УДК 336.717:004.78

**С.П. Евсеев,**
**О.Г. Король,**
**Н.С. Суханова**

# АНАЛИЗ УГРОЗ И МЕХАНИЗМОВ ЗАЩИТЫ ВО ВНУТРИПЛАТЕЖНЫХ СИСТЕМАХ КОММЕРЧЕСКОГО БАНКА

*Здійснюється аналіз внутрішніх платіжних систем комерційного банку (ВПС), можливих загроз на ВПС, розглядаються основні механізми забезпечення безпеки конфіденційної інформації у ВПС (забезпечення аутентичності, цілісності банківської інформації).*

***Ключові слова:*** *внутрішні платіжні системи комерційного банку, конфіденційна інформація, механізми захисту.*

*Проводится анализ внутриплатежных систем коммерческого банка (ВПС), возможных угроз на ВПС, рассматриваются основные механизмы обеспечения безопасности конфиденциальной информации в ВПС (обеспечения аутентичности, целостности банковской информации).*

***Ключевые слова:*** *внутриплатежные системы коммерческого банка, конфиденциальная информация, механизмы защиты.*

*The analysis of intrapayment systems of commercial ban (WPS) , possible threats for them is carried out, basic mechanisms of safety of the confidential information in of intrapayment systems of commercial bank (maintenance of authenticity, integrity of the bank information) are considered.*

***Keywords:*** *intrapayment systems of commercial bank, confidential information, mechanisms of safety.*

Развитие высокорентабельной экономики невозможно без внедрения современной системы денежного обращения и использования эффективных платежных механизмов. Быстрый рост объемов обрабатываемых данных в современных ВПС, появление новых форм электронных услуг, стремительное развитие вычислительной техники выдвигают новые требования к надежности и обеспечению безопасности в ВПС.

Тем не менее, на сегодняшний день не существует научно-обоснованной концепции и механизмов обеспечения финансовой безопасности банковской деятельности национальной платежной системы в целом [2]. Проведенный анализ работ в данном направлении показал, что проблемными вопросами в открытых системах, в том числе и ВПС являются вопросы обеспечения аутентичности и целостности конфиденциальной информации [2–4; 15; 16].

Известным приемом в построении современных механизмов аутентификации является использование стойких криптопримитивов, примером являются схемы UMAC, TTMAC, HMAC и др. Подход, используемый в данных схемах, позволил свести стойкость схем аутентификации к стойкости используемого алгоритма

(DES, TDES, AES), что также не решило возникшей проблемы. Следовательно, современной и востребованной задачей позволяющей решить существующие противоречия при выборе механизмов аутентификации и оценки их стойкости является проведение анализа криптографической стойкости существующих криптопримитивов и разработка рекомендаций по обоснованию стойкости современных систем аутентификации.

Целью статьи является рассмотрение внутриплатежных систем коммерческого банка (ВПС), возможных угроз, анализ основных механизмов обеспечения безопасности конфиденциальной информации в ВПС (обеспечения аутентичности, целостности банковской информации).

***1. Анализ внутриплатежных систем коммерческого банка.***

*Национальная платежная система* – сложная многоуровневая система централизованного управления, обеспечивающая качественный стратегически важный канал проведения финансовых транзакций [1].

Такая система относится к сложным многоуровневым системам управления критического применения (СУКП), в которых передача информации требует контроля безопасности на каждом уровне. Важной составной частью ВПС, предназначенной для обеспечения услуг безопасности, является подсистема криптографической безопасности информации, которая реализуется соответствующими протоколами и механизмами безопасности. Структурная схема СУКП национальной платежной системы представлена на рис. 1.

