

УДК 343.77(477)
ББК 67.408.12

С.П. Евсеев,
кандидат технических наук,
Харьковский национальный экономический университет
А.В. Дорохов,
кандидат технических наук, доцент,
Харьковский национальный экономический университет

ИНФОРМАЦИОННЫЕ УГРОЗЫ И БЕЗОПАСНОСТЬ В БАНКОВСКИХ ПЛАТЕЖНЫХ СИСТЕМАХ УКРАИНЫ

Рассмотрены основные элементы автоматизированных банковских систем коммерческих банков Украины, перспективы развития автоматизированных банковских систем, проанализированы статистические данные роста денежного товарооборота через банковские системы, исследованы возможные угрозы целостности, сохранности и конфиденциальности информации в них, а также основные механизмы обеспечения информационной безопасности в автоматизированных банковских системах на основе международных и внутригосударственных стандартов.

Ключевые слова: автоматизированная банковская система; утечка закрытой информации; информационная безопасность.

S.P. Yevseyev,
Ph.D. in Technical Sciences,
Kharkov National University of Economics
A.V. Dorokhov,
Ph.D. in Technical Sciences,
Kharkov National University of Economics

INFORMATION THREATS AND SAFETY IN UKRAINIAN BANK PAYMENT SYSTEMS

The paper considers key elements of automated banking systems of Ukrainian commercial banks and the prospects of automated banking systems' development; it analyses statistical data of money circulation through banking systems, studies possible threats to integrity, security and confidentiality of information contained in them as well as key mechanisms of ensuring information safety in automated banking systems on the basis of international and national standards.

Key words: automated banking system; confidential information leak; information safety.

Развитие информационных технологий, глобальной сети Интернет, а также стремительный рост вычислительных возможностей компьютерных систем, наращивание объемов обрабатываемых данных в современных автоматизированных банковских системах (АБС), появление новых форм электронных услуг, предлагаемых АБС, – все эти факторы в совокупности выдвигают новые требования к надежности и обеспечению безопасности во внутриплатежных системах (ВПС). Тем не менее сегодня не существует научно обоснованной концепции и механизмов обеспечения финансовой безопасности банковской деятельности национальной платежной системы.

Что представляет собой современная автоматизированная банковская система? Это совокупность правил, организационных мероприятий, программно-технических средств,

средств защиты, используемых банком для выполнения внутрибанковского перевода денег, а также для взаимодействия с другими банковскими платежными системами для обеспечения выполнения межбанковского перевода денег филиалами банка [1]. Данная система относится к многоуровневым критическим системам, так как ее отказ, отступление от задаваемых ограничений либо изменения в работе подсистемы могут повлечь за собой серьезные последствия либо привести к краху всей системы в целом. Проведенный анализ [1–5] показал, что, несмотря на мировой экономический кризис, банковские учреждения во всем мире на основе новых вычислительных возможностей продолжают наращивать сферу услуг через сети банкоматов и POS-терминалов. Так, с 2004 по 2009 г. число банкоматов в мире увеличилось

в 1,5 раза, аналогичная тенденция характерна и для Украины.

Основными направлениями развития этого вида услуг ВПС являются дальнейшее наращивание сети банкоматов, введение новых услуг оплаты через *i*-боксы, развитие электронного банкинга и рост продаж товаров населению через интернет-магазины, что подтверждается ростом транзакций через сети удаленного доступа ВПС. Если в Украине в 2004 г. количество транзакций составляло 295 млн, то в 2009-м – уже 513 млн, а сумма снятия наличных средств увеличилась за тот же период с 70 до 335 млрд в год [10].

Как правило, АБС состоят из следующих структурно-функциональных элементов:

- рабочих станций – отдельных ЭВМ или удаленных терминалов сети, на которых реализуются автоматизированные рабочие места пользователей (абонентов, операторов);

- серверов или Host-машин (служб файлов, печати, баз данных и т. п.), не выделенных или выделенных, т. е. не совмещенных с рабочими станциями высокопроизводительных ЭВМ, предназначенных для реализации функций хранения, печати данных, обслуживания рабочих станций сети и других действий;

- межсетевых мостов (шлюзов, центров коммутации пакетов, коммуникационных ЭВМ) – элементов, обеспечивающих соединение нескольких сетей передачи данных либо нескольких сегментов одной и той же сети, имеющих различные протоколы взаимодействия;

- каналов связи (локальных, телефонных, с узлами коммутации и т. д.).

