналам связи.

В случае выхода из строя отдельных элементов системы другие могут взять на себя их функции. Времени на приведение дублирующих элементов в рабочее состояние очень мало, фактически оно определяется загрузкой из резервных копий (так как аппаратура расщепленного резерва всегда находится в рабочем состоянии).

Такой способ обеспечения непрерывной работы и восстановления очень эффективен, так как позволяет быстро осуществлять переход с основных элементов АСОИБ на дублирующие. Более того, этот переход может быть практически незаметен для пользователей за исключением возрастания нагрузки на отдельные элементы. Однако при использовании «расщепленного резерва» возникает множество проблем, основными из которых являются:

1. Определение критической нагрузки. Распределение аппаратуры, программ и данных по элементам всей АСОИБ таким, чтобы обеспечить оптимальное дублирование и восстановление данных и процесса их обработки в различных ситуациях. Существующие математические методы позволяют рассчитывать оптимальную критическую нагрузку для каждого конкретного случая.

2. Обеспечение безопасности. При распределении программ и данных по различным элементам системы неизбежно увеличивается вероятность различных нарушений. Эта вероятность повышается в критических случаях, когда информация может обрабатываться на других элементах системы, возможно, с нарушением безопасности. В этом случае необходимо разрабатывать политику безопасности и составлять планы с учетом возможных опасных ситуаций и реакции на них.

«Холодный резерв» используется для возобновления процесса обработки после серьезных, нанесший большой ущерб событий, которые привели к полному выходу системы из строя пожара, наводнения и т.д. Время на восстановление в этом случае может исчисляться неделями и месяцами. Естественно, это слишком большой срок, чтобы позволить себе обходиться без обработки информации.

«Холодный резерв» представляет собой резервную систему обработки данных, которая не участвует в повседневной деятельности организации. Резервная система поставляется определенными фирмами (по заранее согласованной договоренности) в течение короткого промежутка времени (24 часа). Так же оперативно выполняются пуско-наладочные работы, после чего резервная система готова принять на себя функции основной.

В результате подобных мероприятий перерыв в работе АСОИБ в результате полного и необратимого выхода ее из строя будет исчисляться днями, а не неделями и месяцами. В то же время, покупка и установка резервной системы — дело дорогое, к тому же она не сможет принять на себя все функции основной, а только некоторую их часть. Поэтому «холодный резерв» целесообразно использовать для возобновления выполнения наиболее важных операций.

В том случае, когда размер ущерба невелик, система серьезно не пострадала, то наилучшим способом может быть отсутствие экстренных действий и продолжение работы.

Важным понятием политики безопасности является избирательная политика безопасности

Основой избирательной политики безопасности является избирательное управление доступом (ИУД), которое подразумевает, что:

- все субъекты и объекты системы должны быть идентифицированы;

- права доступа субъекта к объекту системы определяются на основании некоторого внешнего (по отношению к системе) правила (свойство избирательности).

Для описания свойств избирательного управления доступом применяется модель системы на основе матрицы доступа (МД, иногда ее называют матрицей контроля доступа). Такая модель получила название матричной.

Матрица доступа представляет собой матрицу, в которой объекту системы соответствует столбец, а субъекту — строка. На пересечении столбца и строки матрицы указывается тип (типы) разрешенного доступа субъекта к объекту. Обычно выделяют такие типы доступа субъекта к объекту как «доступ на чтение», «доступ на запись», «доступ на исполнение» и др.

Множество объектов и типов доступа к ним субъекта может изменяться в соответствии с некоторыми правилами, существующими в данной системе. Определение и изменение этих правил также является задачей ИУД. Например, доступ субъекта к конкретному объекту может быть разрешен только в определенные дни (дата-зависимое условие), часы (время-зависимое условие), в зависимости от других характеристик субъекта (контекстно-зависимое условие) или в зависимости от характера предыдущей работы. Такие условия на доступ к объектам обычно используются в СУБД. Кроме того, субъект с определенными полномочиями может передать их другому субъекту (если это не противоречит правилам политики безопасности).

Решение на доступ субъекта к объекту принимается в соответствии с типом доступа, указанным в соответствующей ячейке матрицы доступа. Обычно, избирательное управление доступом реализует принцип «что не разрешено, то запрещено», предполагающий явное разрешение доступа субъекта к объекту.

Матрица доступа — наиболее примитивный подход к моделированию систем, который, однако, является основой для более сложных моделей, наиболее полно описывающих различные стороны реальных АСОИБ.

Вследствие больших размеров и разреженности МД хранение полной матрицы представляется нецелесообразным, поэтому во многих средствах защиты используют более экономные представления МД (профили). Каждый из этих способов представления МД имеет свои достоинства и недостатки, обуславливающие область их применения. Поэтому в каждом конкретном случае надо знать, во-первых, какое именно представление использует средство защиты, и, во-вторых, какие особенности и свойства имеет это представление.

Основу полномочной политики безопасности составляет полномочное управление доступом, которое подразумевает, что:

- все субъекты и объекты системы должны быть однозначно идентифицированы;

- каждому объекту системы присвоена метка критичности, определяющая ценность содержащейся в нем информации;

- каждому субъекту системы присвоен уровень прозрачности, определяющий максимальное значение метки критичности объектов, к которым субъект имеет доступ.

В том случае, когда совокупность меток имеет одинаковые значения, говорят, что они принадлежат к одному уровню безопасности. Организация меток имеет иерархическую структуру и, таким образом, в системе можно реализовать иерархически ненисходящий (по ценности) поток информации (например, от рядовых исполнителей к руководству). Чем важнее объект или субъект, тем выше его метка критичности. Поэтому наиболее защищенными оказываются объекты с наиболее высокими значениями метки критичности.

Каждый субъект кроме уровня прозрачности имеет текущее значение уровня безопасности, которое может изменяться от некоторого минимального значения до значения его уровня прозрачности.

Для моделирования полномочного управления доступом используется модель Белла-Лападула [2, с.159], включающая в себя понятия безопасного (с точки зрения политики) состояния и перехода. Для принятия решения на разрешение доступа производится сравнение метки критичности объекта с уровнем прозрачности и текущим уровнем безопасности субъекта. Результат сравнения определяется двумя правилами: «простым условием защиты» и «свойством». В упрощенном виде, они определяют, что информация может передаваться только «наверх», то есть субъект может читать содержимое объекта, если его текущий уровень безопасности не ниже метки критичности объекта, и записывать в него, - если не выше.

Простое условие защиты гласит, что любую операцию над объектом субъект может выполнять только в том случае, если его уровень прозрачности не ниже метки критичности объекта.

Основное назначение полномочной политики безопасности — регулирование доступа субъектов системы к объектам с различным уровнем критичности и предотвращение утечки информации с верхних уровней должностной иерархии на нижние, а также блокирование возможных проникновении с нижних уровней на верхние. При этом она функционирует на фоне избирательной политики, придавая ее требованиям иерархически упорядоченный характер (в соответствии с уровнями безопасности).

Изначально полномочная политика безопасности была разработана в интересах минобороны США для обработки информации с различными грифами секретности. Ее применение в коммерческом секторе сдерживается следующими основными причинами :

- отсутствием в коммерческих организациях четкой классификации хранимой и 'обрабатываемой информации, аналогичной государственной классификации (грифы секретности сведений);

- высокой стоимостью реализации и большими накладными расходами.

Помимо управления доступом субъектов к объектам системы проблема защиты информации имеет еще один аспект. Чтобы получить информацию о каком-либо объекте системы, вовсе не обязательно искать пути несанкционированного доступа к нему. Можно получать информацию, наблюдая за работой системы и, в частности, за обработкой требуемого объекта. Иными словами, при помощи каналов утечки информации. По этим каналам можно получать информацию не только о содержимом объекта, но и о его состоянии, атрибутах и др. в зависимости от особенностей системы и установленной защиты объектов. Эта особенность связана с тем, что при взаимодействии двух субъектов возникает некоторый поток информации от одного к другому.

Информационные потоки существуют в системе всегда. Поэтому возникает необходимость определить, какие информационные потоки в системе являются «легальными», то есть не ведут к утечке информации, а какие - ведут. Таким образом, возникает необходимость разработки правил, регулирующих управление информационными потоками в системе.

Для этого необходимо построить модель системы, которая может описывать такие потоки. Такая модель называется потоковой [2, с.176]. Модель описывает условия и свойства взаимного влияния (интерференции) субъектов, а также количество информации, полученной субъектом в результате интерференции.

Управление информационными потоками в системе не есть самостоятельная политика, так как оно не определяет правил обработки информации. Управление информационными потоками применяется обычно в рамках избирательной или полномочной политики, дополняя их и повышая надежность системы защиты.

Управление доступом (избирательное или полномочное) сравнительно легко реализуемо (аппаратно или программно), однако оно неадекватно реальным АСОИБ из-за существования в них скрытых каналов. Тем не менее управление доступом обеспечивает достаточно надежную защиту в простых системах, не обрабатывающих особо важную информацию. В противном случае средства защиты должны дополнительно реализовывать управление информационными потоками. Организация такого управления в полном объеме достаточна сложна, поэтому его обычно используют для усиления надежности полномочной политики: ненисходящие (относительно уровней безопасности) информационные потоки считаются разрешенными, все остальные — запрещенными.

Отметим, что кроме способа управления доступом политика безопасности включает еще и другие требования, такие как подотчетность, гарантии и т.д.

Избирательное и полномочное управление доступом, а также управление информационными потоками — своего рода три кита, на которых строится вся защита.

# Глава 5. Безопасность компьютерных сетей в банке.

## Классификация сетей.

Сети компьютеров имеют множество преимуществ перед совокупностью отдельных систем, в их числе следующие:

\* Разделение ресурсов.

Пользователи сети могут иметь доступ к определенным ресурсам всех узлов сети. В их числе, например, наборы данных, свободная память на удаленных узлах, вычислительная мощность удаленных процессоров и т.д. Это позволяет экономить значительные средства за счет оптимизации использования ресурсов и их динамического перераспределения в процессе работы.

\* Повышение надежности функционирования системы. Поскольку сеть состоит из совокупности отдельных узлов, то в случае сбоя на одном или нескольких узлах другие узлы смогут взять на себя их функции. При этом пользователи могут даже и не заметить этого- перераспределение задач возьмет на себя программное обеспечение сети.

\* Распределение загрузки.

В сетях с переменным уровнем загруженности имеется возможность перераспределять задачи с одних узлов сети (с повышенной нагрузкой) на другие, где имеются свободные ресурсы. Такое перераспределение может производиться динамически в процессе работы, более того, пользователи могут даже и не знать об особенностях планирования задач в сети. Эти функции может брать на себя программное обеспечение сети.

\* Расширяемость.

Сеть может быть легко расширена за счет добавления новых узлов. При этом архитектура практически всех сетей позволяет легко адаптировать сетевое программное обеспечение к изменениям конфигурации. Более того, это может производиться автоматически.

Однако с точки зрения безопасности эти достоинства превращаются в уязвимые места, порождая серьезные проблемы.

Особенности работы в сети определяются ее двойственным характером: с одной стороны, сеть следует рассматривать как единую систему, а с другой, - как совокупность независимых систем, каждая из которых выполняет свои функции; имеет своих пользователей. Эта же двойственность проявляется в логическом и физическом восприятии сети: на физическом уровне взаимодействие отдельных узлов осуществляется с помощью сообщений различного вида и формата, которые интерпретируются протоколами. На логическом уровне (т.е. сточки зрения протоколов верхних уровней) сеть представляется как совокупность функций, распределенных по различным узлам, но связанных в единый комплекс.

Сети подразделяются: [8, с.4-7]

1 По топологии сети (классификация по организации физического уровня).

\* Общая шина.

Все узлы соединены с общей высокоскоростной шиной передачи данных. Они одновременно настроены на прием сообщения, но каждый узел может принять только то сообщение, которое предназначено ему. Адрес идентифицируется контроллером сети, при этом в сети может быть только один узел с заданным адресом. Если два узла одновременно заняты передачей сообщения (столкновение пакетов), то один из них или они оба ее прекращают, ожидают случайный интервал времени, затем возобновляют попытку передачи (метод разрешения конфликтов). Возможен другой случай — в момент передачи каким-либо узлом сообщения по сети, другие узлы начать передачу не могут (метод предотвращения конфликтов). Такая топология сети является очень удобной: все узлы являются равноправными, логическое расстояние между любыми двумя узлами равно 1, скорость передачи сообщений велика. Впервые организация сети «общая шина» и соответствующие протоколы нижних уровней были разработаны совместно компаниями DIGITAL и Rank Xerox, она получила название Ethernet.

\* Кольцо.

Сеть построена в виде замкнутого контура однонаправленных каналов между станциями. Каждая станция принимает сообщения по входному каналу, в начале сообщения содержится адресная и управляющая информация. На основании ее станция принимает решение сделать копию сообщения и убрать его из кольца либо передать по выходному каналу на соседний узел. Если в настоящий момент не передается никакого сообщения, станция сама может передать сообщение.

В кольцевых сетях используется несколько различных способов управления:

- гирляндная — управляющая информация передается по отдельным совокупностям (цепям) компьютеров кольца;

- управляющий маркер — управляющая информация оформляется в виде определенного битового шаблона, циркулирующего по кольцу; только при получении маркера станция может выдать сообщение в сеть (наиболее известный способ, получивший название token ring);

- сегментная — по кольцу циркулирует последовательность сегментов. Обнаружив пустой, станция может поместить в него сообщение и передать в сеть;

- вставка регистров — сообщение загружается в регистр сдвига и передается в сеть когда кольцо свободно.