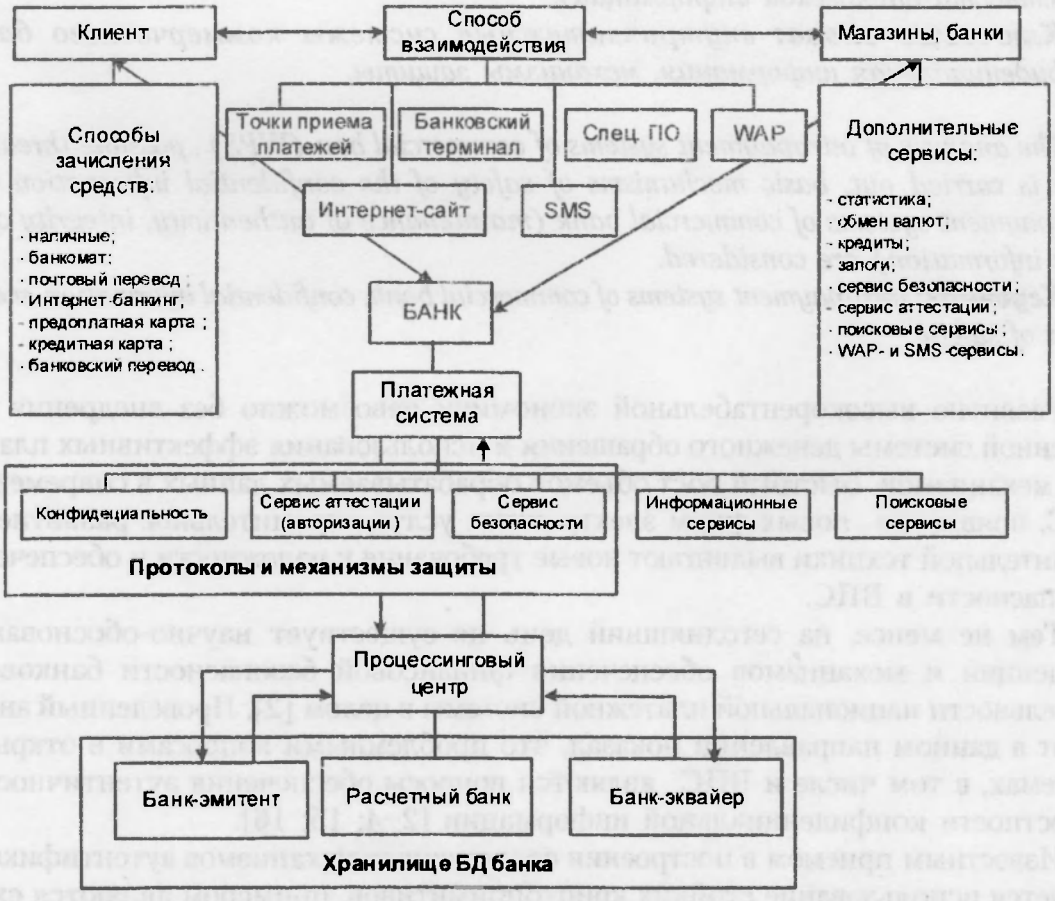


Рис. 1. Структурная схема национальной платежной системы

Проведенный анализ показал [2–5; 16], 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. На рис. 2 приведена диаграмма роста числа банкоматов в мире, на рис. 3 – в Украине [17].


Рис. 2. Рост числа банкоматов в мире

Основными направлениями развития этого вида услуг ВПС является дальнейшее наращивание сети банкоматов, введение новых услуг оплаты через і-боксы, развитие электронного банкинга и рост продаж товаров населению через интернет-магазины, что подтверждается ростом транзакций через сети удаленного доступа ВПС, на рис. 4 представлены результаты анализа денежного товарооборота через банкоматы ВПС Украины [17].


Рис. 4. Рост товарооборота через банкоматы в Украине

Таким образом, проведенный анализ показал, что ВПС, на основе достижений коммуникационных и IT-технологий успешно развивают свои функции по услугам оплаты через сети банкоматов и удаленных пользователей, продаже товаров через интернет-магазины и т.д.

***2. Анализ угроз информационной безопасности в банковской сфере.***

Развитие информационных технологий, глобальной сети Интернет, а также события (военные конфликты, террористические акты) последних лет, показали необходимость обеспечения информационной безопасности страны в целом и ее граждан в частности. Таким образом, обеспечение безопасности ВПС, сети связи финансово-кредитной и банковской сфер выносится на национальный уровень, что свидетельствует о степени важности данного вопроса.