Рабочие станции являются наиболее доступными компонентами сетей, и именно с них могут быть предприняты наиболее многочисленные попытки совершения несанкционированных действий. С рабочих станций осуществляется управление процессами обработки банковских транзакций, запуск программ, ввод и корректировка данных, на дисках рабочих станций могут размещаться важные данные и программы обработки. На видеомониторы и печатающие устройства рабочих станций выводится информация при работе пользователей (операторов), выполняющих различные функции и имеющих разные полномочия по доступу к данным и другим ресурсам системы.

Именно поэтому рабочие станции должны быть надежно защищены от доступа

посторонних лиц и содержать средства разграничения доступа к ресурсам со стороны законных пользователей, имеющих разные полномочия. Кроме того, средства защиты должны предотвращать нарушения нормальной настройки рабочих станций и режимов их функционирования, вызванные неумышленным вмешательством неопытных (невнимательных) пользователей [3, с. 48–54].

В особой защите нуждаются особенно привлекательные для злоумышленников элементы сетей, такие как *серверы* (Host-машины) и *мосты*. Первые – как концентраторы больших объемов информации, вторые – как элементы, в которых осуществляется преобразование (возможно, через открытую, нешифрованную форму представления) данных при согласовании протоколов обмена в различных участках сети.

Для повышения безопасности серверов и мостов благоприятным обстоятельством является наличие возможностей по их надежной защите физическими средствами и организационными мерами, позволяющими сократить до минимума число лиц, имеющих непосредственный доступ к ним. *Каналы и средства связи* в силу своей большой пространственной протяженности (через неконтролируемую или слабо контролируемую территорию) практически всегда подвержены угрозам подключения к ним либо вмешательства в процесс передачи данных.

На рис. 1 представлена классификация причин возникновения основных угроз для внутриплатежных систем коммерческого банка.

Основным объектом атак является персональная информация пользователей (имена, пароли, аккаунты, идентификационные номера, банковские реквизиты, данные о корпоративных сетях). Атаки компьютерных злоумышленников направлены на сбор таких сведений в обход многоуровневых систем защиты от вторжений.

Рассматривая систематизацию аппаратно-программных средств защиты информации в АБС, обычно выделяют следующие подсистемы:

- автоматизированное рабочее место (АРМ) клиентов узла электронных платежей (ЭП);

- АРМ администратора (включающее средства хранения информации, системный блок, средства ввода информации, общесистемное и прикладное программное обеспечение);