\* Звезда.

Сеть состоит из одного узла-концентратора и нескольких соединенных с ним терминальных узлов, непосредственно между собой несвязанных. Один или несколько терминальных узлов могут являться концентраторами другой сети, в этом случае сеть приобретает древовидную топологию.

Управление сетью полностью осуществляется концентратором; терминальные узлы могут связываться между собой только через него. Обычно на терминальных узлах выполняется лишь локальная обработка данных. Обработка данных, имеющих отношение ко всей сети, осуществляется на концентраторе. Она носит название централизованной. Управление сетью обычно осуществляется с помощью процедуры опроса: концентратор через определенные промежутки времени опрашивает по очереди терминальные станции - есть ли для него сообщение. Если есть - терминальная станция передает сообщение на концентратор, если нет - осуществляется опрос следующей станции. Концентратор может передать сообщение одному или нескольким терминальным станциям в любой момент времени.

2. По размерам сети:

\* Локальные. Сеть передачи данных, связывающая ряд узлов в одной локальной зоне (комната, организация); обычно узлы сети комплектуются однотипным аппаратным и программным обеспечением (хотя это и необязательно). Локальные сети обеспечивают высокие скорости передачи информации. Локальные сети характеризуются короткими (не более нескольких километров) линиями связи, контролируемой рабочей средой, низкой вероятностью ошибок, упрощенными протоколами. Для связи локальных сетей с территориальными используются шлюзы.

\* Территориальные. Отличаются от локальных большей протяженностью линий связи (город, область, страна, группа стран), которые могут обеспечиваться телекоммуникационными компаниями. Территориальная сеть может связывать несколько локальных сетей, отдельные удаленные терминалы и ЭВМ и может быть соединена с другими территориальными сетями.

Территориальные сети редко используют какие-либо типовые топологические конструкции, так как они предназначены для выполнения других, обычно специфических задач. Поэтому они как правило строятся в соответствии с произвольной топологией, управление осуществляется с помощью специфических протоколов.

3. По организации обработки информации (классификация на логическом уровне представления; здесь под системой понимается вся сеть как единый комплекс):

\* Централизованная.

Системы такой организации наиболее широко распространены и привычны. Они состоят из центрального узла, реализующего весь комплекс выполняемых системой функций, и терминалов, роль которых сводится к частичному вводу и выводу информации. В основном периферийные устройства играют роль терминалов, с которых осуществляется управление процессом обработки информации. Роль терминалов могут выполнять дисплейные станции или персональные компьютеры, как локальные, так и удаленные. Любая обработка (в том числе связь с другими сетями) выполняется через центральный узел. Особенностью таких систем является высокая нагрузка на центральный узел, в силу чего там должен быть высоконадежный и высокопроизводительный компьютер. Центральный узел является наиболее уязвимой частью системы: выход его из строя выводит из строя всю сеть. В тоже время задачи обеспечения безопасности в централизованных системах решаются наиболее просто и фактически сводятся к защите центрального узла.

Другой особенностью таких систем является неэффективное использование ресурсов центрального узла, а также неспособность гибкой перестройки характера работы (центральный компьютер должен работать все время, а значит какую-то его часть он может работать вхолостую). В настоящее время доля систем с централизованным управлением постепенно падает.

\* Распределенная.

Практически все узлы этой системы могут выполнять сходные функции, причем каждый отдельный узел может использовать оборудование и программное обеспечение других узлов. Основной частью такой системы является распределенная ОС, которая распределяет объекты системы: файлы, процессы (или задачи), сегменты памяти, другие ресурсы. Но при этом ОС может распределять не все ресурсы или задачи, а только часть их, например, файлы и свободную память на диске. В этом случае система все равно считается распределенной, количество ее объектов (функций, которые могут быть распределены по отдельным узлам) называется степенью распределенности. Такие системы могут быть как локальными, так и территориальными. Говоря математическим языком, основной функцией распределенной системы является отображение отдельных задач во множество узлов, на которых происходит их выполнение [7, с.49]. Распределенная система должна обладать следующими свойствами: [11]

1. Прозрачностью, то есть система должна обеспечить обработку информации вне зависимости от ее местонахождения.

2. Механизмом распределения ресурсов, который должен выполнять следующие функции: обеспечивать взаимодействие процессов и удаленный вызов задач, поддерживать виртуальные каналы, распределенные транзакции и службу имен.

3. Службой имен, единой для всей системы, включая поддержку единой службы директорий.

4. Реализацией служб гомогенных и гетерогенных сетей.

5. Контролем функционирования параллельных процессов.

6. Безопасностью. В распределенных системах проблема безопасности переходит на качественно новый уровень, поскольку приходится контролировать ресурсы и процессы всей системы в целом, а также передачу информации между элементами системы. Основные составляющие защиты остаются теми же - контроль доступа и информационных потоков, контроль трафика сети, аутентификация, операторский контроль и управление защитой. Однако контроль в этом случае усложняется.

Распределенная система обладает рядом преимуществ, не присущих никакой другой организации обработки информации: оптимальностью использования ресурсов, устойчивостью к отказам (выход из строя одного узла не приводит к фатальным последствиям - его легко можно заменить) и т.д. Однако при этом возникают новые проблемы: методика распределения ресурсов, обеспечение безопасности, прозрачности и др. В настоящее время все возможности распределенных систем реализованы далеко не полностью.

В последнее время все большее признание получает концепция обработки информации клиент-сервер. Данная концепция является переходной от централизованной к распределенной и одновременно объединяющей обе последних. Однако клиент-сервер - это не столько способ организации сети, сколько способ логического представления и обработки информации.

Клиент-сервер - это такая организация обработки информации, при которой все выполняемые функции делятся на два класса: внешние и внутренние. Внешние функции состоят из поддержки интерфейса пользователя и функций представления информации на уровне пользователя. Внутренние касаются выполнения различных запросов, процесса обработки информации, сортировки и др.

Сущность концепции клиент-сервер заключается в том, что в системе выделяются элементы двух уровней: серверы, выполняющие обработку данных (внутренние функции), и рабочие станции, выполняющие функции формирования запросов и отображения результатов их обработки (внешние функции). От рабочих станций к серверу идет поток запросов, в обратном направлении - результаты их обработки. Серверов в системе может быть несколько и они могут выполнять различные наборы функций нижнего уровня (серверы печати, файловые и сетевые серверы). Основной объем информации обрабатывается на серверах, которые в этом случае играют роль локальных центров; информация вводится и выводится с помощью рабочих станций.

Отличительные особенности систем, построенных по принципу клиент-сервер, следующие:

- наиболее оптимальное использование ресурсов;

- частичное распределение процесса обработки информации в сети;

- прозрачный доступ к удаленным ресурсам;

- упрощенное управление;

- пониженный трафик;

- возможность более надежной и простой защиты;

- большая гибкость в использовании системы в целом, а также разнородного оборудования и программного обеспечения;

- централизованный доступ к определенным ресурсам,

Отдельные части одной системы могут строится по различным принципам и объединяться с использованием соответствующих согласующих модулей. Каждый класс сетей имеет свои специфические особенности как в плане организации, так и в плане защиты.

## Обеспечение безопасности сетей.

Как уже отмечалось выше, несомненные преимущества обработки информации в сетях ЭВМ оборачиваются немалыми сложностями при организации их защиты. Отметим следующие основные проблемы:

\* Разделение совместно используемых ресурсов.

В силу совместного использования большого количества ресурсов различными пользователями сети, возможно находящимися на большом расстоянии друг от друга, сильно повышается риск НСД - в сети его можно осуществить проще и незаметнее.

\* Расширение зоны контроля.

Администратор или оператор отдельной системы или подсети должен контролировать деятельность пользователей, находящихся вне пределов его досягаемости, возможно, в другой стране. При этом он должен поддерживать рабочий контакт со своими коллегами в других организациях.

\* Комбинация различных программно-аппаратных средств.

Соединение нескольких систем, пусть даже однородных по характеристикам, в сеть увеличивает уязвимость всей системы в целом. Система настроена на выполнение своих специфических требований безопасности, которые могут оказаться несовместимы с требованиями на других системах. В случае соединения разнородных систем риск повышается.

\* Неизвестный периметр.

Легкая расширяемость сетей ведет к тому, что определить границы сети подчас бывает сложно; один и тот же узел может быть доступен для пользователей различных сетей. Более того, для многих из них не всегда можно точно определить сколько пользователей имеют доступ к определенному узлу и кто они.

\* Множество точек атаки.

В сетях один и тот же набор данных или сообщение могут передаваться через несколько промежуточных узлов, каждый из которых является потенциальным источником угрозы. Естественно, это не может способствовать повышению защищенности сети. Кроме того, ко многим современным сетям можно получить доступ с помощью коммутируемых линий связи и модема, что во много раз увеличивает количество возможных точек атаки. Такой способ прост, легко осуществим и трудно контролируем; поэтому он считается одним из наиболее опасных. В списке уязвимых мест сети также фигурируют линии связи и различные виды коммуникационного оборудования: усилители сигнала, ретрансляторы, модемы и т.д.

\* Сложность управления и контроля доступа к системе.

Многие атаки на сеть могут осуществляться без получения физического доступа к определенному узлу - с помощью сети из удаленных точек. В этом случае идентификация нарушителя может оказаться очень сложной, если не невозможной. Кроме того, время атаки может оказаться слишком мало для принятия адекватных мер.

По своей сути проблемы защиты сетей обусловлены двойственным характером последних: об этом мы говорили выше. С одной стороны, сеть есть единая система с едиными правилами обработки информации, а с другой, - совокупность обособленных систем, каждая из которых имеет свои собственные правила обработки информации. В частности, эта двойственность относится и к проблемам защиты. Атака на сеть может осуществляться с двух уровней (возможна их комбинация):

1. Верхнего - злоумышленник использует свойства сети для проникновения на другой узел и выполнения определенных несанкционированных действий. Предпринимаемые меры защиты определяются потенциальными возможностями злоумышленника и надежностью средств защиты отдельных узлов.

2. Нижнего - злоумышленник использует свойства сетевых протоколов для нарушения конфиденциальности или целостности отдельных сообщений или потока в целом. Нарушение потока сообщений может привести к утечке информации и даже потере контроля за сетью. Используемые протоколы должны обеспечивать защиту сообщений и их потока в целом.

Защита сетей, как и защита отдельных систем, преследует три цели: поддержание конфиденциальности передаваемой и обрабатываемой в сети информации, целостности и доступности ресурсов и компонентов сети.

Эти цели определяют действия по организации защиты от нападений с верхнего уровня. Конкретные задачи, встающие при организации защиты сети, обуславливаются возможностями протоколов высокого уровня: чем шире эти возможности, тем больше задач приходится решать. Действительно, если возможности сети ограничиваются пересылкой наборов данных, то основная проблема защиты заключается в предотвращении НСД к наборам данных, доступным для пересылки. Если же возможности сети позволяют организовать удаленный запуск программ, работу в режиме виртуального терминала, то необходимо реализовывать полный комплекс защитных мер.

Как и для АСОИБ, защита сети должна планироваться как единый комплекс мер, охватывающий все особенности обработки информации. В этом смысле организация защиты сети, разработка политики безопасности, ее реализация и управление защитой подчиняются общим правилам, которые были рассмотрены выше. Однако необходимо учитывать, что каждый узел сети должен иметь индивидуальную защиту в зависимости от выполняемых функций и от возможностей сети. При этом защита отдельного узла должна являться частью общей защиты. На каждом отдельном узле необходимо организовать:

- контроль доступа ко всем файлам и другим наборам данных, доступным из локальной сети и других сетей;

- контроль процессов, активизированных с удаленных узлов;

- контроль сетевого графика;

- эффективную идентификацию и аутентификацию пользователей, получающих доступ к данному узлу из сети;

- контроль доступа к ресурсам локального узла, доступным для использования пользователями сети;

- контроль за распространением информации в пределах локальной сети и связанных с нею других сетей.

Однако сеть имеет сложную структуру: для передачи информации с одного узла на другой последняя проходит несколько стадий преобразований. Естественно, все эти преобразования должны вносить свой вклад в защиту передаваемой информации, в противном случае нападения с нижнего уровня могут поставить под угрозу защиту сети. Таким образом, защита сети как единой системы складывается из мер защиты каждого отдельного узла и функций защиты протоколов данной сети.

Необходимость функций защиты протоколов передачи данных опять же обуславливается двойственным характером сети: она представляет собой совокупность обособленных систем, обменивающихся между собой информацией с помощью сообщений. На пути от одной системы к другой эти сообщения преобразуются протоколами всех уровней. А поскольку они являются наиболее уязвимым элементом сети, протоколы должны предусматривать обеспечение их безопасности для поддержки конфиденциальности, целостности и доступности информации, передаваемой в сети.