Развитие и укрепление банковской системы Украины (БСУ), а также обеспечение эффективного и бесперебойного функционирования платежной системы Украины являются целями деятельности национального Банка Украины (НБУ).

Важнейшим условием реализации этих целей является обеспечение необходимого и достаточного уровня информационной безопасности (ИБ) организаций БСУ, их активов (в т. ч. информационных), который во многом определяется уровнем информационной безопасности банковских технологических процессов (платежных, информационных и пр.), автоматизированных банковских систем (АБС), эксплуатирующихся организациями БСУ, и т. д.

Особенности банковских систем таковы, что негативные последствия сбоев в работе отдельных организаций могут привести к быстрому развитию системного кризиса платежной системы Украины, нанести ущерб интересам собственников и клиентов, тем самым разрушить всю ВПС. В случаях наступления инцидентов ИБ значительно возрастают результирующий риск и возможность нанесения ущерба организациям БСУ. Поэтому для организаций БСУ угрозы информационным активам, то есть угрозы ИБ, представляют реальную опасность.

Для противостояния таким угрозам и обеспечения эффективности мероприятий по ликвидации неблагоприятных последствий инцидентов ИБ (их влияния на операционные, кредитные и иные риски) в организациях БСУ следует обеспечить достаточный уровень ИБ. Необходимо также сохранить этот уровень в течение длительного времени. По этим причинам обеспечение ИБ является для организаций БСУ одним из основополагающих аспектов их деятельности [7; 15; 16].

В общем случае АБС состоят из следующих основных 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, то есть не совмещенных с рабочими станциями) высокопроизводитслыых ЭВМ, предназначенных для реализации функций

хранения, печати данных, обслуживания рабочих станций сети и т. п. 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 [16; 21].

В особой защите нуждаются "привлекательные" для злоумышленников элементы сетей 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.

Благоприятным для повышения безопасности серверов и мостов обстоятельством является, как правило, 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. 5. представлена классификация основных угроз на внутриплатежные системы коммерческого банка. Это угрозы *финансовым ресурсам* – персональная информация пользователей (имена, пароли, аккаунты, идентификационные номера, банковские реквизиты, данные о корпоративных сетях). Атаки направлены на сбор сведений в обход многоуровневых систем защиты от вторжений. А также угрозы *информационных ресурсов*, которые подразделяются на внешние (технические) и внутренние (неправомерные действия сотрудников). Проведенный анализ основных угроз показал, что дальнейшее развитие вычислительных возможностей и IT-технологий позволяет "модерни-

зировать" виды угроз, создавать новые современные технологии взлома систем безопасности ВПС.

