Содержание:

ВВЕДЕНИЕ

Одной из глобальных проблем в современных информационно-вычислительных системах, в том числе и банковских, является защита данных в компьютерных сетях. На сегодняшний день сформулировано три базовых принципа информационной безопасности, задачей которой является обеспечение:

- целостности данных - защита от сбоев, ведущих к потере информации или ее уничтожения;

- конфиденциальности информации;

- доступности информации для авторизованных пользователей.

Рассматривая проблемы, связанные с защитой данных в сети, возникает вопрос о классификации сбоев и несанкционированности доступа, что ведет к потере или нежелательному изменению данных. Это могут быть сбои оборудования (кабельной системы, дисковых систем, серверов, рабочих станций и т.д.), потери информации (из-за инфицирования компьютерными вирусами, неправильного хранения архивных данных, нарушений прав доступа к данным), некорректная работа пользователей и обслуживающего персонала. Перечисленные нарушения работы в сети вызвали необходимость создания различных видов защиты информации. Условно их можно разделить на три класса:

-средства физической защиты;

-программные средства (антивирусные программы, системы разграничения полномочий, программные средства контроля доступа);

-административные меры защиты (доступ в помещения, разработка стратегий безопасности фирмы и т.д.).

1. ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ ЗАЩИТЫ ИНФОРМАЦИИ В БАНКОВСКИХ СИСТЕМАХ

1.1. Общая характеристика средств защиты в банковской сфере

Сам термин «информационная безопасность» первоначально использовался для определения комплекса мер по защите информации от несанкционированных действий [3,4]. Однако практика показала, что общий объем ущерба, наносимый информационным системам осознанно, в результате противоправных действий, ниже ущерба, возникающего в результате ошибок и сбоев. Поэтому в настоящий момент понятие информационной безопасности включает в себя весь комплекс мер по предотвращению и устранению сбоев в работе информационных систем, по организации и защите информационных потоков от несанкционированного доступа и использования.

Информационная система рассматривается как единое целое программно-аппаратного комплекса и человеческих ресурсов. Под нарушением будем понимать любое нерегламентированное событие в информационной системе, способное привести к нежелательным для организации последствиям.

Рассмотрим основные нарушения возникающие в системе [6]: нарушения конфиденциальности, изменения в системе, утрата работоспособности.

Нарушения конфиденциальности.

Причиной возникновения данной проблемы является нарушение движения информационных потоков или ошибки в системе доступа. Из-за того, что данные виды нарушений никак не влияют на состояние системы, выявить их очень сложно. Только небольшое число подобных нарушений можно вычислить в результате анализа файлов протокола доступа к отдельным объектам системы.

Наиболее часто встречающиеся примеры нарушения доступа к информации:

– ошибки администрирования:

– неправильное формирование групп пользователей и определение прав их доступа;

– отсутствие политики формирования паролей пользователей. При этом до 50% пользователей используют простые, легко подбираемые пароли, такие, как «123456», «qwerty» или собственное имя;

– ошибки в формировании итоговых и агрегированных отчетов и доступа к ним. Примером может являться отчет по выпискам из счетов банка или сводный бухгалтерский журнал, которые хранят всю информацию по операциям кредитной организации и формируются в бухгалтерии, где за доступом к данным отчетам часто не ведется контроль;

– наличие открытого доступа для представителей сторонней организации, выполняющей какие-либо подрядные работы;

– ошибки проектирования информационной системы:

– использование недостаточно защищенной среды для разработки информационной системы. Очень часто, особенно для систем, располагаемых на локальных компьютерах, доступ к информации можно получить не через интерфейс программы, который требует пароля, а напрямую читая из таблиц базы данных;

– ошибки алгоритмов доступа к данным. Особенно это касается разработки систем криптозащиты, где часто вместо дорогостоящих систем в целях экономии используются собственные разработки, только эмитирующие систему защиты;

– небрежность в разработке системы защиты. Один из примеров данной небрежности – забытая разработчиками точка доступа в систему, такая, как универсальный пароль;

– небрежность пользователей в вопросах информационной безопасности:

– нарушение хранения паролей для доступа в информационную систему. Иногда пользователи просто пишут пароль на бумаге и оставляют ее около компьютера. Особенно это распространено в организациях, где администратор системы требует сложных паролей, которые легко забыть. Также часто встречается абсолютно недопустимая практика передачи паролей сотрудниками друг другу;

– сохранение закрытого соединения после окончания работы. Уходя на обед или домой, пользователь не выключает компьютер и не выходит из банковской системы. Если система не имеет механизма временного отключения неактивных пользователей, данное нарушение делает бессмысленным большинство других требований системы безопасности;

– нерегламентированное обсуждение зарытой информации;

– умышленный взлом системы:

– через внешние точки доступа в информационную систему, например через Интернет. Самый опасный вид взлома, так как нарушитель недоступен или почти недоступен для службы безопасности и, чувствуя свою безнаказанность, может нанести максимальный вред организации;

– нерегламентированное подключение к собственной сети (информационным коммуникациям) банка. С развитием сетевых технологий данный вид нарушений встречается достаточно редко;

– анализ неуничтоженных черновых документов системы. Данный вариант утечки информации практически не рассматривается службами безопасности, появляется самым легким методом получения информации для злоумышленников. В первую очередь это относится к черновым распечаткам из отдела информационных технологий.

Нарушение целостности или нерегламентированные изменения в информационной системе приводят к более серьезным последствиям, чем нарушения конфиденциальности. Однако при правильном построении информационной безопасности нерегламентированные изменения могут быть зарегистрированы и выявлены в процессе работы. Кроме того, существуют дополнительные механизмы защиты от них, такие, как электронная подпись, благодаря чему общее количество данных нарушений меньше, чем нарушений доступа на просмотр информации, хотя их последствия более серьезны.