Сетевое программное обеспечение должно входить в состав сетевого узла, в противном случае возможно нарушение работы сети и ее защиты путем изменения программ или данных. При этом протоколы должны реализовывать требования по обеспечению безопасности передаваемой информации, которые являются частью общей политики безопасности. Ниже приводится классификация угроз, специфических для сетей (угрозы нижнего уровня):

1. Пассивные угрозы (нарушение конфиденциальности данных, циркулирующих в сети) — просмотр и/или запись данных, передаваемых по линиям связи:

- просмотр сообщения - злоумышленник может просматривать содержание сообщения, передаваемого по сети;

- анализ графика - злоумышленник может просматривать заголовки пакетов, циркулирующих в сети и на основе содержащейся в них служебной информации делать заключения об отправителях и получателях пакета и условиях передачи (время отправления, класс сообщения, категория безопасности и т.д.); кроме того, он может выяснить длину сообщения и объем графика.

2. Активные угрозы (нарушение целостности или доступности ресурсов сети) — несанкционированное использование устройств, имеющих доступ к сети для изменения отдельных сообщений или потока сообщений:

- отказ служб передачи сообщений - злоумышленник может уничтожать или задерживать отдельные сообщения или весь поток сообщений;

- «маскарад» — злоумышленник может присвоить своему узлу или ретранслятору чужой идентификатор и получать или отправлять сообщения от чужого имени;

- внедрение сетевых вирусов — передача по сети тела вируса с его последующей активизацией пользователем удаленного или локального узла;

- модификация потока сообщений — злоумышленник может выборочно уничтожать, модифицировать, задерживать, переупорядочивать и дублировать сообщения, а также вставлять поддельные сообщения.

Совершенно очевидно, что любые описанные выше манипуляции с отдельными сообщениями и потоком в целом, могут привести к нарушениям работы сети или утечке конфиденциальной информации. Особенно это касается служебных сообщений, несущих информацию о состоянии сети или отдельных узлов, о происходящих на отдельных узлах событиях (удаленном запуске программ, например) — активные атаки на такие сообщения могут привести к потере контроля за сетью. Поэтому протоколы, формирующие сообщения и ставящие их в поток, должны предпринимать меры для их защиты и неискаженной доставки получателю.

Решаемые протоколами задачи аналогичны задачам, решаемым при защите локальных систем: обеспечение конфиденциальности обрабатываемой и передаваемой в сети информации, целостности и доступности ресурсов (компонентов) сети. Реализация этих функций осуществляется с помощью специальных механизмов. К их числу следует отнести:

- Механизмы шифрования, которые обеспечивают конфиденциальность передаваемых данных и/или информации о потоках данных. Используемый в данном механизме алгоритм шифрования может использовать секретный или открытый ключ. В первом случае предполагается наличие механизмов управления и распределения ключей. Различают два способа шифрования: канальное, реализуемое с помощью протокола канального уровня, и оконечное (абонентское), реализуемое с помощью протокола прикладного или, в некоторых случаях, представительного уровня.

В случае канального шифрования защищается вся передаваемая по каналу связи информация, включая служебную. Этот способ имеет следующие особенности:

- вскрытие ключа шифрования для одного канала не приводит к компрометации информации в других каналах;

- вся передаваемая информация, включая служебные сообщения, служебные поля сообщений с данными, надежно защищена;

- вся информация оказывается открытой на промежуточных узлах -ретрансляторах, шлюзах и т.д.;

- пользователь не принимает участия в выполняемых операциях;

- для каждой пары узлов требуется свой ключ;

- алгоритм шифрования должен быть достаточно стоек и обеспечивать скорость шифрования на уровне пропускной способности канала (иначе возникнет задержка сообщений, которая может привести к блокировке системы или существенному снижению ее производительности);

- предыдущая особенность приводит к необходимости реализации алгоритма шифрования аппаратными средствами, что увеличивает расходы на создание и обслуживание системы.

Оконечное (абонентское) шифрование позволяет обеспечивать конфиденциальность данных, передаваемых между двумя прикладными объектами. Другими словами, отправитель зашифровывает данные, получатель - расшифровывает. Такой способ имеет следующие особенности (сравните с канальным шифрованием):

- защищенным оказывается только содержание сообщения; вся служебная информация остается открытой;

- никто кроме отправителя и получателя восстановить информацию не может (если используемый алгоритм шифрования достаточно стоек);

- маршрут передачи несущественен — в любом канале информация останется защищенной;

- для каждой пары пользователей требуется уникальный ключ;

- пользователь должен знать процедуры шифрования и распределения ключей.

Выбор того или иного способа шифрования или их комбинации зависит от результатов анализа риска. Вопрос стоит следующим образом: что более уязвимо — непосредственно отдельный канал связи или содержание сообщения, передаваемое по различным каналам. Канальное шифрование быстрее (применяются другие, более быстрые, алгоритмы), прозрачно для пользователя, требует меньше ключей. Оконечное шифрование более гибко, может использоваться выборочно, однако требует участия пользователя. В каждом конкретном случае вопрос должен решаться индивидуально.

- Механизмы цифровой подписи, которые включают процедуры закрытия блоков данных и проверки закрытого блока данных. Первый процесс использует секретную ключевую информацию, второй — открытую, не позволяющую восстановить секретные данные. С помощью секретной информации отправитель формирует служебный блок данных (например, на основе односторонней функции), получатель на основе общедоступной информации проверяет принятый блок и определяет подлинность отправителя. Сформировать подлинный блок может только пользователь, имеющий соответствующий ключ.

\* Механизмы контроля доступа.

Осуществляют проверку полномочий сетевого объекта на доступ к ресурсам. Проверка полномочий производится в соответствии с правилами разработанной политики безопасности (избирательной, полномочной или любой другой) и реализующих ее механизмов.

\* Механизмы обеспечения целостности передаваемых данных.

Эти механизмы обеспечивают как целостность отдельного блока или поля данных, так и потока данных. Целостность блока данных обеспечивается передающим и принимающим объектами. Передающий объект добавляет к блоку данных признак, значение которого является функцией от самих данных. Принимающий объект также вычисляет эту функцию и сравнивает ее с полученной. В случае несовпадения выносится решение о нарушении целостности. Обнаружение изменений может повлечь за собой действия по восстановлению данных. В случае умышленного нарушения целостности может быть соответствующим образом изменено и значение контрольного признака (если алгоритм его формирования известен), в этом случае получатель не сможет установить нарушение целостности. Тогда необходимо использовать алгоритм формирования контрольного признака как функцию данных и секретного ключа. В этом случае правильное изменение контрольного признака без знания ключа будет невозможно и получатель сможет установить, подвергались ли данные модификации.

Защита целостности потоков данных (от переупорядочивания, добавления, повторов или удаления сообщений) осуществляется с использованием дополнительных формы нумерации (контроль номеров сообщений в потоке), меток времени и т.д.

Желательными компонентами защиты сети являются следующие механизмы: [8, с.34]

\* Механизмы аутентификации объектов сети.

Для обеспечения аутентификации используются пароли, проверка характеристик объекта, криптографические методы (аналогичные цифровой подписи). Эти механизмы обычно применяются для аутентификации одноуровневых сетевых объектов. Используемые методы могут совмещаться с процедурой «троекратного рукопожатия» (троекратный обмен сообщениями между отправителем и получателем с параметрами аутентификации и подтверждениями).

\* Механизмы заполнения текста.

Используются для обеспечения защиты от анализа графика. В качестве такого механизма может использоваться, например, генерация фиктивных сообщений (богусов); в этом случае трафик имеет постоянную интенсивность во времени.

\* Механизмы управления маршрутом.

Маршруты могут выбираться динамически или быть заранее заданы с тем, чтобы использовать физически безопасные подсети, ретрансляторы, каналы. Оконечные системы при установлении попыток навязывания могут потребовать установления соединения по другому маршруту. Кроме того, может использоваться выборочная маршрутизация (то есть часть маршрута задается отправителем явно - в обход опасных участков).

\* Механизмы освидетельствования.

Характеристики данных, передаваемые между двумя и более объектами (целостность, источник, время, получатель) могут подтверждаться с помощью механизма освидетельствования. Подтверждение обеспечивается третьей стороной (арбитром), которой доверяют все заинтересованные стороны и которая обладает необходимой информацией.

Помимо перечисленных выше механизмов защиты, реализуемых протоколами различных уровней, существует еще два, не относящихся к определенному уровню. Они по своему назначению аналогичны механизмам контроля в локальных системах:

\* Обнаружение и обработка событий (аналог средств контроля опасных событий).

Предназначены для обнаружения событий, которые приводят или могут привести к нарушению политики безопасности сети. Список этих событий соответствует списку для отдельных систем. Кроме того, в него могут быть включены события, свидетельствующие о нарушениях в работе перечисленных выше механизмов защиты. Предпринимаемые в этой ситуации действия могут включать различные процедуры восстановления, регистрацию событий, одностороннее разъединение, местный или периферийный отчет о событии (запись в журнал) и т.д.

\* Отчет о проверке безопасности (аналог проверки с использованием системного журнала).

Проверка безопасности представляет собой независимую проверку системных записей и деятельности на соответствие заданной политике безопасности.

Функции защиты протоколов каждого уровня определяются их назначением:

1. Физический уровень - контроль электромагнитных излучений линий связи и устройств, поддержка коммуникационного оборудования в рабочем состоянии. Защита на данном уровне обеспечивается с помощью экранирующих устройств, генераторов помех, средств физической защиты передающей среды.

2. Канальный уровень - увеличение надежности защиты (при необходимости) с помощью шифрования передаваемых по каналу данных. В этом случае шифруются все передаваемые данные, включая служебную информации.

3. Сетевой уровень - наиболее уязвимый уровень с точки зрения защиты. На нем формируется вся маршрутизирующая информация, отправитель и получатель фигурируют явно, осуществляется управление потоком. Кроме того, протоколами сетевого уровня пакеты обрабатываются на всех маршрутизаторах, шлюзах и др. промежуточных узлах. Почти все специфические сетевые нарушения осуществляются с использованием протоколов данного уровня (чтение, модификация, уничтожение, дублирование, переориентация отдельных сообщений или потока в целом, маскировка под другой узел и др.).

Защита от всех подобных угроз осуществляется протоколами сетевого и транспортного уровней и с помощью средств криптозащиты. На данном уровне может быть реализована, например, выборочная маршрутизация.

4. Транспортный уровень - осуществляет контроль за функциями сетевого уровня на приемном и передающем узлах (на промежуточных узлах протокол транспортного уровня не функционирует). Механизмы транспортного уровня проверяют целостность отдельных пакетов данных, последовательности пакетов, пройденный маршрут, время отправления и доставки, идентификацию и аутентификацию отправителя и получателя и др. функции. Все активные угрозы становятся видимыми на данном уровне.

Гарантом целостности передаваемых данных является криптозащита данных и служебной информации. Никто кроме имеющих секретный ключ получателя и/или отправителя не может прочитать или изменить информацию таким образом, чтобы изменение осталось незамеченным.

Анализ графика предотвращается передачей сообщений, не содержащих информацию, которые, однако, выглядят как настоящие. Регулируя интенсивность этих сообщений в зависимости от объема передаваемой информации можно постоянно добиваться равномерного графика. Однако все эти меры не могут предотвратить угрозу уничтожения, переориентации или задержки сообщения. Единственной защитой от таких нарушений может быть параллельная доставка дубликатов сообщения по другим путям.

5. Протоколы верхних уровней обеспечивают контроль взаимодействия принятой или переданной информации с локальной системой. Протоколы сеансового и представительного уровня функций защиты не выполняют. В функции защиты протокола прикладного уровня входит управление доступом к определенным наборам данных, идентификация и аутентификация определенных пользователей, а также другие функции, определяемые конкретным протоколом. Более сложными эти функции являются в случае реализации полномочной политики безопасности в сети.

# Глава 6. Безопасность электронных платежей.

## Электронные платежи в банке.

В главе 4 были рассмотрены особенности подхода к защите электронных банковских систем. Специфической чертой этих систем является специальная форма обмена электронными данными - электронных платежей, без которых ни один современный банк не может существовать.

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

ОЭД обеспечивает оперативное взаимодействие торговых партнеров (клиентов, поставщиков,торговых посредников и др.) на всех этапах подготовки торговой сделки, заключения контракта и реализации поставки. На этапе оплаты контракта и перевода денежных средств ОЭД может приводить к электронному обмену финансовыми документами. При этом создается эффективная среда для торгово-платежных операций: [3, с.71]

\* Возможно ознакомление торговых партнеров с предложениями товаров и услуг, выбор необходимого товара/услуги, уточнение коммерческих условий (стоимости и сроков поставки, торговых скидок, гарантийных и сервисных обязательств) в реальном масштабе времени;

\* Заказ товара/услуг или запрос контрактного предложения в реальном масштабе времени;

\* Оперативный контроль поставки товара, получение по электронной почте сопроводительных документов (накладных, фактур, комплектующих ведомостей и т.д.);

\* Подтверждение завершения поставки товара/услуги, выставление и оплата счетов;

\* Выполнение банковских кредитных и платежных операций. К достоинствам ОЭД следует отнести:

\* Уменьшение стоимости операций за счет перехода на безбумажную технологию. Эксперты оценивают стоимость обработки и ведения бумажной документации в 3-8% от общей стоимости коммерческих операций и доставки товаров. Выигрыш от применения ОЭД оценивается, например, в автомобильной промышленности США более чем в $200 на один изготовленный автомобиль [14];

\* Повышение скорости расчета и оборота денег;

\* Повышение удобства расчетов.

Существует две ключевые стратегии развития ОЭД:

1. ОЭД используется как преимущество в конкурентной борьбе, позволяющее осуществлять более тесное взаимодействие с партнерами. Такая стратегия принята в крупных организациях и получила название «Подхода Расширенного Предприятия» (Extended Enterprise) [2, с.230].