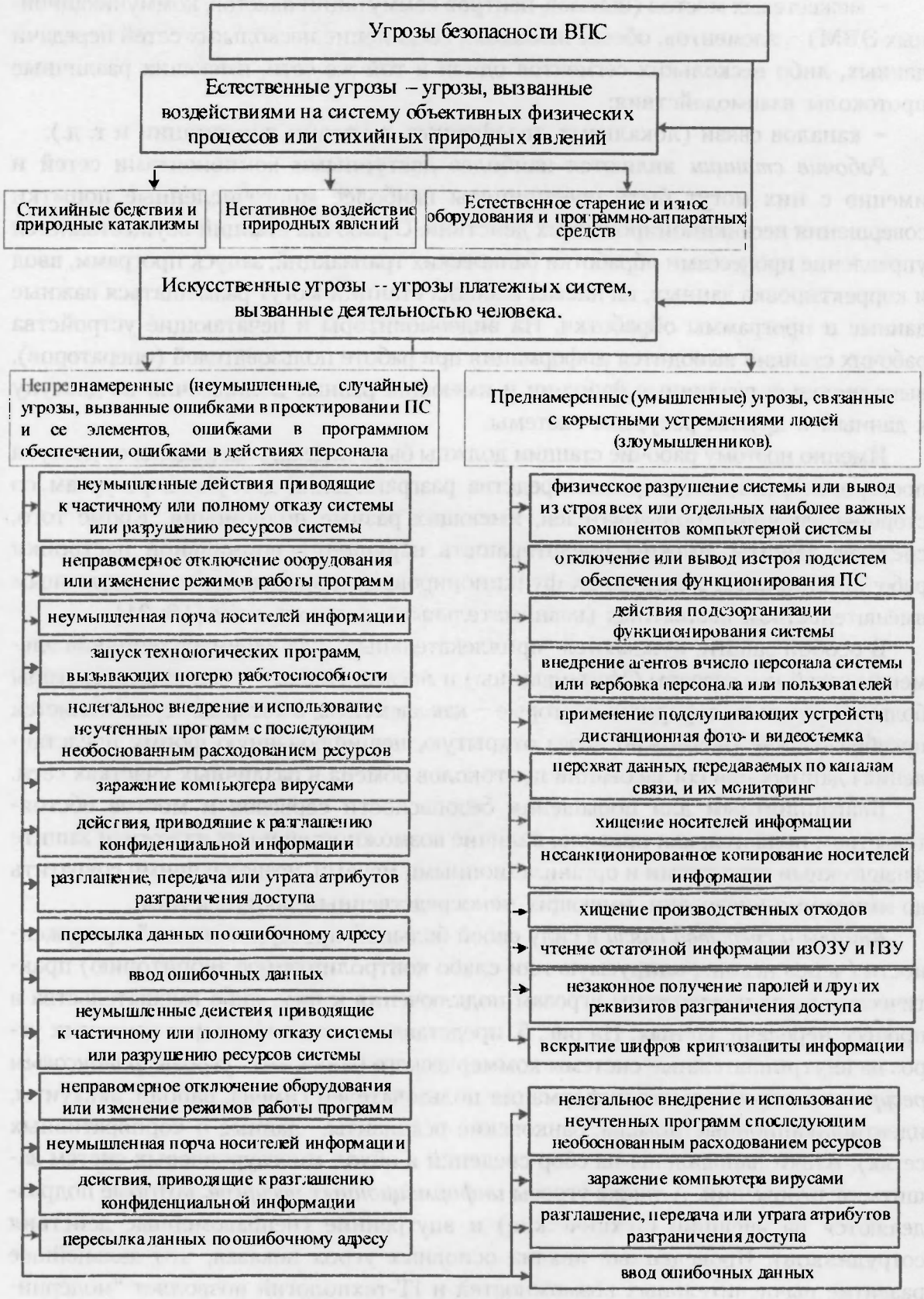


Рис. 5. Классификация основных угроз на ВПС

На рис. 6 представлены результаты анализа возможности несанкционированного доступа в элементы подсистем ВПС на основе реализации соответствующих угроз.


Рис. 6. Анализ возможности несанкционированного доступа в элементы ВПС на основе реализации соответствующих угроз

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 [7; 15]. Неправомерные действия пользователей приводят к значительному ущербу:

– нарушение конфиденциальности данных;
– кража информации;
– искажение информации;
– действия, приводящие к сбоям информационных систем;
– утрата информации.

Лидирующую позицию занимают нарушения конфиденциальности данных, приводящие к утечке закрытой информации. По сведениям специалистов [6; 21], из 100 случаев неправомерных действий сотрудников 65 относятся к нарушению конфиденциальности данных, диаграмма распределения внутренних угроз представлена на рис. 6.