Причины, приводящие к нарушениям записи информации в системе, можно сгруппировать следующим образом:

- ошибки программирования;
- ошибки ввода;
- технические сбои;
- умышленные нарушения в системе;

Утрата работоспособности или производительности не связана с информационными потоками. Ее причины кроются в механизмах самой системы, в ее способности совершать различные действия. Ущерб от подобных нарушений зависит от степени частичного снижения или полной потери работоспособности. Как правило, ущерб от подобных сбоев определяется временем задержки работы и стоимостью работ на их устранение.

Наиболее распространенной причиной нарушений в работе информационных систем являются ошибки их пользователей – непреднамеренные ошибки сотрудников организации. Как правило, данные нарушения не приводят к большому ущербу, хотя возможны и исключения. Современные механизмы контроля и мониторинга позволяют почти полностью исключить этот тип нарушений. Однако из-за большого количества разновидностей ошибок создание системы, полностью исключающей их появление, как правило, невозможно или связано с неоправданными затратами.

Другой случай – это преднамеренные действия сотрудников, нарушения, которые являются самыми сложными для предотвращения. Сотрудник организации, как правило, хорошо ориентируется во внутренних процессах и системах. Часто он знает о механизмах безопасности и, что более опасно, об их отсутствии в определенных модулях системы. У него есть время и возможность смоделировать и протестировать свои действия, оценить последствия.

Еще одним слабым местом в системе безопасности от умышленных действий сотрудников является доверие к ним других работников организации. Часто достаточно простой просьбы к администратору для получения доступа к закрытым данным или требования у разработчика добавления какой-либо, на первый взгляд безопасной, функции системы, чтобы впоследствии использовать ее для противоправных действий.

Причинами, побудившими сотрудников к умышленному нарушению информационной безопасности, являются:

- обида на действия менеджеров, как правило, связанная с конфликтами или увольнением сотрудника;
- попытка дополнительного заработка;
- попытка хищения денег из организации;
- попытка создания зависимости организации от конкретного сотрудника;
- карьерная борьба.

В качестве мер противостояния нарушениям данного типа наиболее эффективны социальные меры, разграничение доступа и мониторинг действий пользователей.

Еще одна группа причин нарушений в работе информационных систем – действия сторонних лиц криминального характера. Несмотря на постоянное обсуждение этой темы в прессе, большое количества фильмов о хакерах, бурное развитие информационных технологий, объем таких нарушений, повлекших реальный

ущерб, скорее растет, чем снижается. Возможно, это вызвано именно завышенной рекламой данных нарушений, но следствием является максимальное количество затрат в области информационных технологий на защиту от них. Однако следует признать, что кредитные организации действительно являются объектом пристального внимания.

Цель у преступников, как правило, одна – деньги, однако методы ее достижения постоянно совершенствуются. Поэтому, анализируя потенциальные нарушения, в первую очередь следует выделять объекты возможной атаки (системы удаленных платежей, системы расчета пластиковыми картами и т.п.). В случае удачи у преступника много шансов остаться безнаказанным.

Основой политики информационной безопасности в коммерческом банке является общая политика безопасности организации. Часто информационная безопасность рассматриваются как часть общей системы безопасности. Постоянное сравнение базовых принципов защиты организации и механизмов защиты информационной системы может привести к значительному росту ее надежности и эффективности.

С другой стороны, система информационной безопасности тесно связана с техническими проблемами, решение которых может потребовать значительных сроков и ресурсов, что может привести к экономической нецелесообразности использования рассматриваемых механизмов. На Рисунок 1 приведена схема организации информационной безопасности.

Обеспечение информационной безопасности достигается системой мер, направленных[8]:

- на предупреждение угроз. Предупреждение угроз – это превентивные меры по обеспечению информационной безопасности в интересах упреждения возможности их возникновения;
- на выявление угроз. Выявление угроз выражается в систематическом анализе и контроле возможности появления реальных или потенциальных угроз и своевременных мерах по их предупреждению;
- на обнаружение угроз. Обнаружение имеет целью определение реальных угроз и конкретных преступных действий;
- на локализацию преступных действий и принятие мер по ликвидации угрозы или конкретных преступных действий;
- на ликвидацию последствий угроз и преступных действий и восстановление статус-кво (рисунок 2).


Общая политика информационной безопасности
Используемые технологии
Бизнес-процессы
Ожидаемые риски и угрозы
Концепция информационной безопасности
Модель защиты и восстановления
Определение технических средств защиты и восстановления
Выработка правил информационной безопасности для сотрудников и прочих пользователей информационной системы
Установка и эксплуатация технических средств
Мониторинг
Восстановление и устранение последствий
Анализ эксплуатации системы безопасности