2. ОЭД используется в некоторых специфических индустриальных проектах или в инициативах объединений коммерческих и других организаций для повышения эффективности их взаимодействия.

Банки в США и Западной Европе уже осознали свою ключевую роль в распространении ОЭД и поняли те значительные преимущества, которые дает более тесное взаимодействие с деловыми и личными партнерами. ОЭД помогает банкам в предоставлении услуг клиентам, особенно мелким, тем, которые ранее не могли позволить себе ими воспользоваться из-за их высокой стоимости.

Основным препятствием широкому распространению ОЭД является многообразие представлений документов при обмене ими по каналам связи. Для преодоления этого препятствия различными организациями были разработаны стандарты представления документов в системах ОЭД для различных отраслей деятельности: [2, с.234]

QDTI - General Trade Interchange (Европа, международная торговля);

МДСНД - National Automated Clearing House Association (США, Национальная ассоциация автоматизированных расчетных палат);

TDCC - Transportation Data Coordinating Committee (Координационный комитет по данным перевозок);

VICS - Voluntary Interindustry Communication Standart (США, Добровольный межотраслевой коммуникационный стандарт);

WINS - Warehouse Information Network Standarts (Стандарты информационной сети товарных складов).

В октябре 1993 года международная группа UN/ECE опубликовала первую версию стандарта EDIFACT. Разработанный набор синтаксических правил и коммерческих элементов данных был оформлен в виде двух стандартов ISO [2, с.241]:

ISO 7372 - Trade Data Element Directory (Справочник коммерческих элементов данных);

ISO 9735 - EDIFACT - Application level syntax rules (Синтаксические правила прикладного уровня).

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

Суть концепции электронных платежей заключается в том, что пересылаемые по линиям связи сообщения, должным образом оформленные и переданные, являются основанием для выполнения одной или нескольких банковских операций. Никаких бумажных документов для выполнения этих операций в принципе не требуется (хотя они могут быть выданы). Другими словами, пересылаемое по линиям связи сообщение несет информацию о том, что отправитель выполнил некоторые операции над своим счетом, в частности над корреспондентским счетом банка-получателя (в роли которого может выступать клиринговый центр), и что получатель должен выполнить определенные в сообщении операции. На основании такого сообщения можно переслать или получить деньги, открыть кредит, оплатить покупку или услугу и выполнить любую другую банковскую операцию. Такие сообщения называются электронными деньгами, а выполнение банковских операций на основании посылки или получения таких сообщений - электронными платежами. Естественно, весь процесс осуществления электронных платежей нуждается в надежной защите. Иначе банк и его клиентов ожидают серьезные неприятности.

Электронные платежи применяются при межбанковских, торговых и персональных расчетах.

Межбанковские и торговые расчеты производятся между организациями (юридическими лицами), поэтому их иногда называют корпоративными. Расчеты с участием физических лиц-клиентов получили название персональных.

Большинство крупных хищений в банковских системах прямо или косвенно связано именно с системами электронных платежей.

На пути создания систем электронных платежей, особенно глобальных, охватывающих большое число финансовых институтов и их клиентов в различных странах, встречается множество препятствий. Основными из них являются:

1. Отсутствие единых стандартов на операции и услуги, что существенно затрудняет создание объединенных банковских систем. Каждый крупный банк стремится создать свою сеть ОЭД, что увеличивает расходы на ее эксплуатацию и содержание. Дублирующие друг друга системы затрудняют пользование ими, создавая взаимные помехи и ограничивая возможности клиентов.

2. Возрастание мобильности денежных масс, что ведет к увеличению возможности финансовых спекуляций, расширяет потоки «блуждающих капиталов». Эти деньги способны за короткое время менять ситуацию на рынке, дестабилизировать ее.

3. Сбои и отказы технических и ошибки программных средств при осуществлении финансовых расчетов, что может привести к серьезным осложнениям для дальнейших расчетов и потере доверия к банку со стороны клиентов, особенно в силу тесного переплетения банковских связей (своего рода «размножение ошибки»). При этом существенно возрастает роль и ответственность операторов и администрации системы, которые непосредственно управляют обработкой информации.

Любая организация, которая хочет стать клиентом какой-либо системы электронных платежей, либо организовать собственную систему, должна отдавать себе в этом отчет.

Для надежной работы система электронных платежей должна быть хорошо защищена.

Торговые расчеты производятся между различными торговыми организациями. Банки в этих расчетах участвуют как посредники при перечислении денег со счета организации-плательщика на счет организации-получателя.

Торговые расчеты чрезвычайно важны для общего успеха программы электронных платежей. Объем финансовых операций различных компаний обычно составляет значительную часть общего объема операций банка.

Виды торговых расчетов сильно различаются для разных организаций, но всегда при их осуществлении обрабатывается два типа информации: платежных сообщений и вспомогательная (статистика, сводки, уведомления). Для финансовых организаций наибольший интерес представляет, конечно, информация платежных сообщений - номера счетов, суммы, баланс и т.д. Для торговых организаций оба вида сведений одинаково важны - первый дает ключ к финансовому состоянию, второй - помогает при принятии решений и выработке политики.

Чаще всего распространены торговые расчеты следующих двух видов: [16]

\* Прямой депозит (direct deposit).

Смысл этого вида расчетов заключается в том, что организация поручает банку осуществлять некоторые виды платежей своих служащих или клиентов автоматически, с помощью заранее подготовленных магнитных носителей или специальных сообщений. Условия осуществления таких расчетов оговариваются заранее (источник финансирования, сумма и т.д.). Они используются в основном для регулярных платежей (выплаты различного рода страховок, погашение кредитов, зарплата и т.д.). В организационном плане прямой депозит более удобен, чем, например, платежи с помощью чеков.

С 1989 г. число служащих, использующих прямой депозит, удвоилось и составило 25% от общего количества. Более 7 млн. американцев получают сегодня заработную плату в виде прямого депозита. Банкам прямой депозит сулит следующие выгоды:

- уменьшение объема задач, связанных с обработкой бумажных документов и, как следствие, экономия значительных сумм;

- увеличение числа депозитов, так как 100% объема платежей должны быть внесены на депозит.

Кроме банков в выигрыше остаются и хозяева, и работники; повышаются удобства и уменьшаются затраты.

\* Расчеты при помощи ОЭД.

В качестве данных здесь выступают накладные, фактуры, комплектующие ведомости и т.д.

Для осуществления ОЭД необходима реализация следующего набора основных услуг :

- электронная почта по стандарту Х.400 ;

- передача файлов;

- связь «точка-точка»;

- доступ к базам данных в режиме on-line;

- почтовый ящик;

- преобразование стандартов представления информации.

Примерами существующих в настоящее время систем торговых расчетов с использованием ОЭД могут служить:

- National Bank и Royal Bank (Канада) связаны со своими клиентами и партнерами с помощью IBM Information Network;

- Bank of Scotland Transcontinental Automated Payment Service (TAPS), основанная в 1986 г., связывает Bank of Scotland с клиентами и партнерами в 15 странах с помощью корреспондентских банков и автоматизированных клиринговых палат.

Электронные межбанковские расчеты бывают в основном двух видов:

\* Клиринговые расчеты с использованием мощной вычислительной системы банка-посредника (клирингового банка) и корреспондентских счетов банков-участников расчетов в этом банке. Система основана на зачете взаимных денежных требований и обязательств юридических лиц с последующим переводом сальдо. Клиринг также широко используется на фондовых и товарных биржах, где зачет взаимных требований участников сделок проводится через клиринговую палату или особую электронную клиринговую систему.

Межбанковские клиринговые расчеты осуществляются через специальные клиринговые палаты, коммерческие банки, между отделениями и филиалами одного банка - через головную контору. В ряде стран функции клиринговых палат выполняют центральные банки. Автоматизированные клиринговые палаты (АКП) предоставляют услуги по обмену средствами между финансовыми учреждениями. Платежные операции в основном сводятся либо к дебетованию, либо к кредитованию. Членами системы АКП являются финансовые учреждения, которые состоят в ассоциации АКП. Ассоциация образуется для того, чтобы разрабатывать правила, процедуры и стандарты выполнения электронных платежей в пределах географического региона. Необходимо отметить, что АКП не что иное, как механизм для перемещения денежных средств и сопроводительной информации. Сами по себе они не выполняют платежных услуг. АКП были созданы в дополнение к системам обработки бумажных финансовых документов. Первая АКП появилась в Калифорнии в 1972 г., в настоящее время в США функционируют 48 АКП. В 1978 г. была создана Национальная Ассоциация АКП (National Automated Clearing House Association; NACHA), объединяющая все 48 сети АКП на кооперативных началах. [2, с.289]

Объем и характер операций постоянно расширяются. АКП начинают выполнять деловые расчеты и операции обмена электронными данными. После трехлетних усилий различных банков и компаний была создана система СТР (Corporate Trade Payment), предназначенная для автоматизированной обработки кредитов и дебетов. По мнению специалистов в ближайшее время тенденция расширения функций АКП будет сохраняться.

\* Прямые расчеты, при которых два банка осуществляют связь непосредственно между собой с помощью счетов "лоро-ностро", возможно, при участии третьего лица, играющего организационную или вспомогательную роль. Естественно, объем взаимных операций должен быть достаточно велик для оправдания затрат на организацию такой системы расчетов. Обычно такая система объединяет несколько банков, при этом каждая пара может связываться непосредственно между собой, минуя посредников. Однако в этом случае возникает необходимость управляющего центра, занимающегося защитой взаимодействующих банков (рассылкой ключей, управлением, контролем функционирования и регистрацией событий).

В мире существует достаточно много таких систем - от небольших, связывающих несколько банков или филиалов, до гигантских международных, связывающих тысячи участников. Наиболее известной системой этого класса является SWIFT.

В последнее время появился третий вид электронных платежей - обработка электронных чеков (electronic check truncation), суть которого состоит в прекращении пути пересылки бумажного чека в финансовой организации, в которой он был предъявлен. В случае необходимости дальше «путешествует» его электронный аналог в виде специального сообщения. Пересылка и погашение электронного чека осуществляются с помощью АКП. [2, с.291]

В 1990 г. NACHA анонсировала первый этап тестирования национальной экспериментальной программы «Electronic Check Truncation». Ее целью является сокращение расходов на обработку огромного количества бумажных чеков.

Пересылка денег с помощью системы электронных платежей включает следующие этапы (в зависимости от конкретных условий и самой системы порядок может меняться):

1. Определенный счет в системе первого банка уменьшается на требуемую сумму.

2. Корреспондентский счет второго банка в первом увеличивается на ту же сумму.

3. От первого банка второму посылается сообщение, содержащее информацию о выполняемых действиях (идентификаторы счетов, сумма, дата, условия и т.д.); при этом пересылаемое сообщение должно быть соответствующим образом защищено от подделки: зашифровано, снабжено цифровой подписью и контрольными полями и т.д.

4. С корреспондентского счета первого банка во втором списывается требуемая сумма.

5. Определенный счет во втором банке увеличивается на требуемую сумму.

6. Второй банк посылает первому уведомление о произведенных корректировках счета; это сообщение также должно быть защищено от подделки способом, аналогичным защите платежного сообщения.

7. Протокол обмена фиксируется у обоих абонентов и, возможно, у третьего лица (в центре управления сетью) для предотвращения конфликтов.

На пути передачи сообщений могут быть посредники - клиринговые центры, банки-посредники в передаче информации и т.п. Основная сложность таких расчетов - уверенность в своем партнере, то есть каждый из абонентов должен быть уверен, что его корреспондент выполнит все необходимые действия.

Для расширения применения электронных платежей проводится стандартизация электронного представления финансовых документов. Она была начата в 70-х годах в рамках двух организаций [2, с. 298]:

1) ANSI (American National Standart Institute) опубликовал документ ANSI X9.2-1080, (Interchange Message Specification for Debit and Credit Card Message Exchange Among Financial Institute, Спецификация обменных сообщений для дебетных и кредитных карточек обмена между финансовыми организациями). В 1988 аналогичный стандарт был принят ISO и получил название ISO 8583 (Bank Card Originated Messages Interchange Message Specifications - Content for Financial Transactions);

2) SWIFT (Society for Worldwide Interbank Financial Telecommunications) разработало серию стандартов межбанковских сообщений.

В соответствии со стандартом ISO 8583 финансовый документ содержит ряд элементов данных (реквизитов), расположенных в определенных полях сообщения или электронного документа (электронной кредитной карточки, сообщения в формате Х.400 или документа в синтаксисе EDIFACT). Каждому элементу данных (ЭД) назначается свой уникальный номер. Элемент данных может быть как обязательным (то есть входить в каждое сообщение данного вида), так и необязательным (в некоторых сообщениях может отсутствовать).

Битовая шкала определяет состав сообщения (те ЭД, которые в нем присутствуют). Если некоторый разряд битовой шкалы установлен в единицу, это означает, что соответствующий ЭД присутствует в сообщении. Благодаря такому методу кодирования сообщений уменьшается общая длина сообщения, достигается гибкость в представлении сообщений со многими ЭД, обеспечивается возможность включения новых ЭД и типов сообщений в электронный документ стандартной структуры. [2, с. 299]

Существует несколько способов электронных межбанковских платежей. Рассмотрим два из них: оплата чеком (оплата после услуги) и оплата аккредитивом (оплата ожидаемой услуги). Другие способы, как например оплата с помощью платежных требований или платежных поручений, имеют сходную организацию.

