Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications 6-8 September 2007, Dortmund, Germany p.599-602
6. "What is DRBD" www.drbd.org
7. Sebek. http://www.honeynet.org/tools/sebek
8. "AIDE - Advanced Intrusion Detection Environment". http://www.cs.tut.fi/~rammer/aide.html
9. "Tripwire® software is a security and data integrity tool". http://sourceforge.net/projects/tripwire/
10. Clam AntiVirus. www.clamav.net/
11. Linenoise. http://www.phrack.com/issues.html?issue=61&id=3
12. Tcpdump www.tcpdump.org/
13. Wireshark. www.wireshark.org
14. Snort - the de facto standard for intrusion detection/prevention. www.snort.org/
15. Prelude IDS. www.prelude-ids.com/
16. Cisco IDS. http://www.informit.com/articles/article.aspx?p=24696
17. Cisco ASA. http://www.cisco-systems.ru/katalog/cisco-asa_51/
18. Nmap - Free Security Scanner For Network Exploration & Security ... nmap.org
19. Nessus Security scanner for Oracle and various flavors of Unix. www.nessus.org
20. Core Impact. www.coresecurity.com/
21. Clam AntiVirus. www.clamav.net
22. Kaspersky Internet Security. http://kaspersky-antivirus.kiev.ua/products/inetsecurity.htm
23. Honeywall CDROM. https://projects.honeynet.org/honeywall/
24. Honeysnap. https://projects.honeynet.org/honeysnap
25. Capture BAT. https://public.honeynet.org/mailman/listinfo/capture-bat
26. M. Dornseif, T. Holz, and C. Klein. NoSEBrEaK - Attacking Honeynets. Proc. of the 5th Annual IEEE Information Assurance Workshop, Westpoint, June 2004.

УДК 336.717:004.78

Кузнецов А.А, Евсеев С.П., Король О. Г.
Харьковский национальный экономический университет

ИССЛЕДОВАНИЕ КРИПТОГРАФИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В ПЛАТЕЖНЫХ СИСТЕМАХ БАНКОВ УКРАИНЫ

Постановка проблемы в общем виде и анализ литературы. Бурное развитие компьютерных систем и сетей привело к возникновению принципиально новых, так называемых, информационно - телекоммуникационных технологий, что позволило расширить услуги платежных систем коммерческих банков (ВПС КБ), внедрить новые сервисы и технологии. Вместе с тем, интенсивное использование компьютерных систем и сетей в ВПС КБ привело к появлению новых видов компьютерного терроризма: неправомерного искажения или фальсификации банковской информации, уничтожению или разглашению определенной ее части, дезорганизации процессов обработки и передачи данных. Жизненно важные интересы субъектов ВПС КБ заключаются в том, чтобы определенная часть информации, касающаяся их безопасности, экономических и других сторон деятельности, конфиденциальная коммерческая и персональная информация, была бы постоянно доступна и в тоже время надежно защищена от неправомерного ее использования [3, 8, 9]. В работах [3, 10, 14] рассмотрены основные виды угроз в информационно-коммуникационных системах, а также механизмы обеспечения аутентичности и целостности передаваемых данных.

Актуальной остается проблема защиты ВПС КБ в связи с дальнейшим распространением территориально-распределенных сетей, и систем с удаленным доступом к совместно используемым ресурсам [3 – 5, 7 – 15].

Целью статьи является анализ угроз безопасности информации в платежных системах коммерческого банка, исследование программных средств защиты информации во ВПС КБ Украины, их возможностей по обеспечению безопасности информации в платежных системах банков Украины.

1. Анализ угроз безопасности информации в платежных системах коммерческого банка. Несмотря на широкое применение различных криптографических алгоритмов на различных уровнях защиты внутриплатежные системы подвержены различным атакам и угрозам.

Основными видами угроз безопасности информации во внутриплатежных системах (угроз коммерческим и персональным интересам субъектов банковских отношений) являются [4, 5, 7 – 9]:

сбои и отказы оборудования (технических средств) ПС;

последствия ошибок проектирования и разработки компонентов ПС (аппаратных средств, технологии обработки информации, программ, структур данных и т.п.);

ошибки эксплуатации (пользователей, операторов и другого персонала);

преднамеренные действия нарушителей и злоумышленников (обиженных лиц из числа персонала, преступников, шпионов, диверсантов и т.п.). Общая классификация угроз безопасности представлена на рис.1.