Рисунок 1 – Схема организации информационной безопасности

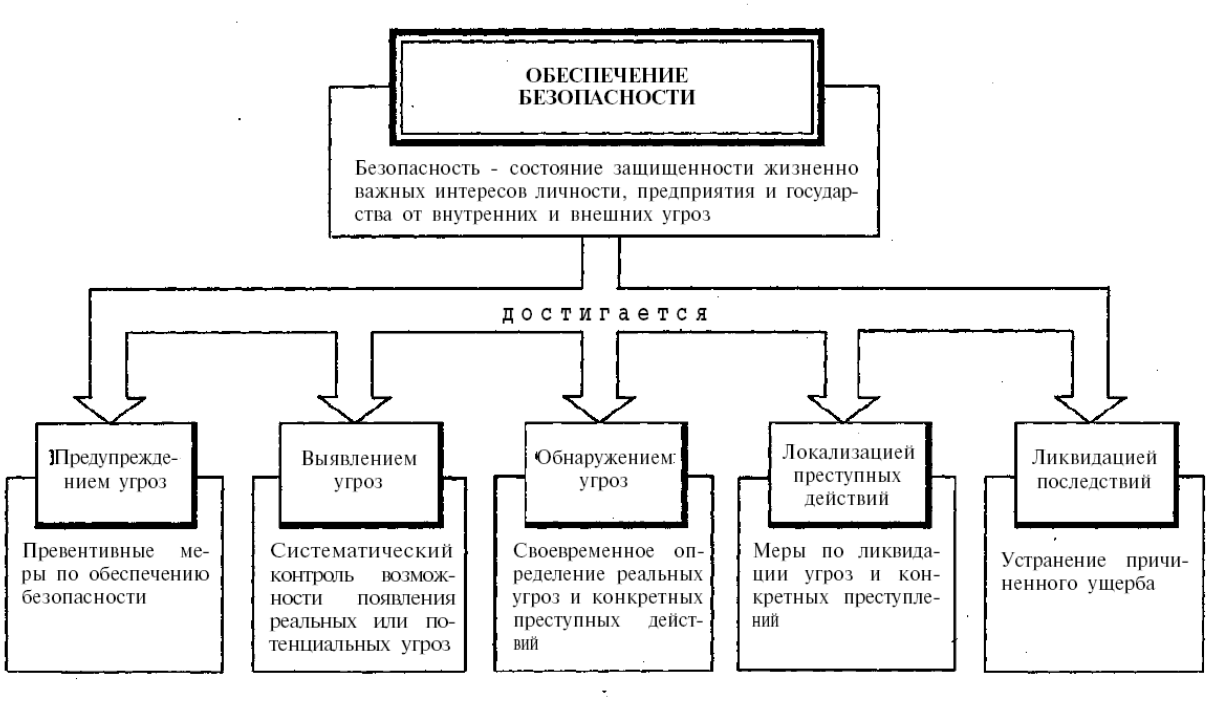

Рисунок 2 – Обеспечение информационной безопасности

Предупреждение возможных угроз и противоправных действий может быть обеспечено самыми различными мерами и средствами, начиная от создания климата глубоко осознанного отношения сотрудников к проблеме безопасности и защиты информации до создания глубокой, эшелонированной системы защиты физическими, аппаратными, программными и криптографическими средствами. Все эти способы имеют целью защитить информационные ресурсы от противоправных посягательств и обеспечить:

- предотвращение разглашения и утечки конфиденциальной информации;
- воспрещение несанкционированного доступа к источникам конфиденциальной информации;
- сохранение целостности, полноты и доступности информации;
- соблюдение конфиденциальности информации;
- обеспечение авторских прав (Рисунок 3).