Оплата чеком основана на бумажном или другом документе, содержащим идентификацию подателя. Этот документ является основанием для перевода определенной в чеке суммы со счета владельца на счет подателя. Платеж чеком включает следующие этапы :

- получение чека;

- представление чека в банк;

- запрос о переводе со счета владельца чека на счет подателя;

- перевод денег;

- уведомление о платеже.

Основными недостатками таких платежей являются необходимость существования вспомогательного документа (чека), который легко подделать, а также значительные затраты времени на выполнение платежа (до нескольких дней).

Поэтому в последнее время более распространен такой вид платежей как оплата аккредитивом. Он включает следующие этапы:

- уведомление банка клиентом о предоставлении кредита;

- уведомление банка получателя о предоставлении кредита и перевод денег;

- уведомление получателя о получении кредита.

Такая система позволяет осуществлять платежи в очень короткие сроки. Уведомление о предоставлении кредита можно направлять по (электронной) почте, на дискетах, магнитных лентах.

Каждый из рассмотренных выше видов платежей имеет свои преимущества и свои недостатки. Чеки наиболее удобны при оплате незначительных сумм, а также при нерегулярных платежах. В этих случаях задержка платежа не очень существенна, а использование кредита нецелесообразно. Расчеты с помощью аккредитива обычно используются при регулярной оплате и для значительных сумм. В этих случаях отсутствие клиринговой задержки позволяет экономить много времени и средств за счет уменьшения периода оборота денег. Общим недостатком этих двух способов является необходимость затрат на организацию надежной системы электронных платежей. [2, с. 300]

## Вопросы безопасности электронных платежей.

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

- подготовка документа к отправке;

- передача документа по каналу связи;

- прием документа и его обратное преобразование.

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

1. Пересылка платежных и других сообщений между банками или между банком и клиентом;

2. Обработка информации внутри организаций отправителя и получателя;

3. Доступ клиента к средствам, аккумулированным на счете.

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

- внутренние системы организаций Получателя и Отправителя должны быть приспособлены к получению/отправке электронных документов и обеспечивать необходимую защиту при их обработке внутри организации (защита оконечных систем);

- взаимодействие Получателя и Отправителя документа осуществляется опосредованно - через канал связи. Это порождает три типа проблем: 1) взаимного опознавания абонентов (проблема установления аутентификации при установлении соединения); 2) защиты документов, передаваемых по каналам связи (обеспечение целостности и конфиденциальности документов); 3) защиты самого процесса обмена документами (проблема доказательства отправления/доставки документа);

- в общем случае Отправитель и Получатель документа принадлежат к различным организациям и друг от друга независимы. Этот факт порождает проблему недоверия - будут ли предприняты необходимые меры по данному документу (обеспечение исполнения документа).

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

- обеспечить защиту от случайных и умышленных ошибок;

- обеспечить адаптацию к частым изменениям количества пользователей, типов оборудования, способов доступа, объемов трафика, топологии;

- поддерживать различные типы аппаратного и программного обеспечения, поставляемого различными производителями;

- осуществлять управление и поддержку сети для обеспечения непрерывности работы и быстрой диагностики нарушений;

- реализовывать полный спектр прикладных задач ОЭД, включая электронную почту;

- реализовывать максимально возможное число требований партнеров;

- включать службы резервного копирования и восстановления после аварий.

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

- равноправная аутентификацию абонентов;

- невозможность отказа от авторства сообщения/приема сообщения;

- контроль целостности сообщения;

- обеспечение конфиденциальности сообщения;

- управление доступом на оконечных системах;

- гарантии доставки сообщения;

- невозможность отказа or принятия мер по сообщению;

- регистрация последовательности сообщений;

- контроль целостности последовательности сообщений;

- обеспечение конфиденциальности потока сообщений.

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

- скрыть содержание документа от посторонних лиц (обеспечение конфиденциальности документа) путем шифрования его содержимого;

- обеспечить совместное использование документа группой пользователей системы ОЭД путем криптографического разделения информации и соответствующего протокола распределения ключей. При этом для лиц, не входящих в группу, документ недоступен;

- своевременно обнаружить искажение, подделку документа (обеспечение целостности документа) путем введения криптографического контрольного признака (имитовставки);

- удостовериться в том, что абонент, с которым происходит взаимодействие в сети является именно тем, за кого он себя выдает (аутентификация абонента/источника данных).

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

Надежность всей криптосистемы в целом во многом зависит от механизмов рассылки (распределения) ключей между участниками взаимодействия. Проблема рассылки ключей в настоящее время не имеет общих решений. В каждом конкретном случае она должна решаться с учетом особенностей функционирования всей защищаемой АСОИБ. Существует много различных подходов к решению этой проблемы. Не вдаваясь в тонкости каждого из них, поскольку это выходит далеко за рамки обсуждаемого предмета, кратко опишем основные: [2, с.305]

\* Метод базовых/сеансовых ключей.

Суть метода состоит в том, что вводится иерархия ключей (главный ключ (ГК)/ключ шифрования ключей (КК)/ключ шифрования данных (КД).

Иерархия может быть двухуровневой (КК/КД) или трехуровневой (ГК/КК/КД). При этом старший ключ в иерархии распространяется между участниками взаимодействия неэлектронным образом, исключающем его перехват и/или компрометацию. Стандарт определяет три способа распространения ключей: непосредственная передача, передача с использованием центра распространения и передача с использованием центра трансляции ключей. Стандарт не применяется для распространения ключей между специализированными банковскими устройствами, такими как банкоматы и устройства расчета в точке продажи;

\* Метод открытых ключей. Основан на односторонних преобразованиях, при которых часть ключа остается открытой и может быть передана по линиям связи в открытом виде. Это избавляет от дорогостоящей процедуры распространения ключей шифрования неэлектронным способом;

\* Метод выведенного ключа, применяется для защиты информации, передаваемой между терминалом системы расчета в точке продажи и компьютером банка. При этом методе ключ для шифрования каждой следующей транзакции вычисляется путем одностороннего преобразования предыдущего ключа и параметров транзакции;

\* Метод ключа транзакции. Также применяется для защиты информации, передаваемой между терминалом системы расчета в точке продажи и компьютером банка. Он отличается от метода выведенного ключа тем, что при вычислении ключа для следующей транзакции не используются ее параметры.

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

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

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

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

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

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

В настоящее время в мире существует большое количество систем электронных платежей. Наиболее известные из них: [2, с.312]

- S.W.I.F.T. (The Society for Worldwide Inter-bank Financial Telecommunication) - бесприбыльное кооперативное международное сообщество, целью которого является организация межбанковских расчетов по всему миру.

- FedWire - самая крупная система американских межбанковских коммуникаций, соединяющая головные конторы округа Federal Reserve, ветви банков Federal Reserve и более 500 других банков с помощью центра коммутации в Вирджинии.

- CHAPS (Clearing Houses Automated Payment System) - система поддержки электронных платежей между сравнительно небольшой (около 300) группой банков Лондона, большинство из которых отделения иностранных банков, использующих Лондон в качестве расчетного центра.

- CHIPS (Clearing Houses Interbank Payment System) - клиринговая система США, организованная Нью-йоркской ассоциацией клиринговых палат (New York Clearing House Association - NYCHA) (см. [1]).

Рассмотрим подробнее организацию некоторых из этих систем, уделив особое внимание рассмотрению вопросов обеспечению их безопасности.

Система SWIFT.

Сообщество SWIFT было организовано в 1973 году и в 1977 г. начали осуществляться первые операции с использованием сетей связи. Члены сообщества находятся в Южной, Центральной и Северной Америке, Европе, Африке, Австралии и на Дальнем Востоке.

Система SWIFT позволяет пользователям получить следующие преимущества :

- повышение эффективности работы банков за счет стандартизации и современных способов передачи информации, способствующих развитию автоматизации и рационализации банковских процессов;

- надежный обмен платежными сообщениями;

- сокращение операционных расходов по сравнению с телексной связью;

- удобный прямой доступ пользователей SWIFT к своим корреспондентам по всему миру (доставка сообщения с обычным приоритетом в любую точку мира - 20 минут, доставка срочного сообщения - 30 секунд);

- использование стандартизованных сообщений SWIFT, позволяющее преодолеть языковые барьеры и свести к минимуму различия в практике осуществления банковских операций;

- повышение конкурентоспособности банков-членов SWIFT за счет того, что международный и кредитный оборот все более концентрируется на пользователях SWIFT.

Стоимость передачи сообщений членами сообщества определяется по единому тарифу и зависит от количества соединений, адреса, объема сообщения. За счет высокой интенсивности графика (более 5 млн. сообщений в день) стоимость передачи одного сообщения оказывается ниже, чем в других средствах связи (телекс, телеграф). Дополнительно к основной функции (обмену сообщениями) система SWIFT также выполняет роль форума для выработки соглашения о стандартах представления и передачи данных.

Существует две системы SWIFT: SWIFT I (введена в строй в 1977 году) и SWIFT II (внедрена с 1990 года). Хотя по архитектуре эти системы различны, пользователь не отличает сообщений, полученных по SWIFT I или SWIFT II. Ниже мы рассмотрим архитектуру и защиту системы SWIFT II.

В архитектуре SWIFT II можно выделить четыре основные уровне иерархии: [7, с.141]

- банковский терминал, который устанавливается в банке и предназначен для доступа персонала банка в сеть. Терминалами системы SWIFT обычно являются персональные компьютеры. Смонтированное оборудование может сдаваться «под ключ» (на базе миниЭВМ компаний Unisys и NCR) или интегрироваться в существующую банковскую систему (например на базе семейство миниЭВМ VAX компании DEC);

- региональный процессор (РП), основным назначением которого является организация взаимодействия пользователей некоторой ограниченной области (республики, страны, группы стран). Места расположения РП заранее не определяются. Как правило, РП оснащаются сдублированными ЭВМ фирмы Unisys;

- слайс-процессор (СП), необходимый для обмена сообщениями между подключенными к нему РП, краткосрочного или длительного архивирования сообщений и генерации системных отчетов. Система SWIFT может сохранять передаваемые сообщения на срок до 14 дней. Это помогает избегать проблем, связанных с трактовкой текстов сообщений. На сегодняшний день существует три СП, каждый из них которых оснащен тремя машинами А12 фирмы Unisys, одна из которой является резервной. Один СП может обработать до 3.5 миллионов сообщений в день. Допускается включение в сеть дополнительных СП;

- процессор управления системой (ПУС), выполняющий функции монитора системы, управления системой и сетью. Существует два ПУС, один из которых находится в Голландии, а второй в США. Каждый ПУС может контролировать состояние и управлять работой СП и РП, работой сетевых программ и оборудования, подключением пользователей и их рабочими сеансами, включая выбираемые пользователем прикладные задачи. ПУС единственный уровень системы, который не занят обработкой сообщений, а предназначен исключительно для управления системой SWIFT в целом.

Сообщения системы SWIFT содержат поля, идентифицирующие всех участников передачи информации и платежей.

Банк заказчика операции информирует банк-отправитель о необходимости послать сообщение и переводит ему соответствующую сумму. Банк получателя при приеме сообщения переводит эту сумму на счет расчетного банка, который осуществляет платежи.

Расчеты между банком-отправителем и банком-получателем осуществляются с помощью счета, который открывается в одном из них для другого. Кто для кого открывает счет, зависит от типа валюты, в которой производятся расчеты. Если платежи осуществляются в валюте государства, в котором находится банк-получатель, то он вносит соответствующую сумму в дебет счета банка-отправителя в своем банке. Наоборот, если платежи осуществляются в валюте государства, в котором находится банк-отправитель, то он открывает у себя счет банка получателя и предоставляет ему кредит на соответствующую сумму.

Безопасность в системе SWIFT обеспечивается применением организационных, программных и технических мер.

В системе SWIFT существует строгое разделение ответственности за поддержание безопасности системы. Так банк, подключенный к системе, отвечает за правильную эксплуатацию и физическую защиту терминалов, модемов и линий связи до регионального процессора, за правильное оформление сообщения при передаче его в сеть и наличие работоспособных терминалов. Всю остальную ответственность за передачу сообщений несет администрация системы. Управление защитой осуществляется управлением Главного инспектора. Контроль защищенности системы осуществляется через случайные промежутки времени, чтобы убедиться, что все требования к: безопасности выполняются должным образом.

Защита банковских терминалов предусматривает разграничение доступа пользователей к нему по паролю и специальной пластиковой карточке. При входе пользователя в систему производится взаимное опознавание терминала и системы. Автоматическое отключение от SWIFT происходит в следующих случаях:

- при обнаружении помехи или обрыве соединения;

- при неоднократном обнаружении ошибки при передаче данных или в принятом сообщении;

- при сбое РП, к которому подсоединены терминалы.

Сведения о подключении и отключении терминала регистрируются в специальном журнале.