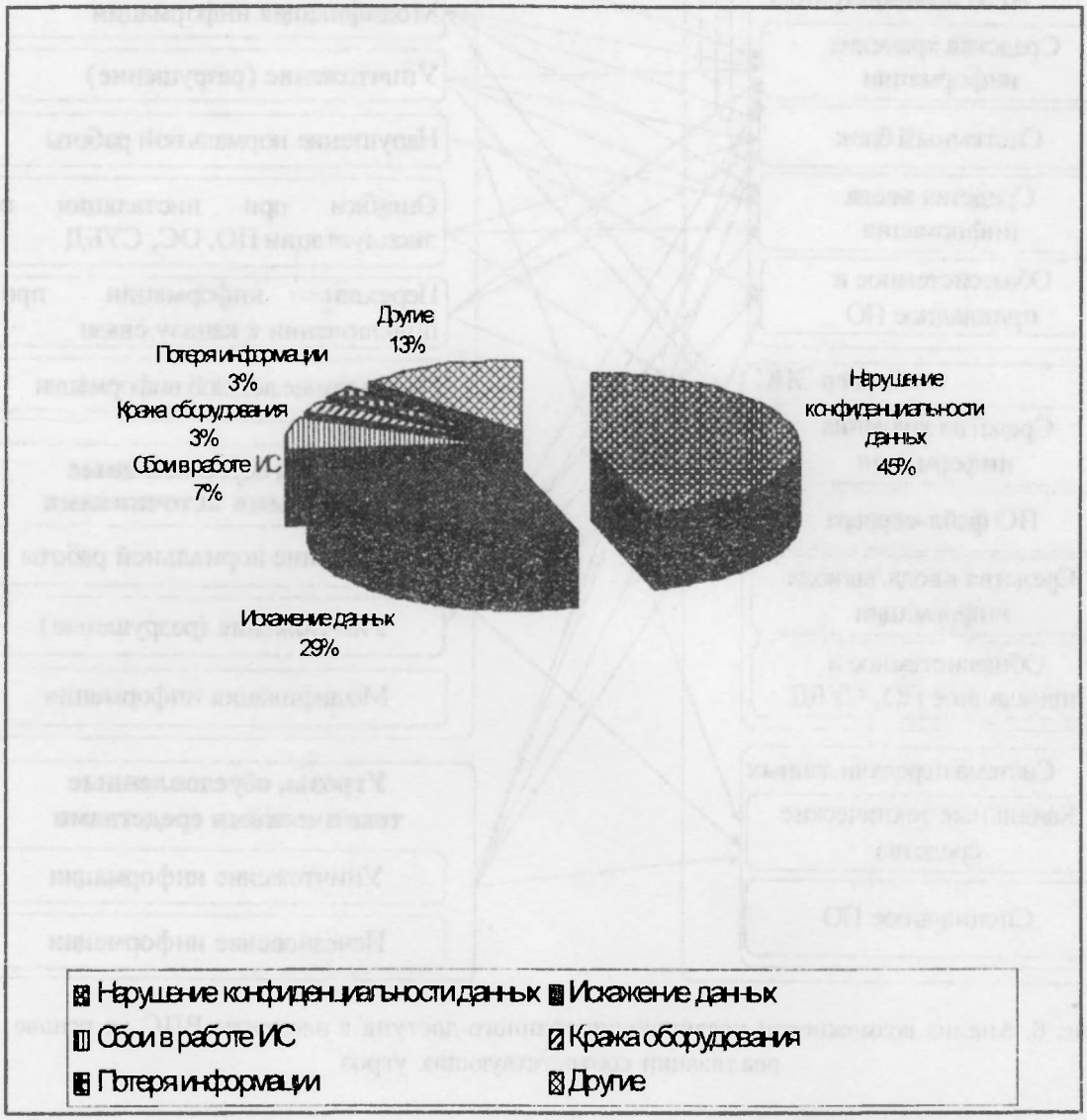


Рис. 6. Диаграмма распределения внутренних угроз

Самыми распространенными путями утечки информации являются электронная почта (до 22 %), интернет (сайты, чаты, форумы, бесплатные почтовые сервисы) до 20 %, интернет-пейджеры (ICQ/AOL, AIM, MSN, Yahoo!) и мобильные накопители (компакт-диски, USB-накопители) до 19 %, печатающие устройства до 8 % и другие источники до 12 %.

На сегодняшний день в мире существует публичный рейтинг суперкомпьютеров Top 500 [20]. В табл. 1 приведены результаты анализа времени реализации лобовой атаки (полного перебора) для перебора половины ключей суперкомпьютерами из этого списка, в табл. 2 – время необходимое для перебора половины ключей суперкомпьютерами из Топ 10. Сделаем предположение, что один перебор составляет 1 FLOPS (вычислительная мощность).