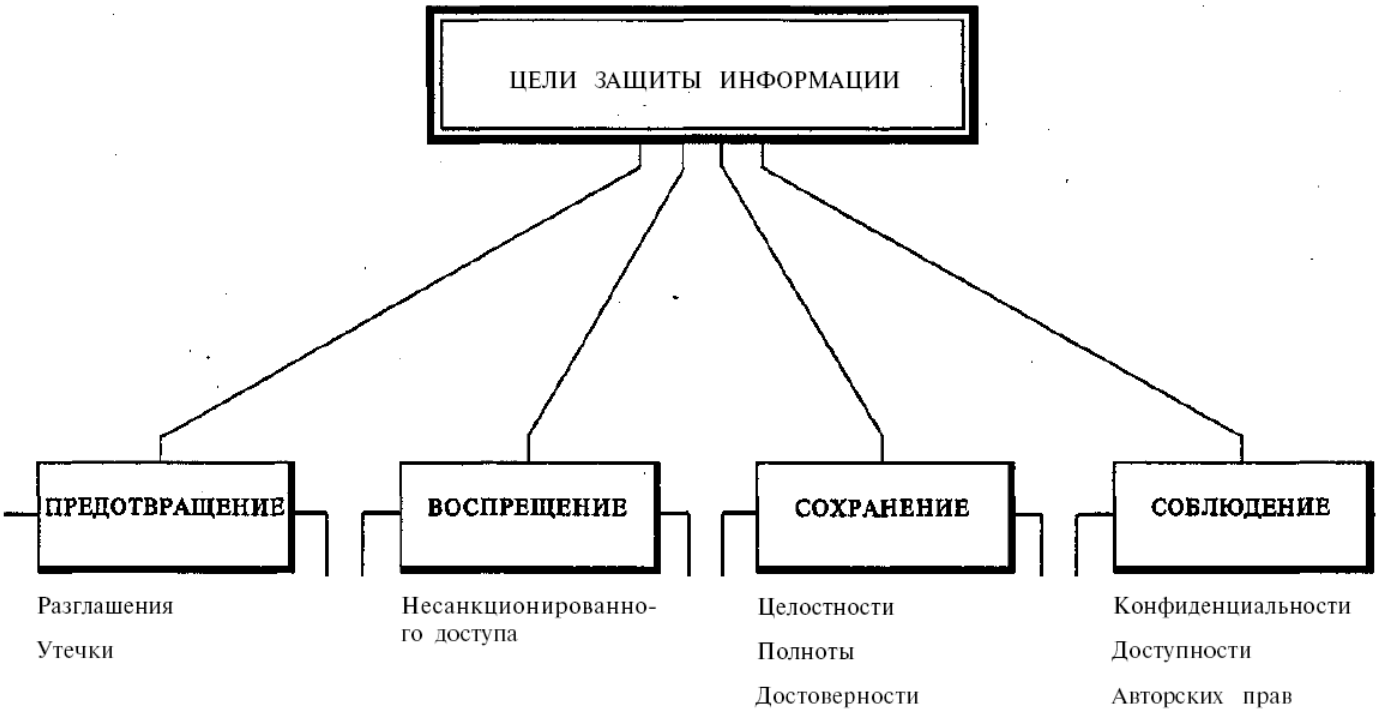

Рисунок 3 – Цели защиты информации

1.2. Применение средств защиты для идентификации пользователей в банке

Основной концепцией обеспечения ИБ объектов является комплексный подход, который основан на интеграции различных подсистем связи, подсистем обеспечения безопасности в единую систему с общими техническими средствами, каналами связи, программным обеспечением и базами данных [7].

Комплексная безопасность предполагает обязательную непрерывность процесса обеспечения безопасности как во времени, так и в пространстве (по всему технологическому циклу деятельности) с обязательным учетом всех возможных видов угроз (несанкционированный доступ, съем информации, терроризм, пожар, стихийные бедствия и т.д.).

В какой бы форме ни применялся комплексный подход, он связан с решением ряда сложных разноплановых частных задач в их тесной взаимосвязи. Наиболее

очевидными из них являются задачи ограничения доступа к информации, технического и криптографического закрытия информации, ограничения уровней паразитных излучений технических средств, технической укрепленности объектов, охраны и оснащения их тревожной сигнализацией. Однако необходимо решение и других, не менее важных задач. Например, выведение из строя руководителей банка или ключевых работников может поставить под сомнение само существование данного банка. Этому же могут способствовать стихийные бедствия, аварии, терроризм и т.д.

Наиболее существенным является эффективность системы обеспечения ИБ объекта, выбранные банком. Эту эффективность для ПЭВМ можно оценить набором программно-аппаратных средств, применяемых в ВС. Оценка такой эффективности может быть проведена по кривой роста относительного уровня обеспечения безопасности от наращивания средств контроля доступа (Рисунок 4).

Рисунок 4 – Кривая роста относительного уровня обеспечения безопасности

Для гарантии того, чтобы только зарегистрированные в АС пользователи могли включить компьютер (загрузить операционную систему) и получить доступ к его ресурсам, каждый доступ к данным в защищенной АС осуществляется в три этапа: идентификация – аутентификация – авторизация [6,7].

Идентификация – присвоение субъектам и объектам доступа зарегистрированного имени, персонального идентификационного номера (PIN-кода), или идентификатора, а также сравнение (отождествление) предъявляемого идентификатора с перечнем присвоенных (имеющихся в АС) идентификаторов. Основываясь на идентификаторах, система защиты «понимает», кто из пользователей в данный момент работает на ПЭВМ или пытается включить компьютер (осуществить вход в систему). Аутентификация определяется как проверка принадлежности субъекту доступа предъявленного им идентификатора, либо как подтверждение подлинности субъекта. Во время выполнения этой процедуры АС убеждается, что пользователь, представившийся каким-либо легальным сотрудником, таковым и является. Авторизация – предоставление пользователю полномочий в соответствии с политикой безопасности, установленной в компьютерной системе. Процедуры идентификации и аутентификации в защищенной системе осуществляются посредством специальных программных (программно-аппаратных) средств, встроенных в ОС или СЗИ. Процедура идентификации производится при включении компьютера и заключается в том, что сотрудник «представляется» компьютерной системе. При этом АС может предложить сотруднику выбрать свое имя из списка зарегистрированных пользователей или правильно ввести свой идентификатор. Далее пользователь должен убедить АС в том, что он действительно тот, кем представился.

Современные программно-аппаратные средства идентификации и аутентификации по виду идентификационных признаков можно разделить на электронные, биометрические и комбинированные. В отдельную подгруппу в связи с их специфическим применением можно выделить системы одноразовых паролей, входящие в состав электронных (Рисунок 5).