Для обеспечения конфиденциальности передаваемых сообщений используется шифрование при помощи специальных устройств, устанавливаемых в тракте передачи «банковский терминал - региональный процессор». Для шифрования информации используются три типа ключей: главный (64 бита), вторичный (128 бит) и шифрования данных (64 бита). Главный и вторичный ключи устанавливаются представителями SWIFT. Ключ шифрования данных генерируется специальным шумовым источником в процессе работы. Смена модулей, содержащих первичный и вторичный ключи, осуществляется периодически по указанию Главного инспектора системы. Банкам предоставляется возможность устанавливать собственные устройства шифрования для защиты линии связи (естественно после консультаций с представителями SWIFT). Обеспечение конфиденциальности сообщений не является самой главной задачей системы, хотя этому также уделяется серьезное внимание.

Для аутентификации пользователей и обеспечения целостности сообщений в системе SWIFT существует оригинальный алгоритм аутентификации, детали которого держатся в секрете. Как и для любого такого алгоритма, базовыми требованиями являются надежное распределение ключей между двумя абонентами и защита их от остальных. Надежная аутентификация достигается за счет четкого распределения ответственности. Ключи рассылаются банкам попарно, другие банки и персонал сети доступа к ним не имеют; рассылается также руководство по управлению ключами: процедура и время замены ключей и т.д. Кроме того, SWIFT может использоваться для обмена конфиденциальной информацией между кооперацией банков, однако, в этом случае ответственность за обеспечение безопасности ложится на участников обмена.

В то же время аутентификации взаимодействующих организаций недостаточно для надежной работы сети, так как она не предполагает защиты от подмены, уничтожения или задержки сообщений.

Для обеспечения целостности потока передаваемых сообщений применяется механизм номеров сообщений. Соединения между SWIFT и пользователями поддерживаются двумя (входной и выходной) последовательностями номеров. Входная последовательность обрабатывается слайс-процессорами системы, выходная - получателями сообщений. Такой механизм обеспечивает полный контроль за последовательностью переданных и полученных сообщений для любой пары оконечных пользователей. Он удостоверяет, что ни одно сообщение не уничтожено и не продублировано.

Еще одна задача защиты - предотвращение передачи ложных сообщений, не искажающих последовательности номеров и имеющих истинную аутентификацию. Эта задача решается банками - оконечными пользователями системы. Именно они ответственны за корректность переданных от их имени сообщений. Кроме того, на пунктах обработки и передачи сообщений также существуют механизмы защиты от подделки сообщений.

Для центральной части SWIFT, состоящей из слайс-процессоров, региональных процессоров и линий связи, защита сообщений является задачей администрации системы. Доступ к системе, программное обеспечение и сообщения пользователей строго контролируются, как и доступ на территорию машинных залов. Международные линии связи, соединяющие слайс-процессоры между собой, слайс-процессоры и региональные процессоры, имеют надежную криптозащиту. Персонал системы SWIFT не имеет доступа к содержимому пересылаемых сообщений. [2, с.356]

В реализации защиты SWIFT отражены основные подходы, которые применяются при организации системы электронных платежей в целом.

# Глава 7. Безопасность персональных платежей физических лиц.

## Основные формы удаленного банковского обслуживания физических лиц.

Выделяют три вида персональных платежей:

- домашнее (телефонное) обслуживание,

- расчет с автоматическим кассовым аппаратом (банкоматом),

- расчет в точке продажи.

В настоящее время появился четвертый вид — финансовый сервис с использованием всемирной сети Интернет.

Домашнее банковское обслуживание позволяет клиентам получить доступ к банковским и информационным услугам не выходя из дома.

Достоинства этого вида обслуживания:

- для клиента - большая доступность данных и управление своими финансовыми делами;

- для банка - уменьшение стоимости обслуживания.

Ввод данных для платежа при голосовой связи (идентификатор, номер счета, размер платежа) производится клиентом либо с клавиатуры телефона либо голосом (что менее надежно с точки зрения безопасности, но более технически доступно).

Системы домашнего (телефонного) обслуживания начали внедряться банками с начала 80-годов, однако, до настоящего времени широкого распространения не получили.

Этот вид обслуживания в разных странах находится на различном уровне. Например, в США домашнее обслуживание не приняло больших масштабов в то время как во Франции около 3.5 млн. домов подключено к сети MiniTel.

Некоторое распространение получило телефонное обслуживание и в Великобритании. Основным банком, обеспечивающим эти услуги является там Trustee Savings Banks. Его система SpeedLink в настоящее время обслуживает более 250.000 клиентов, не имеющих специального оборудования, за исключением современного телефона. [12]

Для получения доступа к услугам SpeedLink клиенту необходимо соединиться с ним и назвать свой номер счета и свой идентификатор (PIN SpeedLine) для подтверждения личности. После установления связи клиенты SpeedLink могут получить уведомление на факс-аппарат или по почте (если факс отсутствует). Система предоставляет также такие услуги как оплата счетов, передача денег, ознакомление с последними шестью транзакциями, перевод денег. Соотношение персональных и корпоративных клиентов этой системы находится в отношении 2:1.

First Direct - полная система телефонного обслуживания клиентов на дому. Она введена в действие Midland Bank Group в 1989 году.

Основное ее отличие в том, что она не использует синтезируемый голос или персональный компьютер для проведения расчетов.

Проведенные после установки First Direct исследования показали, что 30% населения посещают банки для того, чтобы использовать банкоматы, а 30% пользуются телефоном.

В системе First Direct особое внимание уделяется начальной идентификации и проверке абонента. Для идентификации используется десятисимвольный пароль, устанавливаемый клиентом и известный только ему. Проверка абонента осуществляется при взаимодействии с оператором. В начале работы оператор запрашивает наугад одну или несколько букв из пароля пользователя. Дополнительно клиент снабжается кодовым словом, которое используется при этой процедуре. Детали процедуры идентификации и аутентификации системы First Direct держатся в секрете.

Будущее этого вида услуг сильно зависит от прогресса в области распознавания речи и создания надежных и сравнительно недорогих устройств с приемлемыми характеристиками такого распознавания. [12]

Банковский автомат-кассир (АКА, банкомат) - специализированное устройство, предназначенное для обслуживания клиента в отсутствие банковского персонала. Это наиболее существенная часть банковской системы, предназначенная, в основном, для выдачи наличных денег. Помимо этой функции АКА может выполнять ряд дополнительных, а числе которых:

\* проверка состояния счета клиента;

\* изменение параметров счета клиента;

\* осуществление различных платежей;

\* предоставление информации о:

- страховом полисе клиента;

- котировках ценных бумаг на фондовом рынке;

- покупке и продаже акций;

- обменных курсах валют и т.д.

Автоматический кассовый аппарат состоит из трех устройств ввода (считыватель с пластиковых карточек, цифровая и функциональная клавиатура), двух выходных устройств (микродисплей и принтер) и устройства обработки информации. Взаимодействие клиента с АКА осуществляется при помощи пластиковой карточки, на которой записана необходимая информация, выносной клавиатуры и микродисплея.

В настоящее время устройства обработки информации АКА разрабатываются на основе микропроцессоров. Так, например основой АКА компании NCR являются процессоры Intel 80486 и Pentium. Фактически АКА компании NCR представляет собой персональную ЭВМ, работающую под управлением ОС OS/2 и имеющую до 64 Мбайт оперативной памяти, до 3200 Мбайт дисковой памяти, накопитель на гибких магнитных дисках, дисплей, принтер и другие периферийные устройства. Выполнение операций осуществляется с помощью прикладного программного обеспечения. Шифрование конфиденциальной информации при передаче по каналам связи или при записи на диск осуществляется на основе стандарта DES. Кроме крипто-защиты предусмотрены и другие меры безопасности.

В 90-х годах по данным Американской Ассоциации Банкиров в США услуги АКА использовались половиной национальных банков и всеми крупными банками. [2, с.377].

Системы, обеспечивающие расчеты продавца и покупателя в точке продажи, (point-of-sale, POS) получили распространение в США более 25 лет назад. В основном, все терминалы, подключенные к этим системам размещены на предприятиях торговли. Большинство таких терминалов установлены в супермаркетах, так как там совершается большое количество покупок в течении дня, а также в других магазинах и на автозаправочных станциях.

Системы POS обеспечивают следующие услуги:

- проверку и подтверждение чеков;

- проверку и обслуживание дебетовых и кредитных карточек;

- использование системы электронных расчетов.

Банки, финансирующие систему расчетов в точке продажи, таким образом расширяют список своих клиентов путем предоставления им больших удобств для покупок в магазинах с использованием удаленных устройств. Торговля, в свою очередь, увеличивает количество клиентов, расширяет управление имуществом, сохраняет время клиентов и уменьшает риск потери наличных денег.

Существует два типа систем POS. Основной из них предполагает, что продавец и покупатель имеют счета в одном и том же банке. Данные, необходимые для платежа, передаются через терминалы системы POS банковскому компьютеру, производится платеж и деньги переводятся со счета покупателя на счет продавца. В более сложной системе участвуют два или более банков. При платеже сначала вызывается банк покупателя, производится платеж и записывается на магнитную ленту для передачи в расчетную палату. Расчетная палата в свою очередь пересылает данные о платеже в банк продавца, который кредитует платеж.

## Проблемы идентификации клиента при удаленном обслуживании.

Персональный номер (идентификатор) (Personal Identification Number, PIN) - это последовательность цифр, используемая для идентификации клиента. Для ввода PIN как в АКА, так и в терминалах систем POS предусмотрена цифровая клавиатура, аналогичная телефонной. По способу назначения можно выделить следующие типы PIN:

- назначаемые выведенные PIN;

- назначаемые случайные PIN;

- PIN, выбираемые пользователем.

Клиент различает только два типа PIN: PIN, который назначен ему банком, выдавшим карточку, и PIN, который пользователь может выбирать себе самостоятельно.

В связи с тем, что PIN предназначен для идентификации и аутентификации клиента, его значение должно быть известно только клиенту. Однако на практике PIN трудно удержать в памяти и поэтому клиент банка куда-нибудь его запишет (иногда - на саму карточку). В результате задача злоумышленника бывает сильно облегчена.

Использование PIN, назначенных банком, неудобно даже при небольшом их количестве. Много цифр не удержишь в памяти и их придется записывать. Для большего удобства клиента используются PIN, выбираемые им самим. Такой способ определения PIN, во-первых, позволяет клиенту использовать один и тот же PIN для различных целей, и, во-вторых, позволяет задавать PIN как совокупность букв и цифр.

PIN обычно состоит из 4-6 цифр. Следовательно, для его перебора в наихудшем (для защиты естественно) случае необходимо осуществить 10.000 комбинаций (4-х символьный PIN). Такой перебор возможен за короткое время. Поэтому в системах, использующих такой PIN , должны быть предусмотрены меры защиты от подбора PIN.

Всего существуют два основных способа проверки PIN: алгоритмический и неалгоритмический.

Алгоритмический способ проверки заключается в том, что у пользователя запрашивается PIN, который преобразуется по определенному алгоритму с использованием секретного ключа и затем сравнивается со значением PIN, хранившемся на карточке. Достоинством этого метода проверки является:

- отсутствие копии PIN на главном компьютере, что исключает его раскрытие персоналом банка;

- отсутствие передачи PIN между АКА и главным компьютером банка, что исключает его перехват злоумышленником или навязывание результатов сравнения;

- облегчение работы по созданию программного обеспечения системы, так как уже нет необходимости действий в реальном масштабе времени.

Неалгоритмический способ проверки PIN, как это следует из его названия, не требует применения специальных алгоритмов. Проверка PIN осуществляется путем прямого сравнения полученного PIN со значениями, хранимыми в базе данных. Часто сама база данных со значениями PIN шифруется прозрачным образом, чтобы не затруднять процесс сравнения, но повысить ее защищенность.

Как же происходит генерация PIN? Вначале номер счета клиента дополняется нулями или другой константой до 16 шестнадцатеричных цифр (8 байт). Затем получившиеся 8 байт шифруются с использованием секретного ключа. Из получившегося шифртекста (8 байт), начиная с младших байт выделяются по 4 бита. Если значение числа, образуемого этими битами менее 10, то полученная цифра включается в PIN, иначе значение отбрасывается. Таким образом обрабатываются все 8 байт (64 бита). Если в результате обработки не удалось получить требуемое количество десятичных цифр, то из неиспользуемых комбинаций вычитается 10.

В том случае, когда необходимо получить выбираемый пользователем PIN, то каждая его цифра складывается по модулю 10 с соответствующей цифрой выведенного PIN (без учета переноса). Получаемое десятичное число называется «смещением» и запоминается на карточке. Так как выводимый PIN имеет случайное значение, то невозможно получить выбранный пользователем PIN по его «смещению».

В настоящее время ведется большая дискуссия по поводу применения PIN для идентификации клиентов [12]. Сторонники применения утверждают, что вскрытие PIN в Великобритании, например, составило несколько случаев в месяц против несколько сотен миллионов проведенных транзакций в год. Противники же доказывают, что идентификация клиента с использованием PIN работает только в следующих случаях:

- отсутствует перехват карточки и/или PIN при передаче от банка клиенту;

- банковские карточки не воруют, не теряют и их невозможно подделать;

- PIN невозможно узнать при доступе к системе другим пользователем;

- PIN иным образом не может быть скомпрометирован;

- в электронной системе банка отсутствуют сбои и ошибки;

- в самом банке нет мошенников.

В качестве альтернативы PIN предлагается применять устройства идентификации, основанные на биометрическом принципе. Их широкое применение сдерживается высокой стоимостью. Например, устройство, предлагаемое компанией Sats и предназначенное для идентификации человека по геометрии его руки, стоит около $3.500. [12]

Однако в настоящее время к биометрическим системам проявляется все больше интереса.