Анализ рис. 1 показывает на дальнейшее совершенствование атак со стороны злоумышленников, а также внутренних угроз являющихся одной из наиболее актуальных проблем информационной безопасности. Согласно статистике, неправомерные действия сотрудников самих банков причиняют наибольший ущерб и до 90% средств, выделяемых на информационную безопасность, тратится на обеспечение защиты от внутренних атак [16].

Для обеспечения целостности и аутентичности информации во ВПС КБ применяются различные программно-аппаратные средства защиты, основанные на криптографических алгоритмах. Рассмотрим основные их технические характеристики и механизмы.

2. Исследование возможностей программных средств защиты информации во ВПС КБ Украины.

Для обеспечения безопасности в платежных системах КБ Украины применяются криптографические методы, основанные на использовании международных стандартов (ГОСТ 28147-89, ГОСТ 34.310-95, ГОСТ 34.311-95).

Система "Клиент-Банк" и *"Украина-Клиент"* представляет собой комплекс программных средств, предназначенных для организации взаимодействия между клиентами банков и автоматизированными банковскими системами (АБС) по каналам сетей передачи данных произвольного типа [13].

Система реализует единую технологию обработки, обмена и защиты информации, поддерживая формирование и автоматизированную обработку всех типов электронных платежных документов в национальной валюте, предусмотренных инструкциями Национального банка Украины, а также формирование, передачу и обработку документов произвольной и задаваемой пользователем структуры в виде текстовых и RTF файлов. Система гарантирует конфиденциальность и целостность обрабатываемой информации и полностью реализует требования, предъявляемые Национальным банком Украины к защите информации в системах "Клиент-Банк". Для выполнения криптографических преобразований используются сертифицированные средства библиотеки процедур криптографической защиты информации "Тайфун-W322 в. 2.01, реализующей алгоритмы, установленные ГОСТ 28147-89, ГОСТ 34.310-95, ГОСТ 34.311-95, ДСТУ 4145-2002/