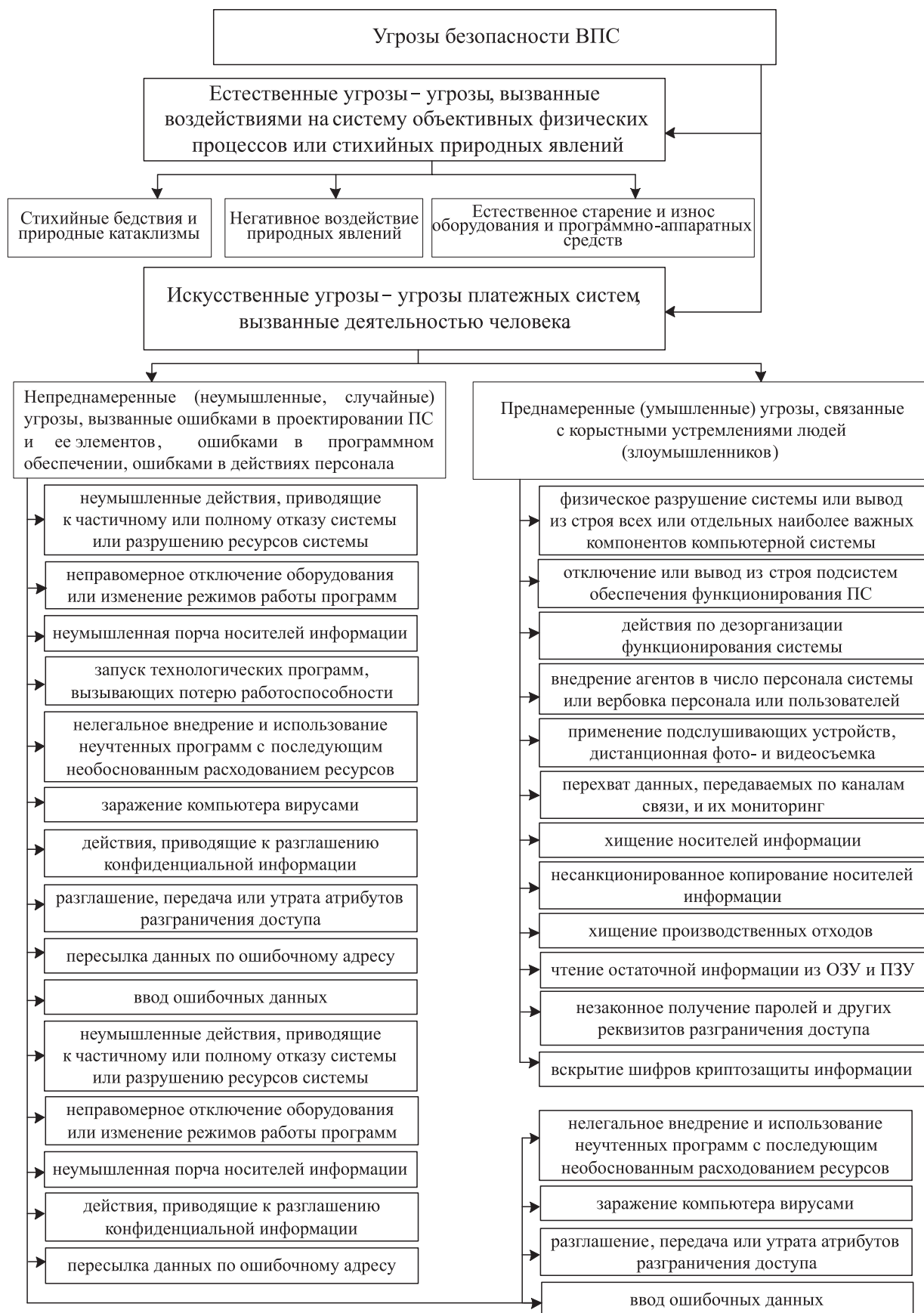


Рис. 1. Классификация причин основных угроз для внутриплатежных систем

– сервер ЭП системы (включающий средства хранения информации, программное обеспечение сервера, средства ввода-вывода информации, системы управления базами данных);

– система передачи данных (включает технические средства каналов связи и специальное программное обеспечение).

С другой стороны, виды угроз также можно разделить на:

– угрозы, обусловленные действиями субъекта (кража информации, ее неправомерная модификация или уничтожение-разрушение, нарушение нормальной работы, инспирированные извне ошибки работы программного обеспечения, перехват информации при подключении к каналам связи, навязывание ложной информации);

– угрозы от стихийных источников (нарушение нормальной работы, уничтожение-разрушение, искажение информации);

– технические угрозы (уничтожение-исчезновение информации).

Проведенный анализ показал, что внутренние угрозы являются одной из наиболее актуальных проблем информационной безопасности. Согласно статистике неправомерные действия сотрудников и обслуживающего персонала организаций причиняют наибольший ущерб, и до 90 % средств, выделяемых на информационную безопасность, тратится на обеспечение защиты от внутренних атак [6]. Неправомерные действия пользователей приводят к значительному ущербу. Они подразделяются на нарушение конфи-

денциальности данных; кражу информации; искажение информации; действия, приводящие к сбоям информационных систем; утрату информации.