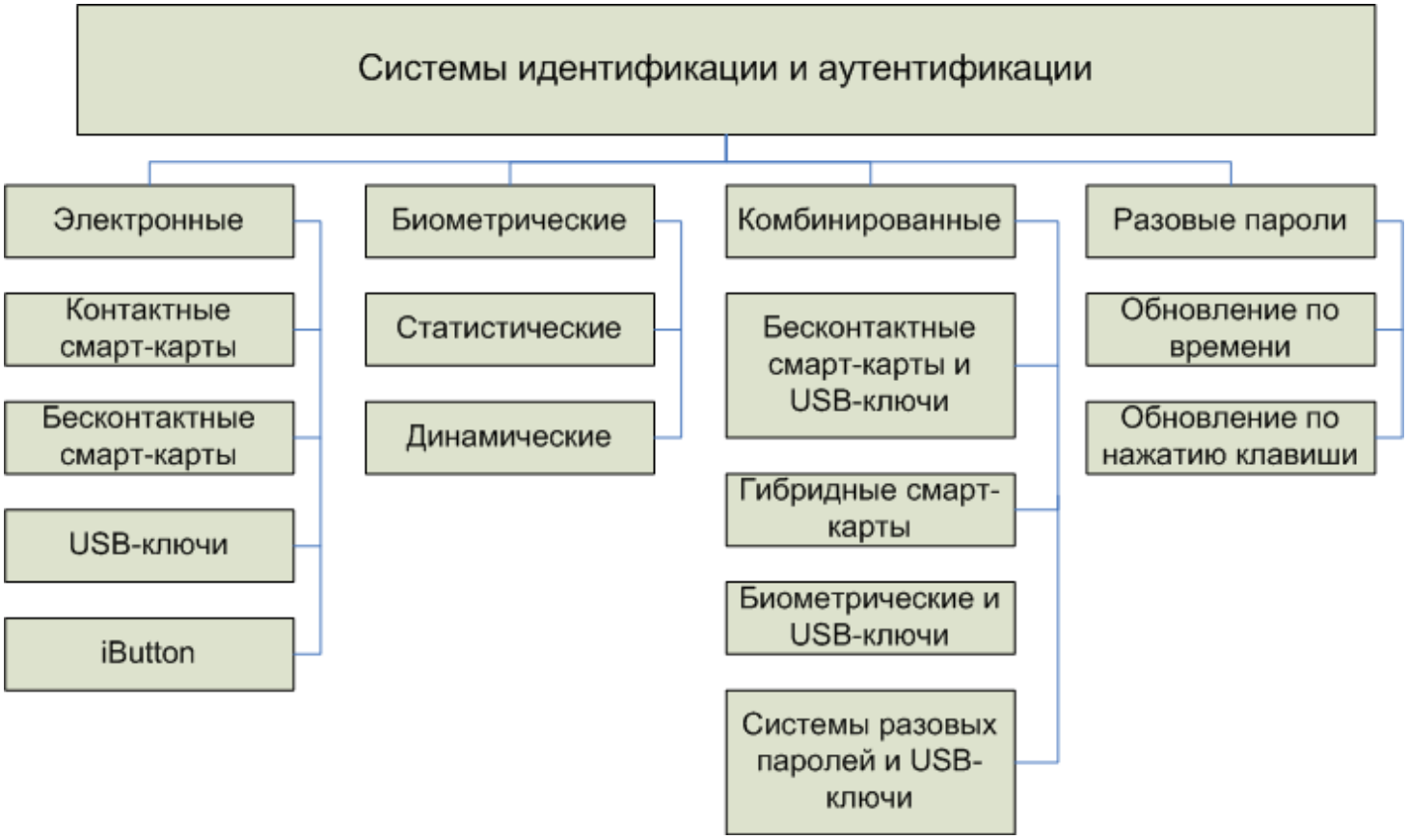

Рисунок 5 – Классификация программно-аппаратных систем идентификации и аутентификации

В электронных системах идентификационные признаки представляются в виде кода, хранящегося в памяти идентификатора (носителя). Идентификаторы в этом случае бывают следующие:

- контактные смарт-карты;
- бесконтактные смарт-карты;
- USB-ключи (USB-token);
- iButton.

В биометрических системах идентификационными являются индивидуальные особенности человека, которые в данном случае называются биометрическими признаками. Идентификация производится за счет сравнения полученных биометрических характеристик и хранящихся в базе шаблонов. В зависимости от характеристик, которые при этом используются, биометрические системы делятся на статические и динамические.

Статическая биометрия основывается на данных (шаблонах), полученных из измерений анатомических особенностей человека (отпечатки пальцев, узор

радужки глаза и т.д.).

Динамическая основывается на анализе действий человека (голос, параметры подписи, ее динамика).

В комбинированных системах используется одновременно несколько признаков, причем они могу принадлежать как системам одного класса, так и разным.

В состав электронных систем идентификации и аутентификации входят контактные и бесконтактные смарт-карты и USB-token [2].

Бесконтактные смарт-карты разделяются на идентификаторы Proximity и смарт-карты, базирующиеся на международных стандартах ISO/IEC 15693 и ISO/IEC 14443. В основе большинства устройств на базе бесконтактных смарт-карт лежит технология радиочастотной идентификации.

Таблица 1 – Радиочастотные идентификаторы

Характеристика	Proximity	Смарт-карты	
		ISO/IEC 14443	ISO/IEC 15693
Частота радиоканала	125 кГц	13,56 МГц	13,56 МГц
Дистанция чтения	До 1 м	До 10 см	До 1 м
Встроенные типы чипов	Микросхема памяти, микросхема с жесткой логикой	Микросхема памяти, микросхема с жесткой логикой, процессор	Микросхема памяти, микросхема с жесткой логикой
Функции памяти	Только чтение	Чтение-запись	Чтение-запись
Емкость памяти	8–256 байт	64 байт – 64 кбайт	256 байт – 2 кбайт

Алгоритмы шифрования и аутентификации	Нет	Технология MIRAGE, DES, 3DES, AES, RSA, ECC	DES, 3DES
Механизм антиколлизии	Опционально	Есть	Есть

Основными компонентами бесконтактных устройств являются чип и антенна. Идентификаторы могут быть как активными (с батареями), так и пассивными (без источника питания). Идентификаторы имеют уникальные 32/64 разрядные серийные номера.

Системы идентификации на базе Proximity криптографически не защищены, за исключением специальных заказных систем.

USB-ключи работают с USB-портом компьютера. Изготавливаются в виде брелоков. Каждый ключ имеет прошиваемый 32/64 разрядный серийный номер.

Таблица 2 – Характеристики USB-ключей

Изделие	Емкость памяти, кБ	Разрядность серийного номера	Алгоритмы шифрования
iKey 20xx	8/32	64	DES (ECB и CBC), DESX, 3DES, RC2, RC5, MD5, RSA-1024/2048
eToken R2	16/32/64	32	DESX (ключ 120 бит), MD5
eToken Pro	16/32	32	RSA/1024, DES, 3DES, SHA-1
ePass 1000	8/32	64	MD5, MD5-HMAC

ePass 2000	16/32	64	RSA, DES, 3DES, DSA, MD5, SHA-1
ruToken	8/16/32/64/128	32	ГОСТ 28147–89, RSA, DES, 3DES, RC2, RC4, MD4, MD5, SHA-1
uaToken	8/16/32/64/128	32	ГОСТ 28147–89

USB-ключи, представленные на рынке:

- eToken R2, eToken Pro – компания Aladdin Knowledge Systems;
- iKey10xx, iKey20xx, iKey 3000 – компания Rainbow Technologies;
- ePass 1000 ePass 2000 – фирма Feitian Technologies;
- ruToken – разработка компании «Актив» и фирмы «АНКАД»;
- uaToken – компания ООО «Технотрейд».