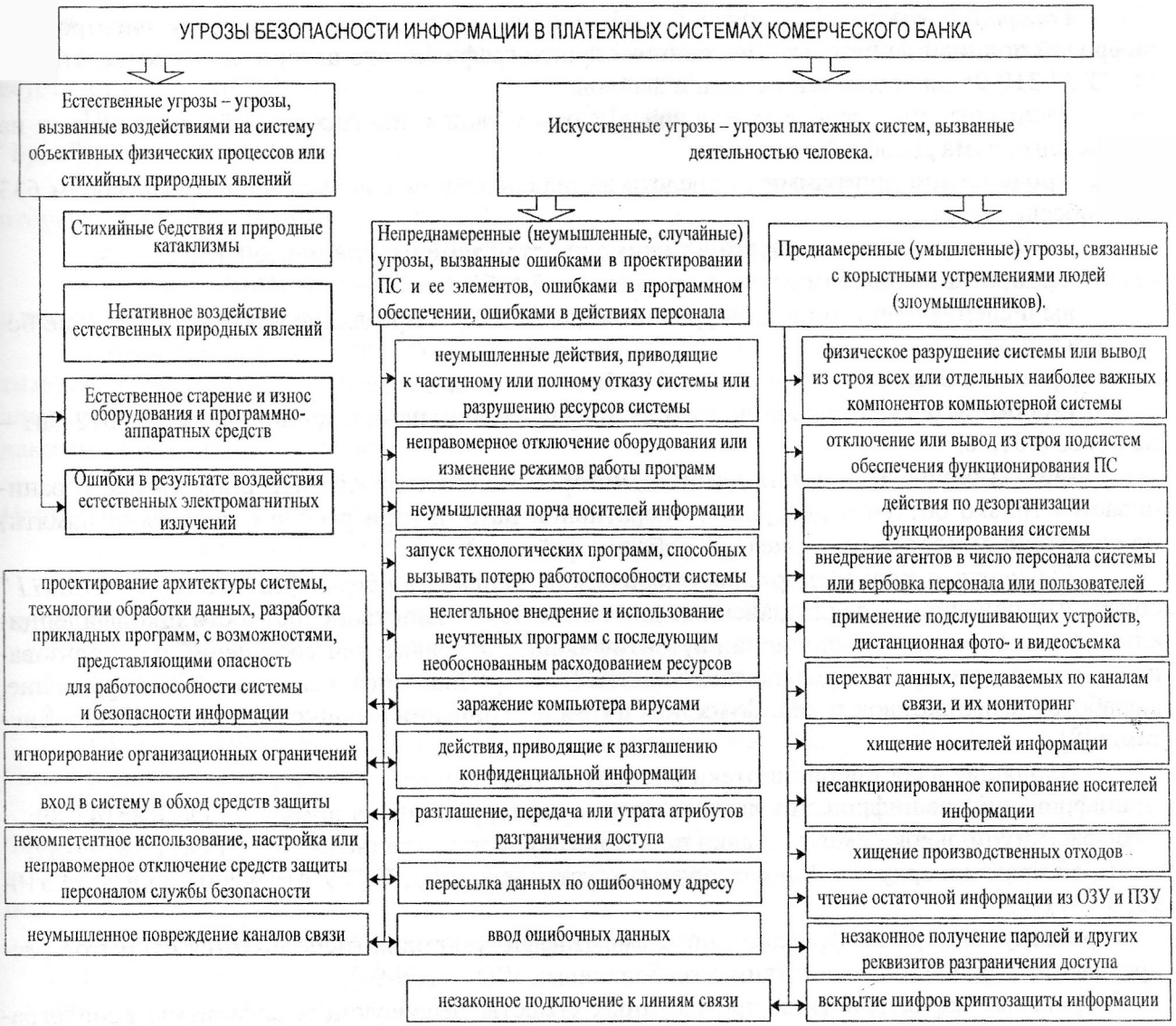

Рис. 1. Общая классификация угроз безопасности

Рассмотрим комплексные программные средства защиты, используемые в платежных системах *"Клиент-Банк"* и *"Украина-Клиент"*.

Программное средство "Грифон-Б" ("Грифон-Л") предназначено для криптографической защиты конфиденциальной информации (обеспечения конфиденциальности, целостности и аутентичности данных, выполнения функций генерации, сертификации и распределения ключей) в ВПС и применяется для обмена информацией внутри корпоративной сети банка, с клиентами, работающими по системе "Клиент-Банк", в системах обслуживания пластиковых карт и пр. [7, 8].

Программные средства обеспечивают реализацию следующих алгоритмов:

Криптографического преобразования в соответствии с ГОСТ 28147-89 в режимах простой замены, гаммирования и гаммирования с обратной связью для областей памяти и файлов;

Формирования имитовставки длиной 32 бит в соответствии с ГОСТ 28147;

Хеширования в соответствии с ГОСТ 34.311-95 для областей памяти и файлов;

Генерации секретного ключа электронной цифровой подписи x, секретного параметра k для реализации ГОСТ 34.310-95, а также генерацию сеансовых ключей для реализации ГОСТ 28147-89;

Генерации открытой ключевой информации, вычисление и проверку электронной цифровой подписи на базе асимметричного криптографического алгоритма в соответствии с ГОСТ 34.310-95 для областей памяти и файлов;

Распределения сеансовых ключей в соответствии с протоколом обмена ключами на основе алгоритма Диффи-Хеллмана.

Быстродействие программных средств на персональном компьютере с процессором 633 МГц обеспечивает:

шифрование области памяти в режиме простой замены – не менее 5 Мб/с;

хеширование области памяти – не менее 1.5 Мб/с;

вычисление электронной цифровой подписи (ЭЦП) при длине ключа 512 бит – не более 0.015 с;

проверка ЭЦП при длине ключа 512 бит – не более 0.02с;

генерация общего ключа по методу Диффи-Хеллмана при длине ключа 512 бит – не более 0.015 с.

Объем обрабатываемых данных, которые подписываются или шифруются, ограничивается только объемом доступной оперативной памяти (при работе с областями памяти) или свободным местом на диске (при работе с файлами).