*Таблица 1*

**Время необходимое для перебора половины ключей суперкомпьютерами ведущими странами мира**

| Страна | 56 бит, мин | 64 бит, часов | 70 бит, суток | 75 бит, лет | 90 бит, лет | 256 бит, лет |
|---|---|---|---|---|---|---|
| США | 0,0537 | 0,224 | 0,611 | 0,0536 | 1760 | 1,15E+53 |
| Янония | 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 |

*Таблица 2*

**Время необходимое для перебора половины ключей суперкомпьютерами**

| Поз. | Производительность, FLOPS | 56 бит, мин | 64 бит, часов | 70 бит, суток | 75 бит, лет | 90 бит, лет | 256 бит, лет |
|---|---|---|---|---|---|---|---|
| 1 | Roadrunner - BladeCenter QS22 | 0,543 | 2,26 | 6,18 | 0,542 | 17800 | 1,16E+54 |
| 2 | Jaguar - Cray XT5 QC | 0,567 | 2,36 | 6,45 | 0,566 | 18600 | 1,22E+54 |
| 3 | Pleiades - SGI Altix ICE 8200EX | 1,23 | 5,13 | 14 | 1,23 | 28500 | 2,64E+54 |
| 4 | BlueGene/L - eServer Blue Gene Solution | 1,26 | 5,23 | 14,3 | 1,25 | 29000 | 2,69E+54 |
| 5 | Blue Gene/P Solution | 1,33 | 5,56 | 15,2 | 1,33 | 30800 | 2,86E+54 |

Развитие IT-технологий позволяет злоумышленникам развивать новые направления видов атак – методы изъятия данных аутентификации: фишинг и фарминг [19].

Суть обсих атак заключается в том, что пользователь вводит свои данные аутентификации не на web-странице автоматизированной ВПС, а на "фальшивой", визуально полностью похожей на нее. В первом случае используется сиам-рассылка "от имени" ВПС, в которой пользователю предлагают посетить ВПС, указывая при этом адрес фальшивой страницы. Второй тип атак похож на описанный выше и предполагает переадресацию на хакерский web-сайт, что становится возможным за счет уязвимостей браузеров, операционных систем или DNS-атак.

### *3. Механизмы обеспечения безопасности в ВПС.*

В соответствии с международными стандартами ISO 7498, ISO/IEC 10181 для обеспечения требуемых показателей безопасности определены пять базовых общепринятых услуг, для их обеспечения используются механизмы безопасности, большинство из которых реализуется на основе криптографических методов преобразования информации, взаимосвязь между показателями и механизмами безопасности представлены на рис. 7.


Рис. 7. Взаимосвязь услуг и механизмов безопасности

Основные механизмы обеспечения целостности и аутентичности информации в ВПС на различных уровнях основаны на использовании стандартов блочно-симметричных шифров (DES, ГОСТ 28147-89). Примером программной реализации рассмотренных механизмов являются программные средства криптографической защиты информации "Грифон-Б" и "Грифон-Л" предназначенных для криптографической защиты конфиденциальной информации в автоматизированных банковских системах [9; 10]. На рис. 8 приведена взаимосвязь между механизмами и применяемыми стандартами в подсистеме безопасности ВПС.

Проведенный анализ используемых стандартов показал, что для обеспечения конфиденциальности, аутентичности и целостности используется БСШ ГОСТ 28147-89 [11 – 14; 18] – устаревший алгоритм симметричного шифрования, разработанный в 1989 году, кроме того криптостойкость БСШ, основывается на криптостойкости S-боксов, которые для данного шифра "поступают" из Российской Федерации, что существенно влияет на безопасность ВПС в целом. На сегодняшний день в Украине нет национальных стандартов на алгоритмы БСШ и формирования хеш-функций, используемых в электронных цифровых подписях, что не позволяет использовать свой национальный стандарт ДСТУ-


4145 (ЭЦП) и БСШ для обеспечения конфиденциальности, аутентичности и целостности обрабатываемых данных в автоматизированных ВПС.

Таким образом, проведенные исследования показали, что дальнейшее развитие вычислительных и IT-технологий приводят не только к увеличению роста денежного оборота через банкоматы и другие системы удаленного пользования ВПС, расширению услуг, предоставляемых через ВПС населению, но и модернизации старых, появлению новых видов угроз на элементы ВПС.