USB-ключи – это преемники смарт-карт, в силу этого структуры USB-ключей и смарт-карт идентичны.

Внедрение комбинированных систем существенно увеличивает количество идентификационных признаков и тем самым повышает безопасность.

Таблица 3 – Основные функции комбинированных систем

	Комбинированные системы		
Функция	На базе бесконтактных смарт-карт и USB-ключей	На базе гибридных смарт-карт	Биоэлектронные системы
Идентификация и аутентификация компьютеров	Есть	Есть	Есть

Блокировка работы компьютеров и разблокирование при предъявлении персонального идентификатора	Есть	-	Есть
Идентификация и аутентификация сотрудников при их доступе в здание, помещение (из него)	Есть	Есть	-
Хранение конфиденциальной информации (ключей шифрования, паролей, сертификатов и т.д.)	Есть	Есть	Есть
Визуальная идентификация	-	Есть	Есть

2. ПРАКТИЧЕСКИЕ АСПЕКТЫ ЗАЩИТЫ ИНФОРМАЦИИ В БАНКОВСКИХ СИСТЕМАХ

2.1. Применение средств защиты для аутентификации работников в банке

Аутентификация в защищенных АС может осуществляться несколькими методами [2,3]:

• парольная аутентификация (ввод специальной индивидуальной для каждого пользователя последовательности символов на клавиатуре);

• на основе биометрических измерений (наиболее распространенными методами биометрической аутентификации пользователей в СЗИ являются чтение

папиллярного рисунка и аутентификация на основе измерений геометрии ладони, реже встречаются голосовая верификация и считывание радужной оболочки или сетчатки глаз);

• с использованием физических носителей аутентифицирующей информации.

Наиболее простым и дешевым способом аутентификации личности в АИС является ввод пароля (трудно представить себе компьютер без клавиатуры). Однако существование большого количества различных по механизму действия атак на систему парольной защиты делает ее уязвимой перед подготовленным злоумышленником.

Биометрические методы в СЗИ пока не нашли широкого применения. Непрерывное снижение стоимости и миниатюризация, например, дактилоскопических считывателей, появление «мышек», клавиатур и внешних флеш-носителей со встроенными считывателями неминуемо приведет к разработке средств защиты с биометрической аутентификацией.

В настоящее время для повышения надежности аутентификации пользователей в СЗИ применяют внешние носители ключевой информации. В технической литературе производители этих устройств и разработчики систем безопасности на их основе пользуются различной терминологией. Можно встретить подходящие по контексту термины: электронный идентификатор, электронный ключ, внешний носитель ключевой или кодовой (аутентифицирующей) последовательности. Следует понимать, что это устройства внешней энергонезависимой памяти с различным аппаратным интерфейсом, работающие в режимах чтение или чтение / запись и предназначенные для хранения ключевой (для шифрования данных) либо аутентифицирующей информации. Наиболее распространенными устройствами являются электронные ключи «Touch Memory» на базе микросхем серии DS199X фирмы Dallas Semiconductors. Другое их название – «iButton» или «Далласские таблетки».

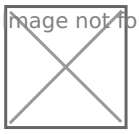

Рисунок 6 – Внешний вид электронного ключа iButton

В СЗИ активно используются пластиковые карточки различных технологий (чаще всего с магнитной полосой или проксими-карты, Рисунок 7). Пластиковые карточки

имеют стандартный размер 54x85,7x0,9 – 1,8 мм.

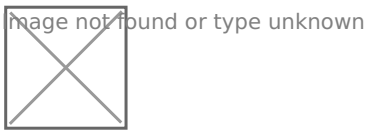

Рисунок 7 – Пластиковая карта с магнитной полосой

Удобными для применения в СЗИ являются электронные ключи eToken (Рисунок 8), выполненные на процессорной микросхеме семейства SLE66C Infineon, обеспечивающей высокий уровень безопасности. Они предназначены для безопасного хранения секретных данных, например, криптографических ключей. eToken выпускается в двух вариантах конструктивного оформления: в виде USB-ключа и в виде смарт-карты стандартного формата. В большинстве программно-аппаратных средств защиты информации предусмотрена возможность осуществлять аутентификацию личности пользователя комбинированным способом, т.е. по нескольким методам одновременно. Комбинирование способов аутентификации снижает риск ошибок, в результате которых злоумышленник может войти в систему под именем легального пользователя.

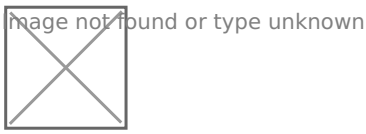

Рисунок 8 – Электронные ключи eToken

Тема аутентификации (подтверждения подлинности идентификатора объекта) последние пять лет является одной из самых обсуждаемых практически на всех конференциях по информационной безопасности (ИБ) международного и национального уровней. С одной стороны, это объясняется тем, что в условиях глобализации размываются границы предприятия, мир становится мобильным, ресурсы – все более распределенными (отметим, что все более активными становятся хакеры, а значит, увеличивается процент мошенничества). Соответственно, обостряется вопрос о необходимости доподлинно знать, тот ли это ресурс, за который он себя выдает (противодействие фишингу), и является ли пользователь, который стремится получить доступ к данному ресурсу, легальным? С другой стороны, аутентификация как один из основных сервисов безопасности – обязательная составляющая систем защиты от несанкционированного доступа (НСД), в качестве подсистемы входящая в ряд систем ИБ.