Библиотека процедур криптографической защиты информации "Тайфун-PKCS#11" содержит процедуры, предназначенные для обеспечения защиты целостности и конфиденциальности информации, выполнения аутентификации отправителей сообщений с использованием механизмов криптографической защиты (электронная цифровая подпись, шифрование, выработка имитовставок и хеш-функций) путем встраивания в конкретные прикладные системы [8].

Входящие в состав библиотеки процедуры реализуют:

шифрование/расшифрование данных по алгоритму, установленному ГОСТ 28147-89;

выработку/проверку имитовставки по алгоритму, установленному ГОСТ 28147-89;

выработку/проверку ЭЦП по алгоритмам, установленным ДСТУ 4145-2002, ГОСТ 34.310-95, 34.311-95;

выработку ключей шифрования по схеме Диффи-Хеллмана (используется открытое распределение ключей в соответствии с требованиями ISO 11166-94).

Скоростные характеристики программных средств, реализующих алгоритмы криптографических преобразований (для ПЭВМ на базе Intel Celeron 2,4 ГГц):

скорость зашифрования/ расшифрования данных в режиме простой замены согласно ГОСТ 28147-89 не менее 8 Мбайт/сек;

скорость вычисления хеш-функции данных согласно ГОСТ 34.311-95 не менее 3 Мбайт/с;

время выработки ЭЦП согласно ГОСТ 34.310-95 при длине ключа 512 бит не более 0.003 с;

время проверки ЭЦП согласно ГОСТ 34.310-95 при длине ключа 512 бит не более 0.006 с;

время выработки ЭЦП согласно ГОСТ 34.310-95 при длине ключа 1024 бит не более 0.01 с;

время проверки ЭЦП согласно ГОСТ 34.310-95 при длине ключа 1024 бит не более 0.02 с;

время выработки ЭЦП (с вычислением предподписи) согласно ДСТУ 4145-2002 для основного поля степени 163 не более 0.0068 с;

время проверки ЭЦП согласно ДСТУ 4145-2002 для основного поля степени 163 не более 0.013 с.

Криптографические преобразования в библиотеке "Тайфун-PKI PKCS#11" реализуются с использованием объектной библиотеки программных процедур криптографической защиты информации "Тайфун-W32" версии 2.01.

Система защищенной электронной почты "Бриз" предназначена для осуществления обмена электронными сообщениями в формате SMF-70, защищенными с использованием механизмов криптографической защиты (электронная цифровая подпись, зашифрова-

ние/расшифрование, выработка имитовставок), между клиентами электронной почты (ЭП), зарегистрированными на узлах ЭП, через сеть передачи данных произвольного типа и соответствует критериям НД ТЗІ 2.5-004-99 [9].

По сравнению с другими системами ЭП (например, Microsoft Exchange), система "Бриз" дополнительно реализует:

гарантированную доставку сообщений получателю (или гарантированное оповещение отправителя о невозможности доставки);

непрерывную защиту сообщений на всем пути от отправителя до получателя;

гарантированное оповещение отправителя о факте получения сообщения получателем с невозможностью последующего отказа от факта получения;

возможность автоматической обработки входящих и исходящих сообщений в автоматизированном рабочем месте (АРМ) клиента, что позволяет легко интегрировать средства электронной почты с различными автоматизированными системами, выполняющими обмен данными в автоматическом режиме;

возможность автоматического обмена почтовыми сообщениями с электронной почтой Национального банка Украины.

В состав системы входят программные средства:

серверов узлов ЭП,

АРМ клиентов ЭП со встроенными средствами защиты ЭП,

АРМ администраторов ЭП со встроенными средствами защиты ЭП,

АРМ управления криптографическими ключами клиентов ЭП,

АРМ центра сертификации ключей (АРМ ЦСК) клиентов ЭП.

Схема взаимодействия между узлами и клиентами ЭП, реализованная в системе "Бриз", приведена на рис. 2.

В качестве средств телекоммуникации могут использоваться любые средства, обеспечивающие передачу сообщений в виде файлов. Для работы в сети передачи данных с протоколом TCP/IP в АРМ клиента интегрированы программные средства, реализующие протокол передачи файлов FTP.