Для обеспечения безопасности банковской информации в ВПС используются криптографические симметричные и асимметрические алгоритмы шифрования, прошедшие стандартизацию и сертификацию на государственном уровне. Однако отсутствие Доктрины информационной безопасности; сертифицированных национальных стандартов по основным специальным механизмам безопасности не позволяют использовать современные национальные алгоритмы, обеспечивающие конфиденциальность, аутентичность и целостность сообщений, что существенно влияет на степень защиты информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем как уже развернутых, так и создаваемых на территории государства, и в целом на уровень обеспечения национальной безопасности государства.

## СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ


1. http ://www.cryptopro.ru/cryptopro/documentation/dig-cert.htm.
2. *Артеменко Д. А.* Механизм обеспечения финансовой безопасности банковской деятельности [Текст] : дисс. ... канд. экон. наук : 08.00.10 / Д.А. Артеменко. – Ростов н/Д, 1999. – 190 с.
3. *Гайкович В.Ю.* Безопасность электронных банковских систем / В.Ю. Гайкович, А.Ю. Першин. - М. : Ед. Европа, 1994.
4. *Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф.* Защита информации в компьютерных системах и сетях / Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгин; под ред. В.Ф. Шаньгина. – 2-е изд., перераб. и доп. – М. : Радио и связь, 2001. – 376 с.
5. Межбанковские расчеты на Украине [Электронный ресурс]. – Режим доступа : http : // e2000.kyiv.org/biblioteka/biblio/stat/ukr_bank.html.
6. http ://www.carteblanche-online.info/index.php?option=com_content&task=view&id=105.
7. *Вихорев С.В.* Классификация угроз информационной безопасности [Электронный ресурс]. – Режим доступа : http://www2.cnews.ru/comments/security/elvis_class.shtml
8. http ://www.jetinfo.ru/2005/10/1/article1.9.200518.html.
9. Программное средство криптографической защиты информации "Грифон-Б" [Электронный ресурс]. – Режим доступа: http://www.banksoft.com.ua/index.php?id=28.
10. Программное средство "Библиотека функций криптографической защиты информации "Грифон-Л" // http ://www.banksoft.com.ua/index.php?id=27.
11. ГОСТ 34.310-95. Межгосударственный стандарт. Информационная технология. Криптографическая защита информации. Процедура выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма. – Киев. Госстандарт Украины, 1998.
12. ГОСТ 34.311-95. Межгосударственный стандарт. Информационная технология. Криптографическая защита информации. Функция хеширования. – Киев : Госстандарт Украины., 1998.
13. ГОСТ Р 34.10-94. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма.
14. ГОСТ Р34.11-94. Информационная технология. Криптографическая защита информации. Функция хэширования.
15. *Анохин М.И.* Криптография в банковском деле / М.И. Анохин, П.П. Варновский, В.М. Сидельников, В.В. Ященко. – МИФИ, 1997. – 274 с.
16. *Логинов А.А.* Общие принципы функционирования электронных платежных систем и осуществление мер безопасности при защите от злоупотребления и мошенничества / А.А. Логинов, Н.С. Елхимов // Конфидент. – 1995. – № 4. – С. 48–54.
17. "Retail Banking Research : ATMs and Cash Dispensers Central & Eastern Europe 2010".
18. Шефановский Д.Б. ГОСТ 34.11. – 94. Функция хеширования. Краткий анализ. Учебный центр "Инфозащита". – 2001. – 9 с.
19. *Щеглов А.Ю.* Как защищать конфиденциальную информацию и персональные данные в современных условиях? / А.Ю. Щеглов, ЗАО "НПП "Информационные технологии в бизнесе" [Электронный ресурс]. – Режим доступа : Bankir.Ru.
20. BOINC – Berkeley Open Infrastructure for Network Computing, Dr. David Anderson describes SETI@home, BOINC and Distributed Computing, youtube.com.
21. http ://www.jetinfo.ru/2005/10/1/article1.9.200518.html.


Отримано 12.04.2011