## Безопасность при использовании пластиковых карт.

Использование систем POS и АКА потребовало появления некоторого носителя информации, который мог бы идентифицировать пользователя и хранить некоторые учетные данные. В качестве такого носителя стали выступать пластиковые карточки.

В настоящее время выпущено более миллиарда карточек в различных странах мира [5, с.26]. Наиболее известные из них:

- кредитные карточки Visa (более 350 млн. карточек) и MasterCard (200 млн. карточек);

- международные чековые гарантии Eurocheque и Posteheque;

- карточки для оплаты путешествий и развлечений American Express (60 млн. карточек) и Diners Club.

По принципу действия можно выделить пассивные и активные пластиковые карточки. Пассивные всего лишь хранят информацию на том или ином носителе. Отличительной особенностью активных карточек является наличие встроенной в него микросхемы. Карточка с микропроцессором называется «интеллектуальной» (smart card).

По характеру расчетов, проводимых с использованием пластиковых карточек, можно выделить кредитные и дебетовые карточки.

По характеру использования карточки подразделяются на корпоративные и личные. Главное отличие корпоративных (которые могут быть выданы только юридическим лицам) от индивидуальных состоит в том, что их владельцы имеют право на получение дополнительных услуг.

Например, такими карточками может одновременно пользоваться большое количество сотрудников фирмы, но счета по совершенным ими сделкам будут выставлены фирме.

На магнитной карточке расположена магнитная полоса, состоящая из трех дорожек. Каждая из них имеет соответствующее назначение. Размеры карточки, формат хранимых данных определены специальным стандартом ISO 7811 1985 года.

Процессорный тип карточек изобретен и запатентован Роланом Мореном во Франции. Микросхемы, установленные на карточке, могут быть как обычными - энергонезависимой памяти, так и достаточно сложными микропроцессорами. Емкость обычной карточки с энергонезависимой памятью составляет от 2 до 16 килобайт. В постоянное запоминающее устройство, установленное на карточке, прошивается специальный набор программ. Иначе говоря, сердцем таких карточек является не просто микропроцессор, а микроЭВМ. Эти карточки обеспечивают обширный набор функций:

- возможность работы с защищенной файловой системой (доступ к файлам требует предъявления полномочий почтению/записи информации);

- шифрование данных с применением различных алгоритмов;

- ведение ключевой системы и т.д.

Некоторые карточки обеспечивают режим «самоблокировки» (невозможность дальнейшей работы с ней) при попытке несанкционированного доступа.

Преимуществом интеллектуальных карточек является больший объем хранимой информации, устойчивость к подделке и возможность использования во многих приложениях.

Интеллектуальные карточки позволяют существенно упростить процедуру идентификации клиента. Это позволяет оказаться от работы АКА в режиме реального времени и централизованной проверки PIN. Для проверки PIN применяется алгоритм, реализуемый микропроцессором на карточке. Физическая защита интеллектуальной карты позволяет гарантировать корректность результата проверки PIN.

В то же время интеллектуальные карточки обладают и существенными недостатками которые обусловили их ограниченное распространение. Основных недостатков два:

- высокая стоимость производства карточки;

- увеличенная по сравнению со стандартом толщина, из-за чего она не может быть прочитана обыкновенным АКА. Для чтения таких карточек необходима установка специальных считывателей.

Кредитные карточки - наиболее распространенный тип пластиковых карточек. К ним относятся карточки общенациональных систем США Visa и Mastercard, American Express и AmEx's Optima, карточка Discovery Card фирмы Sears, Universal Card фирмы AT&T, местные и региональные карточки универсальных магазинов. Ими пользуются миллионы людей в США.

Карточки предъявляются на предприятиях торговли и обслуживания для оплаты товаров и услуг. При оплате с помощью кредитных карточек банк покупателя открывает ему кредит на сумму покупки и затем через некоторое время (обычно 25 дней) присылает счет по почте. Покупатель возвращает оплаченный чек обратно в банк.

Visa, MasterCard и Discover требуют от обладателей карточек производства по крайней мере фиксированного минимального платежа.

Разновидностью кредитных карточек являются affinity-карточки. Они выпускаются банком, кредитным объединением или финансовой компанией, заключившими специальное соглашение с профессиональной, общественной, религиозной или другой некоммерческой организацией. Обычно знак этой организации помещается на кредитную карточку. Производитель карточек обязуется отчислять своему контрагенту некоторый (сравнительно небольшой) процент от прибыли при использовании карточек. В ответ на это организация, с которой заключен договор, помогает производителю карточек внедрить их среди ее членов.

Дебетовые карточки используются для дебетовых расчетов. Другие ее названия: карточка наличных средств или расчетная. Она во многом аналогична кредитной. Для дебетовых транзакций чаще всего используются АКА. Дебетовые карточки предназначены для замены наличных денег и персональных чеков.

Пластиковая карточка, как основной носитель информации для АКА и оборудования POS, является притягательным объектом для злоумышленника. Поэтому перед выпуском таких карточек необходимо четко представлять степень их защиты от различных воздействий. Существует два основных требования к банковским карточкам: уникальность и необратимость.

Первое требование означает, что среди всех выпущенных банком карточек не должно быть ни одной одинаковой по характеристикам. Создание подобной карточки должно быть исключено для злоумышленника. Согласно второму требованию, не может быть восстановлена первоначальная информация на карточке.

Для реализации этих требований каждая фирма-изготовитель предусматривает свои схемы защиты, все тонкости которых она хранит в секрете. Рассмотрим два основных способа защиты магнитных карточек от подделки: метод магнитных водяных знаков и метод «сэндвича».

Метод магнитных водяных знаков предусматривает нанесение на магнитную ленту, расположенную на карточке, специального рисунка. Этот рисунок наносится при помощи магнитного поля и выполняет ту же самую функцию, что и обычные водяные знаки на ценных бумагах. При изготовлении карточка подвергается воздействию сильного электромагнитного поля под углом 45 градусов к продольной оси. Затем на нее воздействует специальное записывающее устройство, которое преобразует направленность магнитных полей на карточке к особому виду.

Проверка карточки с нанесенными магнитными водяными знаками осуществляется специальными устройствами. Этот метод защиты не влияет на информацию, которая записана на информационных дорожках, а добавляет на неиспользуемую нулевую дорожку от 50 до 100 разрядов дополнительной информации. Эти знаки используется для дополнительной проверки.

Метод «сэндвича» является альтернативой методу водяных знаков и заключается в том, что одна полоска содержит участки с различными уровнями намагниченности, причем участок с меньшей намагниченностью расположен ближе к головке чтения/записи. Для записи информации на карточку используется сильное магнитное поле. В считывателе информации карточка вначале проходит через стирающее поле. При этом на участке со слабой намагниченностью информация стирается, а с сильной намагниченностью - не изменяется. Затем информация с полосы считывается обычным образом. Надежность этого метода защиты основана на двух предположениях: во-первых, если злоумышленник использует одинарную полосу для подделки карточки, то вся информация на ней будет затерта стирающим полем; во-вторых, для записи на двухслойную полосу требуется специальное оборудование для создания необходимого по величине магнитного поля.

Современные пластиковые карточки имеют несколько степеней (уровней) защиты. Например, карточки системы VISA имеют семь уровней защиты:

1. Торговое имя продукта, которое идентифицирует тип Visa карточки, вместе с символом защиты;

2. Вокруг панели расположена кайма впечатанных кодов идентификации банка;

3. Поле fine-line в области идентификации продукции:

- символ защиты;

- идентификатор банка над символом защиты;

- голубь (эмблема Visa), который видим только в ультрафиолетовых лучах;

- трехмерная голограмма голубя.

В настоящее время не существует достоверной статистики по потерям, которые связаны с использованием пластиковых карточек. По некоторым оценкам, они составляют до $2 млрд. в год. Основной причиной потерь является неправильное использование карточек их законными владельцами. [12]

Пропорции злоупотреблений с пластиковыми карточками зависят от структуры банковской индустрии и поэтому сильно меняются от страны к стране. Например, по сравнению с Западной Европой, в США большие потери происходят именно за счет неправильного использования карточек. Но при этом, по оценкам экспертов, ущерб от мошенничества с применением технических средств составляет не менее $500 млн. в год. [3, с.52]

Ниже приведена статистика потерь для Visa и MasterCard (данные 1993 года). [2, с.24]

|  |
| --- |
|  |
| Причина | Доля в общих потерях, % |
| Мошенничество продавца | 22.6 |
| Украденные карты | 17.2 |
| Подделка карт | 14.3 |
| Изменение рельефа карты | 8.1 |
| Потерянные карты | 7.5 |
| Неправильное применение | 7.4 |
| Мошенничество по телефону | 6.3 |
| Мошенничество при пересылке почтой | 4.5 |
| Почтовое мошенничество | 3.6 |
| Кражи при производстве пересылке | 2.9 |
| Сговор с владельцем карточки | 2.1 |
| Прочие | 3.5 |

Одно из важнейших требований безопасности при работе с пластиковыми карточками — обеспечение безопасности банкоматов.

В настоящее время на автоматические кассовые аппараты (АКА) возлагаются следующие задачи:

- идентификация и аутентификация клиента;

- выдача наличных денег;

- оповещение о состоянии счета клиента;

- перевод денег клиента с одного счета на другой;

- регистрация всех произведенных операций и выдача квитанций.

Основная задача АКА - выдача наличных денег клиенту. Так как внутри АКА кроме различных устройств находятся и наличные деньги, то должна быть предусмотрена его серьезная физическая защита.

По имеющимся данным [6, с.82] в Великобритании АКА установлены:

\* 67 % - в виде, вмонтированном в стену;

\* 21 % - внутри банков;

\* 5 % - в вестибюлях банков;

\* 7 % - отдельно стоящие банкоматы вне банков.

При рассмотрении дальнейшей защиты хранимой в АКА информации предполагается, что нарушение его внешней физической защиты маловероятно.

Автоматический кассовый аппарат может работать в одном из двух режимов:

1. Off-line (автономный режим). В автономном режиме АКА функционирует независимо от компьютеров банка. При этом запись информации о транзакциях производится на внутренний магнитный диск и выводится на встроенный принтер.

2. On-line (режим реального времени). Для работы в этом режиме АКА должен быть подсоединен (непосредственно, либо через телефонную сеть) к главному компьютеру банка. При этом регистрация транзакций осуществляется непосредственно на главном компьютере, хотя подтверждение о транзакции выдается на принтер АКА.

Как автономный режим работы АКА, так и режим реального времени обладают своими достоинствами и недостатками (см. табл. 17).

Преимуществами автономного режима АКА является его относительная дешевизна и независимость от качества линий связи. Это особенно следует отметить в отечественных условиях, когда качество телефонных линий, мягко говоря, не идеально. В то же время низкая стоимость установки напрямую обуславливает высокую стоимость эксплуатации этих аппаратов. Ведь для того, чтобы обновлять списки потерянных карточек, «черные списки» необходимо хотя бы раз в день специально выделенному человеку обновлять в месте расположения АКА. При значительном количестве таких устройств подобное обслуживание затруднительно. Отказ от ежедневного обновления списков может привести к большим потерям для банка в случае подделки карточки или при пользовании украденной карточкой.

Сложности возникают также и при идентификации (аутентификации) клиента. Для защиты информации, хранящейся на магнитной карточке применяется ее шифрование. Для того, чтобы АКА одного и того же банка воспринимали пластиковые карточки в них для шифрования/расшифрования должен быть использован один ключ. Компрометация его хотя бы на одном из АКА приведет к нарушению защиты на всех АКА.

Режим реального времени имеет большие преимущества по сравнению с автономным. Он позволяет клиенту не только получить наличные деньги, но и осуществлять манипуляции со своим счетом. Централизованная идентификация/аутентификация позволяет существенно повысить устойчивость системы к компрометации ключей шифрования. Централизованная проверка идентификатора пользователя делает возможным быстрое обновление списков запрещенных к использованию карточек, а также введение ограничений на количество наличных денег, которые может получить клиент в течение одного дня (для защиты от использования украденных карточек).

Однако этот режим работы возможен лишь при наличии надежных каналов связи между АКА и банком (банками), что делает его довольно дорогим.

Наличие канала связи порождает и другие угрозы безопасности по сравнению с автономным режимом работы. Это перехват информационного потока, анализ графика и имитация работы главного компьютера. При этом анализируются данные, передаваемые АКА главному компьютеру и получение на их основе информации о счетах, суммах, условиях платежей и т.д. Главный компьютер может быть имитирован компьютером злоумышленника и на запрос АКА о результатах идентификации/аутентификации выдавать положительный ответ.

В том случае, когда АКА работает в режиме реального времени для осуществления идентификации он обменивается с главным компьютером банка тремя сообщениями, каждое из которых должно соответствовать специальному алгоритму с использованием шифра, части которого находятся как в банкомате, так и в главном компьютере. Без серьезной математической подготовки и хорошего компьютерного оборудования злоумышленник не сможет осуществить перехват информации.

Для борьбы с подбором PIN применяется ограничение на его ввод — обычно трехкратное. Если три попытки ввода PIN оказались неудачными, то в платеже клиенту отказывается. Ранние системы после трех неудачных попыток не возвращали карточку, однако, такое решение проблемы, особенно с кредитными карточками, не вызвало восторга клиентов.