Программные средства клиента ЭП реализуют следующие функции:

подготовку и передачу сообщений;

прием и обработку принятых сообщений;

автоматическое формирование квитанций о доставке сообщений на АРМ получателя;

ведение справочников почтовых адресов клиентов-корреспондентов;

ведение архивов обработанных сообщений;

протоколирование выполненных операций;

зашифрование/расшифрование передаваемых сообщений по алгоритму, установленному в ГОСТ 28147-89;

выработку/проверку имитовставки по алгоритму, установленному в ГОСТ 28147-89;

выработку/проверку ЭЦП сообщений по алгоритму, установленному в ГОСТ 34.310-95, 34.311-95;

выработку/проверку ЭЦП квитанций по алгоритму, установленному ГОСТ 34.310-95, 34.311-95.

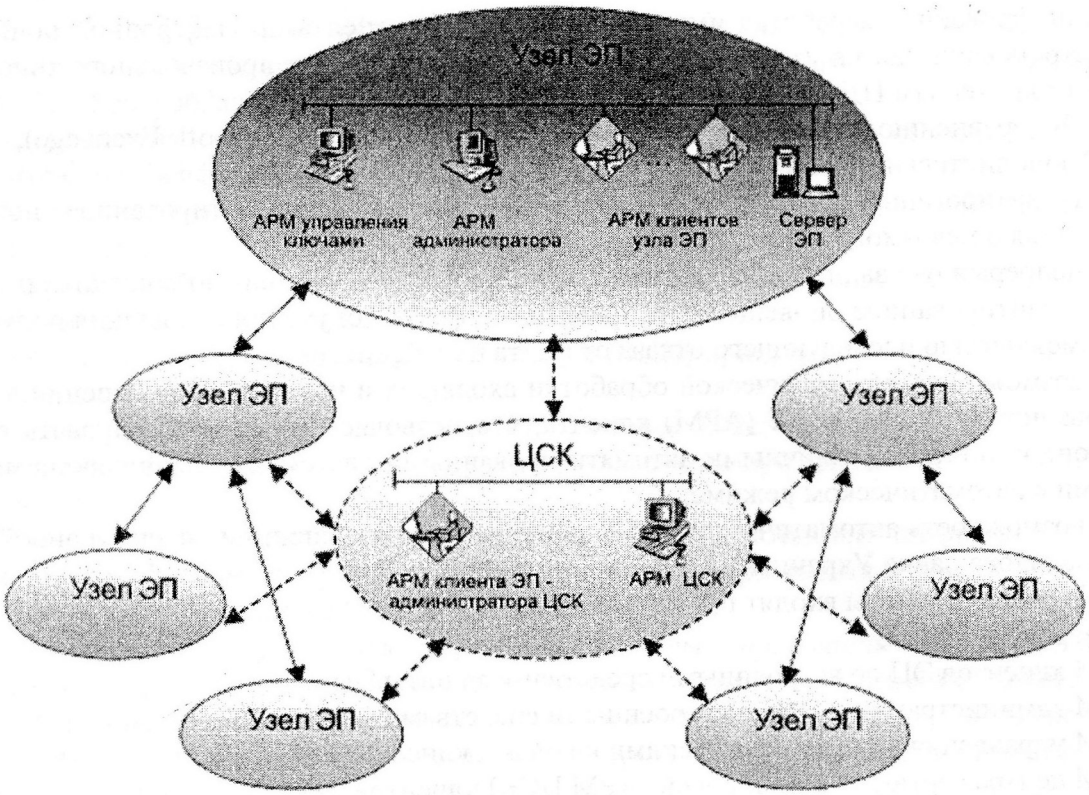

Рис. 2. Схема взаимодействия между узлами и клиентами ЭП

При обмене электронными сообщениями между пользователями ЭП реализуется технология, приведенная на рис. 3.

Комплекс средств защиты (КСЗ) информации с ограниченным доступом (ИсОД), от несанкционированного доступа (НСД) **"Гриф–Мережа"** версии 2.01 предназначен для обеспечения защиты ИсОД, обрабатываемой в локальных вычислительных сетях (ЛВС). Комплекс позволяет создать на базе ЛВС специализированную АС класса 2 для обработки ИсОД и обеспечить защиту обрабатываемой ИсОД от угроз нарушения целостности, конфиденциальности и доступности при реализации политики административного управления доступом к информации [9].