Лидирующую позицию занимают нарушения конфиденциальности данных, приводящие к утечке закрытой информации. По сведениям специалистов [7], из 100 случаев неправомерных действий сотрудников-инсайдеров (под «инсайдером» понимается санкционированный пользователь, допущенный к обработке информации на вычислительном средстве в рамках выполнения своих служебных обязанностей) 65 относятся к нарушению конфиденциальности данных. Цели и мотивы инсайдеров представлены на рис. 2.

Таким образом, инсайдер может нанести непоправимый ущерб не только самой компании (коммерческому банку), но и АБС в целом, что может привести к разрушению всей АБС и, соответственно, к полному недоверию клиентов банка.

Развитие IT-технологий позволяет злоумышленникам осваивать новые направления видов атак. Сегодня они используют такие методы изъятия данных аутентификации, как фишинг и фарминг, добиваясь того, чтобы пользователь АБС «поделится» конфиденциальными данными с заинтересованными лицами, причем так, что сам он даже не будет подозревать об этом до тех пор, пока с его счета не исчезнет некоторая сумма денег.

Суть обеих атак заключается в том, что пользователь вводит свои данные аутен-

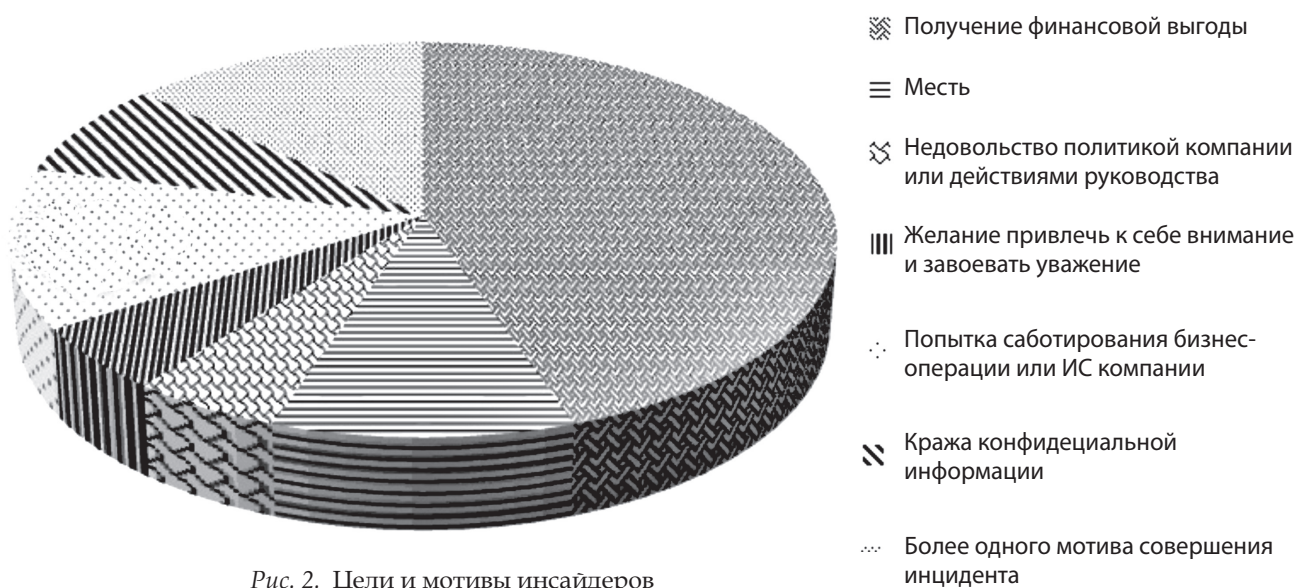


Рис. 2. Цели и мотивы инсайдеров

Таблица 1

Время, необходимое для перебора половины ключей суперкомпьютерами

Страна – владелец суперЭВМ	Длина ключа, бит / время взлома					
	56 бит	64 бит	70 бит	75 бит	90 бит	256 бит
	Время взлома, мин	Время взлома, часов	Время взлома, суток	Время взлома, лет	Время взлома, лет	Время взлома, лет
США	0,0537	0,224	0,611	0,0536	1760	1,15E+53
Япония	1,15	4,78	13,1	1,15	37600	2,46E+54
Германия	0,746	3,11	8,50	0,746	17300	1,60E+54
Великобритания	0,651	2,71	7,41	0,650	15100	1,40E+54
Франция	0,677	2,82	7,70	0,676	15600	1,45E+54

тификации не на web-странице АБС, а на фальшивой странице, визуально полностью похожей на нее. С фальшивой страницы данные попадают к злоумышленникам, что позволяет им пройти аутентификацию в АБС от имени пользователя со всеми вытекающими последствиями – вплоть до обнуления счета.