Для АКА, работающих в автономном режиме, возврат карточки в случае трехкратного неудачного ввода PIN является весьма опасным, так как позволяет дальше подбирать PIN.

Кроме одиночных АКА в настоящее время эксплуатируются и сети АКА, в которых участвуют несколько банков. Участники такой сети преследуют следующие цели:

- разделение затрат и риска при разработке новых видов услуг между участниками сети;

- уменьшение стоимости операций для участников;

- придание оказываемым услугам общенационального характера и, соответственно, повышение их субъективной ценности для потребителя;

- возможность для региональных банков, так же как и для банков, расположенных в финансовых центрах, немедленно получить выгоду от либерализации законодательства, регулирующего выход на рынки других стран;

- преодоление имеющихся географических ограничений, которых не существует для небанковских учреждений. В настоящее время в США насчитывается три общенациональных сети:

1. MasterCard/Cirrus;

2. Plus System;

3. Visa U.S.A.

При совместном использовании банками сети АКА появляется новая проблема - защита конфиденциальной информации банков друг от друга (ключи шифрования, списки номеров запрещенных к использованию карточек и т.д.). Для ее успешного решения была предложена схема централизованной проверки PIN каждым банком в своем центре связи с АКА. При этом также усложняется система распределения ключей между всеми участниками сети.

К эмитенту карточки предъявляются следующие требования:

- выпускаемые им карточки должны восприниматься всеми АКА сети;

- он должен обладать технологией проверки собственных обменных PIN (если в АКА используется встроенная проверка принадлежности транзакции, то главный компьютер должен эмулировать результаты проверки в таком же формате).

К банку, выдающему «чужие» карточки, в свою очередь, предъявляются другие требования:

- в АКА или главном компьютере банка должна быть реализована проверка принадлежности транзакции;

- если нет возможности проверить правильность чужого PIN, банк должен передать данные о транзакции на сетевой маршрутизатор.

Для защиты взаимодействия компьютеров банков между собой и с АКА применяется оконечное шифрование информации, передаваемой по линиям связи.

Наиболее часто используется следующий метод: вся сеть АКА разбита на зоны и в каждой из них используется свой Главный зональный управляющий ключ. Он предназначен для шифрования ключей при обмене между сетевым маршрутизатором и главным компьютером банка. Ключ индивидуален для всех участников сети. Обычно он случайно генерируется маршрутизатором и неэлектронным способом передается в банк. Раскрытие ключа приведет к раскрытию всех PIN, которые передаются между маршрутизатором и главным компьютером банка.

В неразделяемой сети АКА достаточно на всех АКА использовать один открытый ключ, а на главном компьютере банка закрытый ключ. Это позволит шифровать запрос и подтверждающее сообщение и проверять подлинность ответного сообщения из банка, так как обеспечение конфиденциальности ответного сообщения не обязательно. Особого внимания стоит проблема защиты запроса от активных атак (изменения или введения ложного запроса). Но и она в случае неразделяемой сети может быть решена с использованием пароля для идентификации АКА.

В случае сети совместно используемых АКА применение системы шифрования с открытым ключом позволяет отказаться от зональных ключей и дорогостоящей процедуры их смены. Однако в этом случае схема идентификации АКА по паролю не будет работать. Эта проблема может быть решена в том случае, когда каждый АКА вместе с запросом будет пересылать и свой открытый ключ, заверенный банком. [7, с.49]

Системы POS предназначены для сокращения расходов по обработке бумажных денег и для уменьшения риска покупателя и продавца, связанного с этой обработкой.

Покупатель для оплаты покупки предъявляет свою дебетовую или кредитную карточку и для подтверждения личности вводит PIN. Продавец со своей стороны вводит сумму, которую необходимо уплатить за покупку или за услуги.

Запрос на перевод денег направляется в банк продавца. Тот для проверки подлинности карточки, предъявленной покупателем, переадресует запрос в банк покупателя. Если карточка подлинная и покупатель имеет право применять ее для оплаты продуктов и услуг банк покупателя переводит деньги в банк продавца на его счет. После перевода денег банк продавца посылает извещение на терминал POS, в котором сообщает о завершении транзакции. После этого продавец выдает покупателю извещение.

Необходимо обратить внимание на тот путь, который должна проделать информация прежде чем будет осуществлена транзакция. Во время его прохождения возможна потеря сообщений. Во избежание этого банк продавца должен повторять выдачу сообщений при обнаружении их потери.

Для защиты системы POS должны соблюдаться следующие требования:

1. Проверка PIN, введенного покупателем, должна производиться системой банка покупателя. При пересылке по каналам связи PIN должны быть зашифрованы.

2. Сообщения, содержащие запрос на перевод денег (или подтверждение о переводе), должны проверяться на подлинность для защиты от внесения изменений и замены при прохождении по линиям связи к обрабатывающим процессорам.

Самым уязвимым местом системы POS являются ее терминалы. Все построение системы охраны исходит из предположения абсолютно надежной физической защиты банкомата. Для терминалов POS это не так. Изначально предполагается, что терминал системы POS незащищен от внешнего воздействия.

В связи с этим предположением возникают новые типы угроз для терминала. Они связаны с раскрытием секретного ключа, который находится в терминале POS и служит для шифрования информации, передаваемой терминалом в банк продавца. Угроза вскрытия ключа терминала весьма реальна, так как они устанавливаются в таких неохраняемых местах как магазины, автозаправочные станции и пр. Эти угрозы получили следующие названия: [2, с.391]

1. «Обратное трассирование». Сущность этой угрозы заключается в том, что если злоумышленник получит ключ шифрования, то он будет пытаться восстановить значения PIN, использованные в предыдущих транзакциях.

2. «Прямое трассирование». Сущность этой угрозы заключается в том, что если злоумышленник получит ключ шифрования, то он будет пытаться восстановить значения PIN, используемые в транзакциях, которые произойдут после того, как он получит ключ.

Для защиты от этих угроз были предложены три метода: метод ключа транзакции, метод выведенного (полученного) ключа и метод открытых ключей. Сущность первых двух заключается в том, что они предусматривают изменение ключа шифрования передаваемых данных для каждой транзакции.

Метод ключа транзакции был впервые предложен в 1983 году. Информация, передаваемая между каждым терминалом и каждым эмитентом карточек, должна быть зашифрована на уникальном ключе, который, в свою очередь, должен изменяться от транзакции к транзакции. Однако применение этого метода для большого количества терминалов и эмитентов карточек делает затруднительным управление ключами. Поэтому, в подавляющем большинстве практических приложений, он применяется не к связи «терминал-эмитент карточек», а к связи «терминал-получатель», так как каждый получатель имеет ограниченный набор обслуживаемых терминалов. При генерации нового ключа используются следующие составляющие: однонаправленная функция от значения предыдущего ключа, содержание транзакции и информация, полученная с карточки. При этом подразумевается, что предыдущая транзакция завершилась успешно. Такая схема обеспечивает защиту как от «обратного трассирования», так и от «прямого трассирования». Раскрытие одного ключа не дает возможности злоумышленнику вскрыть все предыдущие или все последующие транзакции.

Метод предусматривает также раздельную генерацию двух ключей - одного для шифрования PIN, другого для получения MAC. Это необходимо для разделения функций банков продавца и получателя. Недостатком схемы является ее сложность.

Метод выведенного ключа более прост в использовании, однако, и менее надежен. Он обеспечивает смену ключа при каждой транзакции независимо от ее содержания. Для генерации ключа здесь используется однонаправленная функция от текущего значения ключа и некоторое случайное значение. Метод обеспечивает защиту только от «обратного трассирования».

Применение открытых ключей позволяет надежно защититься от любых видов трассирования и обеспечить надежное шифрование передаваемой информации. В этом методе терминал РОЗ снабжается секретным ключом, на котором шифруется запрос к банку продавца.

Этот ключ генерируется при инициализации терминала. После генерации секретного ключа терминал посылает связанный с ним открытый ключ на компьютер продавца. Обмен между участниками взаимодействия осуществляется с использованием открытого ключа каждого из них. Подтверждение подлинности участников осуществляется специальным центром регистрации ключей с использованием своей пары открытого и закрытого ключей. Недостатком метода является его сравнительно малое быстродействие.

# Заключение.

Банки играют огромную роль в экономической жизни общества, их часто называют кровеносной системой экономики. Благодаря своей специфической роли, со времени своего появления они всегда притягивали преступников. К 90-м годам XX века банки перешли к компьютерной обработке информации, что значительно повысило производительность труда, ускорило расчеты и привело к появлению новых услуг. Однако компьютерные системы, без которых в настоящее время не может обойтись ни один банк, являются также источником совершенно новых угроз, неизвестных ранее. Большинство из них обусловлены новыми информационными технологиями и не являются специфическими исключительно для банков.

Существуют однако два аспекта, выделяющих банки из круга остальных коммерческих систем:

1. Информация в банковских системах представляет собой «живые деньги», которые можно получить, передать, истратить, вложить и т.д.

2. Она затрагивает интересы большого количества организаций и отдельных лиц.

Поэтому информационная безопасность банка — критически важное условие его существования.

В силу этих обстоятельств, к банковским системам предъявляются повышенные требования относительно безопасности хранения и обработки информации. Отечественные банки также не смогут избежать участи тотальной автоматизации по следующим причинам:

- усиления конкуренции между банками;

- необходимости сокращения времени на производство расчетов;

- необходимости улучшать сервис.

В США, странах Западной Европы и многих других, столкнувшихся с этой проблемой довольно давно, в настоящее время создана целая индустрия защиты экономической информации, включающая разработку и производство безопасного аппаратного и программного обеспечения, периферийных устройств, научные изыскания и др.

Сфера информационной безопасности — наиболее динамичная область развития индустрии безопасности в целом. Если обеспечение физической безопасности имеет давнюю традицию и устоявшиеся подходы, то информационная безопасность постоянно требует новых решений, т.к. компьютерные и телекоммуникационные технологии постоянно обновляются, на компьютерные системы возлагается все большая ответственность.

Статистика показывает, что подавляющее большинство крупных организаций имеют план с правилами доступа к информации, а также план восстановления после аварий.

Безопасность электронных банковских систем зависит от большого количества факторов, которые необходимо учитывать еще на этапе проектирования этой системы.

При этом для каждого отдельного вида банковских операций и электронных платежей или других способов обмена конфиденциальной информацией существуют свои специфические особенности защиты. Таким образом, организация защиты банковских систем есть целый комплекс мер, которые должны учитывать как общие концепции, но и специфические особенности.

Основной вывод, который можно сделать из анализа развития банковской отрасли, заключается в том, что автоматизация и компьютеризация банковской деятельности (и денежного обращения в целом) продолжает возрастать. Основные изменения в банковской индустрии за последние десятилетия связаны именно с развитием информационных технологий. Можно прогнозировать дальнейшее снижение оборота наличных денег и постепенный переход на безналичные расчеты с использованием пластиковых карт, сети Интернет и удаленных терминалов управления счетом юридических лиц.

В связи с этим следует ожидать дальнейшее динамичное развитие средств информационной безопасности банков, поскольку их значение постоянно возрастает.

# Список литературы

1. Абрамов А.В. Новое в финансовой индустрии: информатизация банковских технологий. — СПБ: Питер, 1997 г.
2. Гайкович Ю.В, Першин А.С. Безопасность электронных банковских систем. — М: Единая Европа, 1994 г.
3. Демин В.С. и др. Автоматизированные банковские системы. — М: Менатеп-Информ, 1997 г.
4. Крысин В.А. Безопасность предпринимательской деятельности. — М:Финансы и статистика, 1996 г.
5. Линьков И.И. и др. Информационные подразделения в коммерческих структурах: как выжить и преуспеть. — М: НИТ, 1998 г.
6. Титоренко Г.А. и др. Компьютеризация банковской деятельности. — М: Финстатинформ, 1997 г.
7. Тушнолобов И.Б., Урусов Д.П., Ярцев В.И. Распределенные сети. — СПБ: Питер, 1998 г.
8. Novell NetWare. Руководство пользователя, 1998 г.
9. Аглицкий И. Состояние и перспективы информационного обеспечения российских банков. — Банковские технологии, 1997 г. №1.
10. Аджиев В. Мифы о безопасности программного обеспечения: уроки знаменитых катастроф. — Открытые системы, 1998 г., №6.
11. Джонсон Джордж, Распределенные системы в многофилиальной структуре. — PC Magazine/Russian Edition, 1998 г., №10.
12. Заратуйченко О.В. Концепции построения и реализации информационных систем в банках. — СУБД, 1996 г., №4.
13. Кузнецов В.Е. Измерение финансовых рисков. — Банковские технологии, 1997, №9.
14. Мур Г. Глобальный информационный рынок. — Материалы агентства VDM-News, мониторинг иностранной прессы, 14.01.99 г.
15. Семеновых В.А. Некоторые вопросы информационно-аналитической работы в банке. — Материалы Семинара «Практические вопросы информационно-аналитической работы в коммерческом банке», 24-26.03.98 г.
16. Тарасов П.И. Диасофт предлагает комплексные решения для банков. — Мир ПК, 1998 г., №5.
17. Материалы агентства «Интерфакс». 1995-99 гг.
1. Под классической информационной безопасностью понимается система разделения прав доступа к информации, мероприятия по защите от прослушивания, предотвращение утечек со стороны персонала и другие меры, непосредственно не связанные с АСОИБ. [↑](#footnote-ref-1)