Комплекс "Гриф-Мережа" реализует следующие функции:

идентификацию и аутентификацию пользователей на основании имени, пароля и персонального электронного идентификатора (Touch Memory, Flash Drive или дискеты) при загрузке ОС рабочей станции до загрузки каких-либо программных средств с дисков. Это позволяет заблокировать использование рабочей станции посторонним лицом, а также опознать конкретного легального пользователя и в дальнейшем реагировать на запросы этого пользователя в соответствии с его полномочиями;

блокировку устройств интерфейса пользователя (клавиатуры, мыши, монитора) на время его отсутствия;

контроль целостности и самотестирование КСЗ при старте и по запросу администратора, что позволяет обеспечить устойчивое функционирование КСЗ и не допустить обработку ИсОД в случае нарушения его работоспособности;

разграничение обязанностей пользователей и выделение нескольких ролей администраторов, которые могут выполнять различные функции по администрированию (регистрацию защищаемых ресурсов, регистрацию пользователей, назначение прав доступа, обработку протоколов аудита и т.п.).

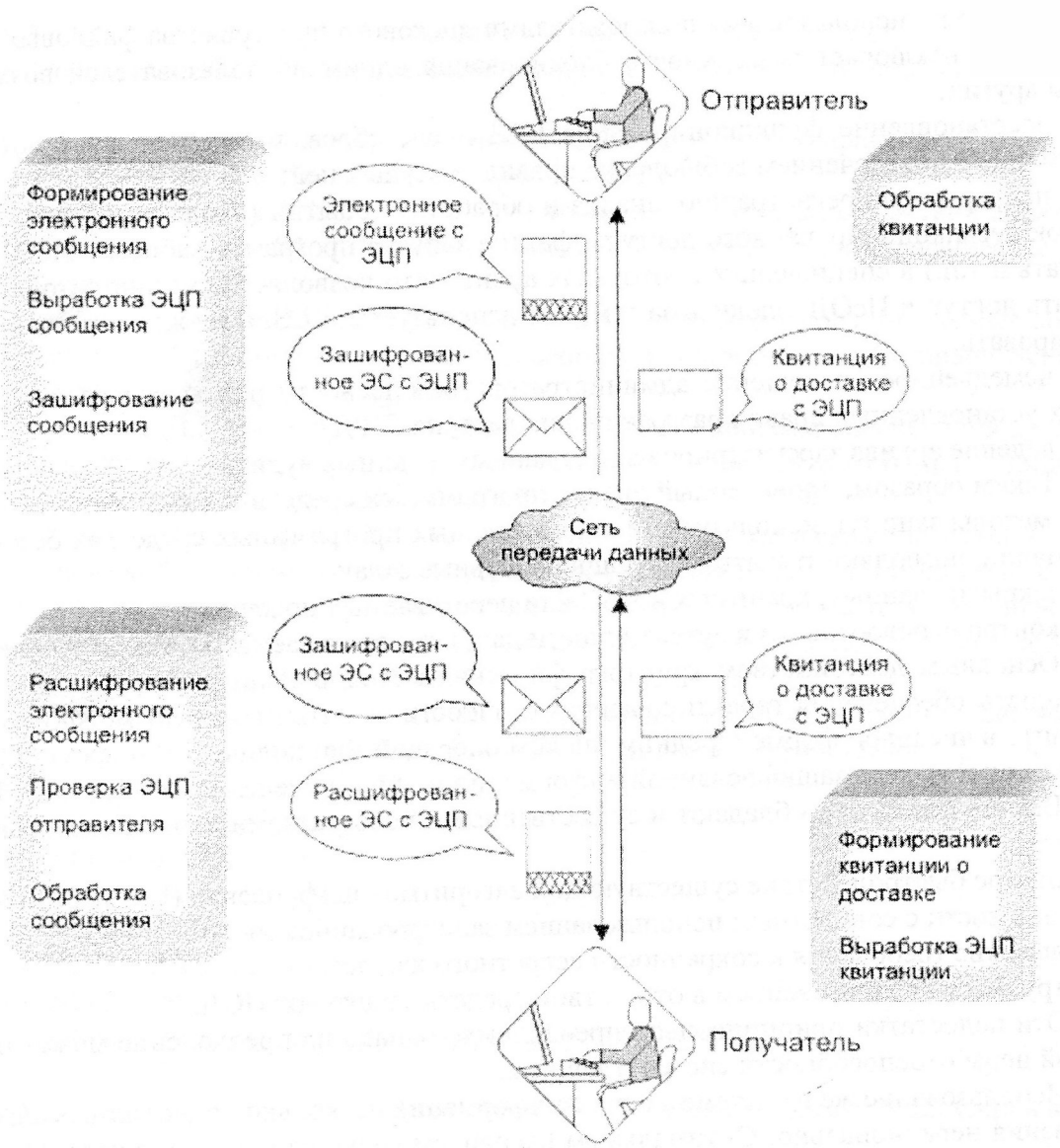

Рис. 3. Технология обмена сообщениями между пользователями ЭП

разграничение доступа пользователей к выбранным каталогам (папкам), размещенным на рабочих станциях и файловых серверах ЛВС, что позволяет организовать одновременную совместную работу нескольких пользователей ЛВС, имеющих разные служебные обязанности и права по доступу к ИсОД;

управление потоками информации и блокировку потоков информации, приводящих к снижению ее уровня конфиденциальности;

контроль вывода информации на печать;

контроль экспорта/импорта информации на сменные носители;

гарантированное удаление информации путем затирания содержимого файлов, содержащих ИсОД, при их удалении;

разграничение доступа прикладных программ к выбранным каталогам и находящимся в них файлам, что позволяет обеспечить защиту ИсОД от случайного удаления, модификации и соблюсти технологию ее обработки;

контроль целостности прикладного программного обеспечения (ПО) и программного обеспечения КСЗ, а также блокировку загрузки программ, целостность которых нарушена, что позволяет обеспечить защиту от вирусов и соблюдение технологии обработки ИсОД;