Разница между этими атаками заключается лишь в способе попадания пользователя на фальшивую страницу. В первом случае используется спам-рассылка от имени АБС, в которой пользователю предлагается посетить АБС, указывая при этом адрес фальшивой страницы. Во втором – предполагается переадресация на хакерский web-сайт, что становится возможным за счет уязвимостей браузеров, операционных систем или DNS-атак. Кроме того, не стоит забывать о троянском программном обеспечении, которое успешно «ворует» данные.

При этом АБС содержат информационные разделы, описывающие правила безопасного выполнения финансовых интернет-операций: ручной ввод адресов в АБС, работа только по защищенному протоколу, проверка и использование антивирусов и т. д. Кроме того, практически во всех случаях дополнительно указывается, что данная платежная система никогда не рассылает письма с предложением посетить АБС, и все рассылки, если таковые имеют место быть, персонализированы. Однако проблема заключается в том, что эти правила в подавляющем большинстве игнорируются пользователями, что и делает возможным осуществление описанных выше атак [6]. Для предотвращения возможных угроз необходимо не только обеспечить защиту

операционных систем, программного обеспечения и контроль доступа, но и выявить категории нарушителей и те методы, которые они используют.

Учитывая особенности распределенных систем, а также уязвимые структурно-функциональные элементы АБС, можно сформулировать условия для организации эффективных атак:

- наличие больших вычислительных ресурсов, что позволяет производить взлом криптографических преобразований в АБС, что может достигаться за счет привлечения суперкомпьютеров, а также систем распределенных вычислений;

- наличие большого количества управляемых компьютеров сети Интернет, что позволяет проводить массовые атаки на публичные ресурсы ВПС за счет привлечения систем распределенных вычислений.

На сегодня существует мировой рейтинг суперкомпьютеров Top 500 [9]. В табл. 1 приведены результаты анализа среднего времени реализации атаки для перебора половины ключей суперкомпьютерами определенной страны.

Приведенные результаты показывают, что при использовании симметричных алгоритмов шифрования (стойкость которых основывается на стойкости ключа) взлом при длине ключа 56 бит составляет от 0,0537 до 1,15 мин (см. первую колонку табл. 1), что приводит к мгновенному взлому системы защиты и потере денежных средств АБС. Учитывая это, в стандартах симметричных алгоритмов шифрования установлены минимальные размеры ключей – 128, 256 и 512 бит, что обеспечивает временную стойкость данных криптосистем.

Таблица 2

Время, необходимое для перебора половины ключей суперкомпьютерами

Название супер-компьютера	Длина ключа, бит / время взлома					
	56 бит, время взлома, мин	64 бит, время взлома, часов	70 бит, время взлома, суток	75 бит, время взлома, лет	90 бит, время взлома, лет	256 бит, время взлома, лет
Roadrunner - BladeCenter QS22	0,543	2,26	6,18	0,542	17800	1,16E+54
Jaguar - Cray XT5 QC	0,567	2,36	6,45	0,566	18600	1,22E+54
Pleiades - SGI Altix ICE 8200EX	1,23	5,13	14	1,23	28500	2,64E+54
BlueGene/L - eServer Blue Gene Solution	1,26	5,23	14,3	1,25	29000	2,69E+54
Blue Gene/P Solution	1,33	5,56	15,2	1,33	30800	2,86E+54

В табл. 2 приведены результаты оценки необходимого времени для перебора половины ключей для пяти лучших суперкомпьютеров.