2.2. Средства и методы аутентификации

Перед многими специалистами ИБ стоит задача выбора средств и методов аутентификации. Банки активно учатся оценивать риски, в частности, связанные с информационной безопасностью. Этому немало способствует и всплеск мошенничества с операциями по банковским картам, с модным нынче web-доступом к личным кабинетам по управлению инвестиционным портфелем и с уже вполне «привычными» для нашего уха хакерскими операциями со счетами, системами клиент-банк и т.д. Банки, уже ощутившие финансовый ущерб от подобных атак мошенников, начинают применять современные средства защиты, в том числе надежные технологии аутентификации, в качестве одной из мер снижения рисков финансовых потерь. Нередко встречаются и такие типы защитных мер, как рекомендации банков своим клиентам. Действуя по принципу «Предупрежден – значит, вооружен», клиентам банка рассылаются предупреждения о том, что при переводе сумм выше определенного уровня ответственность переносится на клиентов.

С точки зрения применяемых технологий аутентификации, безусловно, самой надежной является взаимная строгая двухфакторная аутентификация. В ее основе лежит технология электронной цифровой подписи (ЭЦП) с применением USB-ключей или смарт-карт в качестве надежного хранилища закрытых ключей пользователей. Под взаимностью понимается возможность проверки валидности сертификата цифровой подписи как клиента сервером, так и наоборот. Однако эта технология требует развитой инфраструктуры открытых ключей, наличия доверенной среды, а также средств проверки ЭЦП на клиентской рабочей станции.

При отсутствии возможностей для выполнения этих условий, в частности, для организации удаленного доступа из недоверенной среды, были разработаны достаточно надежные схемы с применением одноразовых паролей (технология OTP – One Time Password). Суть концепции одноразовых паролей состоит в использовании различных паролей при каждом новом запросе на предоставление доступа. Одноразовый пароль действителен только для одного входа в систему. Динамический механизм задания пароля является одним из лучших способов защитить процесс аутентификации от внешних угроз. Аутентификация с применением механизма OTP называется усиленной.

И, наконец, при самом низком уровне рисков и ничтожно малом возможном ущербе при разглашении информации, доступ к которой необходимо организовать, широко используется способ аутентификации, основанный на применении парольной защиты.

Итак, лучшей практикой для подтверждения подлинности идентификатора является двусторонняя строгая аутентификация, основанная на технологии ЭЦП. В ситуациях, когда данную технологию использовать невозможно, необходимо применять OTP, и только при минимальном уровне рисков проникновения злоумышленника к информационным ресурсам рекомендуется применение технологий аутентификации с помощью многоразовых паролей.

В последнее время все более актуальной становится тема предоставления сервисов удаленного доступа к информационным ресурсам посредством мобильных устройств – телефонов, смартфонов, «наладонников». Однако желание заказчика иметь полнофункциональный мобильный доступ и производить защищенные транзакции с помощью своего мобильного устройства сталкивается, прежде всего, с технологическими трудностями осуществления полнофункциональной двусторонней (клиент – сервер) аутентификации. Подавляющая часть предоставляемых на рынке сервисов недостаточно защищена от различного рода атак, в том числе типа «человек посередине». Кроме того, ситуацию усугубляют, с одной стороны, постоянно повышающийся уровень распространения интернет-мошенничества, с другой – неискушенность пользователей в вопросах безопасности. Со стороны клиента в данном случае вопросы аутентификации пользователя подменяются вопросами аутентификации даже не самого мобильного устройства, а всего лишь SIM-карты, зарегистрированной оператором связи в контракте, который пользователь подписывает при ее приобретении. Действительно, пользователь имеет нечто (в рассматриваемой ситуации – SIM-карту) и знает нечто (четырехзначный PIN-код), процесс аутентификации для него заканчивается после правильно введенного PIN-кода при включении телефона. PIN-код участвует только в обмене устройство – пользователь как средство доказательства владельцем того, что это именно его SIM-карта. Все дальнейшие действия выполняются от имени идентифицированной сервером SIM-карты по ее уникальному ID – номеру, который карта «приобрела» в момент ее производства. Клиент никак не может аутентифицировать (проверить подлинность) сервер, на который поступает заявка, скажем, о переводе некоторой суммы. Процесс обмена SMS-сообщениями, часто происходящий при предоставлении подобных сервисов, абсолютно не защищен, кстати, как и сам SMS-сервер.

Одним из бурно развивающихся сервисов в настоящее время является организация web-доступа к различным приложениям. В частности, для банков актуальны задачи выполнения защищенных on-line запросов, например, организация выписок

состояния счета клиента, а также само выполнение защищенных транзакций. Главная проблема ИБ при этом – недостаточная защита клиентских рабочих станций. Естественным выходом из ситуации является перенос возможно большей части операций на сторону сервера. Современные технологические решения позволяют осуществлять подгрузку необходимых форм (например, платежных поручений) на клиентскую часть с сервера после авторизации легального пользователя на клиентской стороне. Пользователю необходимо лишь заполнить форму и подтвердить свои намерения электронной цифровой подписью. Подобные решения обычно строятся с применением трехзвенной архитектуры. Весь защищенный диалог с участием клиента организовывается на сервере приложений, к базе данных по защищенному каналу обращается лишь сервер приложений с запросами по согласованным форматам. Для обеспечения допустимого уровня рисков, как правило, необходимо полнофункциональное решение по организации доступа пользователей с применением технологии ЭЦП на основе развитой инфраструктуры открытых ключей. Такое решение должно исключать и возможность подмены сервера (фишинг) финансовых услуг и его защиту от НСД, и возможность подмены пользователя.