контроль использования пользователями дискового пространства файловых серверов (квоты), что исключает возможность блокирования одним из пользователей возможности работы других;

восстановление функционирования КСЗ после сбоев, что гарантирует доступность информации с обеспечением соблюдения правил доступа к ней;

непрерывную регистрацию, анализ и обработку событий (входа пользователей в ОС, попыток несанкционированного доступа, фактов запуска программ, работы с ИсОД, вывода на печать и т.п.) в специальных протоколах аудита, что позволяет администраторам контролировать доступ к ИсОД, следить за тем, как используется КСЗ, а также правильно его конфигурировать;

немедленное оповещение администратора безопасности обо всех выявленных нарушениях установленных правил разграничения доступа (ПРД);

ведение архива зарегистрированных данных и данных аудита.

Таким образом, проведенный анализ программных средств показал, что криптографические методы защиты, используемые в комплексных программных средствах безопасности информации, позволяют решать следующие основные задачи:

закрытие данных, хранимых в АБС или передаваемых по каналам связи;

контроль целостности и аутентичности данных, передаваемых по каналам связи.

Основным достоинством криптографических методов защиты информации является возможность обеспечения гарантированной стойкости защиты, которую можно рассчитать и выразить в числовой форме (средним числом операций или количеством времени, необходимого для раскрытия зашифрованной информации или вычисления ключей) [3, 10, 14].

Вместе с тем, они обладают и существенными недостатками, к числу которых можно отнести:

низкое быстродействие существующих алгоритмов шифрования (ГОСТ 28147-89);

трудности с совместным использованием зашифрованной информации;

высокие требования к сохранности секретного ключа;

трудности с применением в отсутствии средств защиты от НСД.

Эти недостатки принципиально преодолимы, однако их преодоление может привести к полной неработоспособности системы защиты.

Использование же в системе защиты информации нескольких однотипных алгоритмов шифрования нерационально. Оптимальным вариантом является система, в которой средства криптозащиты являются общесистемными, то есть выступают в качестве расширения функций операционной системы и включают сертифицированные алгоритмы шифрования всех типов (блочные и потоковые, с закрытыми и открытыми ключами) [10 – 15].