В соответствии с международными стандартами для обеспечения требуемых показателей безопасности, основа которых – криптографические методы преобразования информации, определены пять базовых общепринятых услуг:

- аутентификация объекта и источника данных;
- конфиденциальность данных (установления соединения, трафика передачи данных, выделенного поля данных);
- целостность данных (возможность соединения с восстановлением данных при прерывании связи и без него, целостность данных во время соединения);
- управление доступом;
- принадлежность (подтверждение получения-отправки сообщений при обмене ими).

Этим услугам соответствуют базовые механизмы безопасности: управление доступом, шифрование, цифровые подписи, обеспечение целостности данных, аутентификацию участников обмена информацией, контроль трафика и управление маршрутизацией.

Следует отметить, что основные механизмы обеспечения целостности и аутен-

тичности информации в АБС Украины на различных уровнях основаны на использовании устаревших стандартов блочно-симметричных шифров (БСШ). На рис. 3 приведена взаимосвязь между механизмами и применяемыми стандартами в подсистеме безопасности АБС.

Таким образом, проведенные исследования показали, что дальнейшее развитие вычислительных и IT-технологий приводит не только к увеличению роста денежного оборота через банкоматы и другие системы удаленного пользования АБС, расширению услуг, предоставляемых через глобальную сеть Интернет населению, но и к модернизации существующих, а также появлению новых видов угроз на элементы АБС.

Для обеспечения безопасности банковской информации в ВПС используются криптографические симметричные и асимметричные алгоритмы шифрования, прошедшие стандартизацию и сертификацию на государственном уровне. Однако отсутствие национальных стандартов по специальным механизмам обеспечения информационной безопасности АБС (шифрование, ЦП, целостность данных, аутентификация) существенно влияет на уровень обеспечения информационной безопасности банковских транзакций и надежности АБС в целом.

УСЛУГИ И МЕХАНИЗМЫ БЕЗОПАСНОСТИ В АБС

КОНФИДЕНЦИАЛЬНОСТЬ ДАННЫХ

соединения

без установления
соединения

выделенного поля данных

трафика

АУТЕНТИФИКАЦИЯ

аутентификация объекта

аутентификация источника

ЦЕЛОСТНОСТЬ ДАННЫХ

соединения без
восстановления

соединения с
восстановлением

выделенного поля без
установления соединения

выделенного поля с
установлением соединения

блока данных без
соединения

ПРИМЕНЯЕМЫЕ СТАНДАРТЫ В АБС УКРАИНЫ

БСШ (ГОСТ 28147-89). Алгоритм криптографического преобразования

в режимах простой замены, гаммирования и
гаммирования с обратной связью для областей
памяти и файлов

формирования имитовставки длиной
32 бит

Функция хеширования на основе БСШ;
Процедура выработки и проверки ЦП;
Алгоритм Диффи-Хеллмана; генерация сеансовых
ключей на основе стандарта X9.17

Хеширование, формирование системных
параметров, вычисление и проверка ЦП

БСШ (ГОСТ 28147-89);

DDC (Diebold Direct Connect – для
банкоматов Diebold и Wincor Nixdorf);
NDC (NCR Direct Connect – для банкоматов
NCR и Wincor Nixdorf).

Протокол Triple DES

формирования имитовставки длиной
32 бит, в режимах простой замены,
гаммирования и гаммирования с обратной
связью для областей памяти и файлов

сетевые протоколы сообщений с
авторизованными серверами

шифрование запроса на снятие наличных

Рис. 3. Взаимосвязь механизмов и стандартов информационной безопасности в автоматизированных банковских системах Украины

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Артеменко Д.А. Механизм обеспечения финансовой безопасности банковской деятельности : дис. ... канд. экон. наук. – Ростов н/Д, 1999. – 190 с.
2. Гайкович В.Ю., Першин А.Ю. Безопасность электронных банковских систем. – М., 1994. – 363 с.
3. Логинов А.А., Елхимов Н.С. Общие принципы функционирования электронных платежных систем и осуществление мер безопасности при защите от злоупотребления и мошенничества // Конфидент. – 1995. – № 4. – С. 48–54.