Для организации подобных решений необходимо применение строгой двухфакторной аутентификации, решений по разграничению доступа (каждый пользователь, в том числе администратор, имеет доступ только к необходимой ему, согласно занимаемой должности, информации), защите доступа (доступ к данным может получить пользователь, прошедший процедуру аутентификации), шифрованию данных (шифровать необходимо как передаваемые в сети данные для защиты от перехвата, так и данные, записываемые на носитель, для защиты от кражи носителя и от несанкционированного просмотра / изменения нештатными средствами системы управления БД) и аудиту доступа к данным (действия с критичными данными должны протоколироваться; доступ к протоколу не должны иметь пользователи, на которых он ведется). Данный подход позволяет персонифицировать действия пользователей и ввести понятие неотказуемости от совершенных действий. Это может стать основой профилактики правонарушений, в частности, послужить эффективным средством для предотвращения такого распространенного явления, как инсайдерские кражи баз данных.

ЗАКЛЮЧЕНИЕ

Использование компьютеров и автоматизированных технологий сейчас приводит к появлению ряда проблем для руководства организацией. Компьютеры, часто объединенные в сети, могут предоставлять доступ к колоссальному количеству самых разнообразных данных. Поэтому люди беспокоятся о безопасности информации и наличии рисков, связанных с автоматизацией и предоставлением гораздо большего доступа к конфиденциальным, персональным или другим критическим данным. Все увеличивается число компьютерных преступлений, что может привести, в конечном счете, к подрыву экономики. И поэтому должно быть ясно, что информация - это ресурс, который надо защищать.

Ответственность за защиту информации лежит на низшем звене руководства. Но также кто-то должен осуществлять общее руководство этой деятельностью, поэтому в организации должно иметься лицо в верхнем звене руководства, отвечающее за поддержание работоспособности информационных систем.

И так как автоматизация привела к тому, что теперь операции с вычислительной техникой выполняются простыми служащими организации, а не специально подготовленным техническим персоналом, нужно, чтобы конечные пользователи знали о своей ответственности за защиту информации.

Единого рецепта, обеспечивающего 100% гарантии сохранности данных и надёжной работы сети не существует. Однако создание комплексной, продуманной концепции безопасности, учитывающей специфику задач конкретной организации, поможет свести риск потери ценнейшей информации к минимуму.

СПИСОК ЛИТЕРАТУРЫ

1. Газета «Коммерсантъ» №58 (4113) от 02.04.2009
2. Журнал «Мир связи» 11/2008. Алексей Сабанов. Актуальные задачи аутентификации.
3. Тютюнник А.В., Шевелев А.С. Информационные технологии в банке – Издательская группа «БДЦ-пресс». – 2003 г.
4. Киселева И.А. Коммерческие банки: модели и информационные технологи в процедурах принятия решений. – М.: Едиториал УРСС, 2002. – 400 с.
5. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. – М.: Академический Проект; Гаудеамус, 2-е изд. – 2004. – 544 с.
6. Мельников В.П. Информационная безопасность и защита информации: учеб. пособие для студ. высш. учеб. заведений. – 3-е изд., стер. – М.: Издательский

центр «Академия», 2008. – 336 с.
7. Курило А.П., Зефиров С.Л., Голованов В.Б и др. Аудит информационной безопасности. – М.: Издательская группа «БДЦ-пресс», 2006. – 304 с.
8. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий [Текст]: РД: утв. Гостехкомиссией России. – М., 2002.
9. ГОСТ Р 51275–99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию [Текст]. – Введ. 2000–01–01 – М.: Изд-во стандартов, 1999. – 8 с.
10. ГОСТ Р 50922–96. Защита информации. Основные термины и определения [Текст]. М.: Изд-во стандартов, 1996.
11. ГОСТ Р 51624–2000. [Текст]. М.: Изд-во стандартов, 2000.
12. Автоматизированные системы. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации [Текст]: РД: утв. Гостехкомиссией России. – М.: Изд-во стандартов, 1992.
13. Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации [Текст]: РД: утв. Гостехкомиссией России. – М.: Изд-во стандартов, 1992.
14. Защита от несанкционированного доступа к информации. Термины и определения [Текст]: РД: утв. Гостехкомиссией России. – М.: Изд-во стандартов, 1992.
15. ГОСТ Р 15408–02. Критерии оценки безопасности информационных технологий [Текст]. – Введ. 2004–01–01 – М.: Изд-во стандартов, 2002.
16. ISO/IEC 17799:2000. Информационные технологии. Свод правил по управлению защитой информации. Международный стандарт [Текст] / ISO/IEC, 2000.
17. Девянин П.Н. Теоретические основы компьютерной безопасности [Текст]: учеб. пособие для вузов / П.Н. Девянин, О.О. Михальский, Д.И. Правиков, А.Ю. Щербаков. – М.: Радио и связь, 2000. – 192 с.
18. Ресурсы Microsoft Windows NT Workstation 4.0 [Текст]: [пер. с англ.] / Корпорация Майкорософт. – СПб.: BHV – Санкт-Петербург, 1998. – 800 с.: ил.; 28 см. + 1 электрон. опт. диск. – Перевод изд.: Microsoft Windows NT Workstation 4.0 Resource Kit / Microsoft Corporation, 1996.