Выводы

Опыт построения и эксплуатации комплексных систем защиты информации показывает, что более 60% нарушений безопасности приходится на несанкционированную модификацию сообщений, нарушение целостности и аутентичности данных в компьютерных системах и сетях. Отсутствие украинских стандартов в области обеспечения аутентичности и целостности данных, применение стандартов хеширования и симметричного шифрования бывшего СССР и Российской федерации (ГОСТ 28147-89, ГОСТ 34.310-95, ГОСТ 34.311-95) не позволяют обеспечить в полной мере безопасность. Следовательно, исследование перспективных методов и механизмов, обеспечения целостности и аутентичности данных является актуальным направлением.

Литература:

1. Ахо А., Хопкрофт Дж., Ульман Дж. *Структуры данных и алгоритмы: Учебное пособие* / Пер. с англ.: М.: Вильямс, 2000. 384 с.

2. Копытов Е., Иванова С., Птицина И. *Структуры данных и их обработка на компьютере: Учебное пособие/* Под ред. Е. Копытова. Рига: Институт транспорта и связи, 2003. 128 с.

3. В. Столлингс Криптография и защита сетей: принципы и практика, 2-е изд. : пер. с англ. — М.: издательский дом «Вильям», 2001. — 672 с.

4. Шефановский Д.Б. ГОСТ Р 34.11- 94. Функция хеширования. Краткий анализ.

5. ГОСТ Р 34.11- 94. "Информационная технология. Криптографическая защита. Функция хеширования".

6. M. Bellare, R. Canetti, and H. Krawczyk. Keying hash functions for message authentication. Advances in Cryptology - Crypto 96 Proceedings, Lecture Notes in Computer Science Vol. 1109, N. Koblitz ed, Springer-Verlag, 1996.

7. Євсеєв С.П., Чевардин В.Е., Радковский С.А. Механизмы обеспечения аутентичности банковских данных во внутриплатежных системах комерческого банка. / Збірник наукових статей ХНЕУ. – Харків: ХНЕУ. – 2008. – Вип. 6. – С. 40-44.

8. Кузнецов А.А., Король О.Г., Ткачов А.М. Анализ механизмов обеспечения безопасности банковской информации во внутриплатежных системах коммерческого банка / Матеріали І міжнародної науково-практичної конференції «Безпека та захист інформації в інформаційних і телекомунікаційних системах» 28 – 29 травня 2008 р. Зб. наук. статей «Управління розвитком». ХНЕУ. № 6 – Х.: 2008. – С. 28 – 35.

9. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. НД ТЗІ 2.5-004-99.— [Чинний від 1999-28-04].]. — К. : Держспоживстандарт України 1999. — 53 с.

10. http://www.cryptopro.ru

11. http://e-signature.com.ua

12. http://www.ict.com.ua

13. http://www.vano-zhuk.narod.ru

14. http://bezpeka.ladimir.kiev.ua

15. http://www.infocity.kiev.ua

16. http://www.jetinfo.ru/2005/10/1/article1.9.200518.html

УДК 629.07.5

Дудикевич[1] В.Б., Томашевський[2] Б.В., Сергієнко[2] Р.В.

[1]Національний університет "Львівська Політехніка"
[2]Львівський Військовий інститут
Сухопутних військ імені гетьмана Петра Сагайдачного

ПРОТОКОЛИ І МЕХАНІЗМИ БЕЗПЕКИ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ І МЕРЕЖАХ

В умовах стрімкої інформатизації суспільства, широкого застосування засобів обчислювальної техніки і комп'ютерних систем особливої актуальності набувають питання інформаційної безпеки, найбільш складними з яких є необхідність захисту цінної конфіденційної і секретної інформації в державних і приватних підприємствах, в органах і установах державного управління, у банківській і інших системах [1-5].

Задля безпеки (автентичності, конфіденційності і цілісності) інформації з обмеженим доступом застосовуються різні криптографічні послуги і механізми безпеки [3-6].

Метою статті є аналіз існуючих протоколів і механізмів забезпечення автентичності,