4. Межбанковские расчеты на Украине [Электронный ресурс]. — URL: http://e2000.kyiv.org/biblioteka/biblio/stat/ukr_bank.html
5. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях / под ред. В.Ф. Шаньгина. — 2-е изд., перераб. и доп. — М., 2001. — 376 с.
6. Шеглов А.Ю. Как защищать конфиденциальную информацию и персональные данные в современных условиях? [Электронный ресурс]. — URL: www.bankir.ru
7. [Электронный ресурс]. — URL: http://www.cartelblanche-online.info/index.php?option=com_content&task=view&id=105
8. [Электронный ресурс]. — URL: <http://www.cryptopro.ru/cryptopro/documentation/dig-cert.htm>
9. [Электронный ресурс]. — URL: <http://www.youtube.com/watch?v=8iSRLIK-x6A>
10. Retail Banking Research: ATMs and Cash Dispensers Central & Eastern Europe 2010 [Электронный ресурс]. — URL: http://www.rbrlondon.com/reports/ATM_CEE10_Brochure.pdf

REFERENCES

1. Artemenko D.A. *Mekhanizm obespecheniya finansovoy bezopasnosti bankovskoy deyatel'nosti (avto-ref. kand. dis.)* [Mechanism of Providing Financial Safety of Banking Activities (Cand. Dis. Thesis)]. Rostov-on-Don, 1999, 190 p.
2. Gaykovich V.Yu., Pershin A.Yu. *Bezopasnost' elektronnykh bankovskikh system* [Safety of Electronic Banking Systems]. Moscow, 1994, 363 p.
3. Loginov A.A., Elkhimov N.S. *Konfident* [Confidant]. 1995, no. 4, pp. 48–54.
4. *Mezhhbankovskie raschety na Ukraine* [Interbank Accounts in Ukraine]. Available at: http://e2000.kyiv.org/biblioteka/biblio/stat/ukr_bank.html
5. Romanets Yu.V., Timofeev P.A., Shan'gin V.F. *Zashchita informatsii v komp'yuternykh sistemakh i setyakh* [Information Protection in Computer Systems and Networks]. Moscow, 2001, 376 p.
6. Shsheglov A.Yu. *Kak zashchishchat' konfidentsial'nuyu informatsiyu i personal'nye dannye v sovremennykh usloviyakh?* [How to Protect Confidential Information and Personal Data in Modern Conditions?]. Available at: www.bankir.ru
7. http://www.cartelblanche-online.info/index.php?option=com_content&task=view&id=105
8. <http://www.cryptopro.ru/cryptopro/documentation/dig-cert.htm>
9. <http://www.youtube.com/watch?v=8iSRLIK-x6A>
10. Retail Banking Research: ATMs and Cash Dispensers Central & Eastern Europe 2010. Available at: http://www.rbrlondon.com/reports/ATM_CEE10_Brochure.pdf

Информация об авторах

Евсеев Сергей Петрович (Украина, Харьков) — кандидат технических наук, старший научный сотрудник, доцент кафедры информационных систем. Харьковский национальный экономический университет (61001, Украина, Харьков, проспект Ленина, 9а, e-mail: aleks.dorokhov@meta.ua)

Дорохов Александр Васильевич (Украина, Харьков) — кандидат технических наук, доцент, доцент кафедры информационных систем. Харьковский национальный экономический университет (61001, Украина, Харьков, проспект Ленина, 9а, e-mail: aleks.dorokhov@meta.ua)

Information about the authors

Yevseyev, Sergey Petrovich (Kharkov, Ukraine) — Ph.D. in Technical Sciences, Chief Researcher, Ass. Professor, Chair of Information Systems. Kharkov National University of Economics (Lenin prospect, 9a, Kharkov, 61001, Ukraine, e-mail: aleks.dorokhov@meta.ua)

Dorokhov, Aleksandr Vasilyevich (Kharkov, Ukraine) — Ph.D. in Technical Sciences, Ass. Professor, Chair of Information Systems. Kharkov National University of Economics (Lenin prospect, 9a, Kharkov, 61001, Ukraine, e-mail: aleks.dorokhov@meta.ua)