Захист інформації

УДК 336.717:004.78

О.Г. Король

Харківський національний економічний університет імені Семена Кузнеця, Харків

АНАЛІЗ ЗАГРОЗ І МЕХАНІЗМІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ В СИСТЕМІ ЕЛЕКТРОНнИХ ПЛАТЕЖІВ КОМЕРЦІЙНОГО БАНКУ УКРАЇНИ

Розглядаються основні загрози і механізми забезпечення безпеки банківських транзакцій в системах електронних платежів (СЕП) комерційних банків України. Проводиться аналіз основних вимог стандарту СОУ Н НБУ 65.1 СУІБ 1.0:2010 який відповідає стандарту ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements щодо формування основних вимог і функцій побудови системи управління інформаційною безпекою (СУІБ).

Ключові слова: *механізми забезпечення безпеки, автентичність, цілісність, конфіденційність, внутрішньоплатижні системи комерційного банку України.*

Постановка проблеми

Інформація є ресурсом, який подібно іншим важливим бізнес-ресурсам, є суттєвим для бізнесу організації і тому потребує відповідного захисту. Це суттєво важливо у все більш взаємопов'язаному діловому середовищі. Внаслідок цієї зростаючої взаємопов'язаності інформація тепер наражається на зростаючу кількість і більшу різноманітність загроз та вразливостей [14, 15]. Розвиток інформаційних технологій, глобальної мережі Інтернет, а також стрімке зростання обчислювальних можливостей комп'ютерних систем, швидке зростання обсягів оброблюваних даних у сучасних системах електронних платежів комерційного банку (СЕП КБ), поява нових форм електронних послуг, запропонованих СЕП, висувають нові вимоги до надійності і забезпеченню безпеки у внутрішньоплатіжних банківських системах (ВПС).

На сьогоднішній день не існує науково-обґрунтованої концепції й механізмів забезпечення фінансової безпеки банківської діяльності національної платіжної системи в цілому [1]. Система електронних платежів являє собою сукупність правил, організаційних заходів, програмно-технічних засобів, які використовуються банком для забезпечення здійснення розрахунків у межах України між банками як за дорученнями клієнтів банків, так і за зобов'язаннями банків. СЕП виконує міжбанківський переказ у файловому режимі та в режимі реального часу. [1]. Дана система належить до багаторівневих критичних систем, тому що її відмова, відступ від обмежень, що задаються, або зміни в роботі підсистеми можуть викликати серйозні наслідки або привести до краху всієї системи в цілому. Загальна структурна схема системи електронних платежів наведена на рис. 1. **Метою статті** є аналіз основних ризиків й механізмів забезпечення безпеки інформаційних повідомлень у системах електронних платежів комерційного банку України.

Результати досліджень

У відповідності до СОУ Н НБУ 65.1 СУІБ 1.0:2010 який відповідає стандарту ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements Національний банк України має власний досвід створення платіжних та інформаційних систем. Зокрема Національним банком України було створено Систему електронних платежів Національного банку України (СЕП НБУ), яка визначена законодавством України як державна система міжбанківських розрахунків, та систему роздрібних платежів із використанням платіжних карток – Національну систему масових електронних платежів [14, 15].

Для захисту платіжних повідомлень використовується система захищеної електронної пошти (СЗЕП), призначена для обміну електронними повідомленнями у форматі SMF-70 через мережу передачі даних довільного типу відповідно до критеріїв НД ТЗІ 2.5-004-99 [3]. Загальна структура підсистеми захисту інформації під ВПБС і можливих загроз на окремі її складові наведені на рис. 2.

Національна система масових електронних платежів складається з:

регіональних процесінгових центрів (РПЦ) в обласних управліннях НБУ або комерційних підприємствах – до 25 РПЦ на всю Україну;

банків-емітентів і банків-еквайєрів НСМЕП зі своїми банківськими підсистемами, торгівельною інфраструктурою та інфраструктурою сфери послуг. Загальна структура НСМЕП включає в себе такі основні елементи:

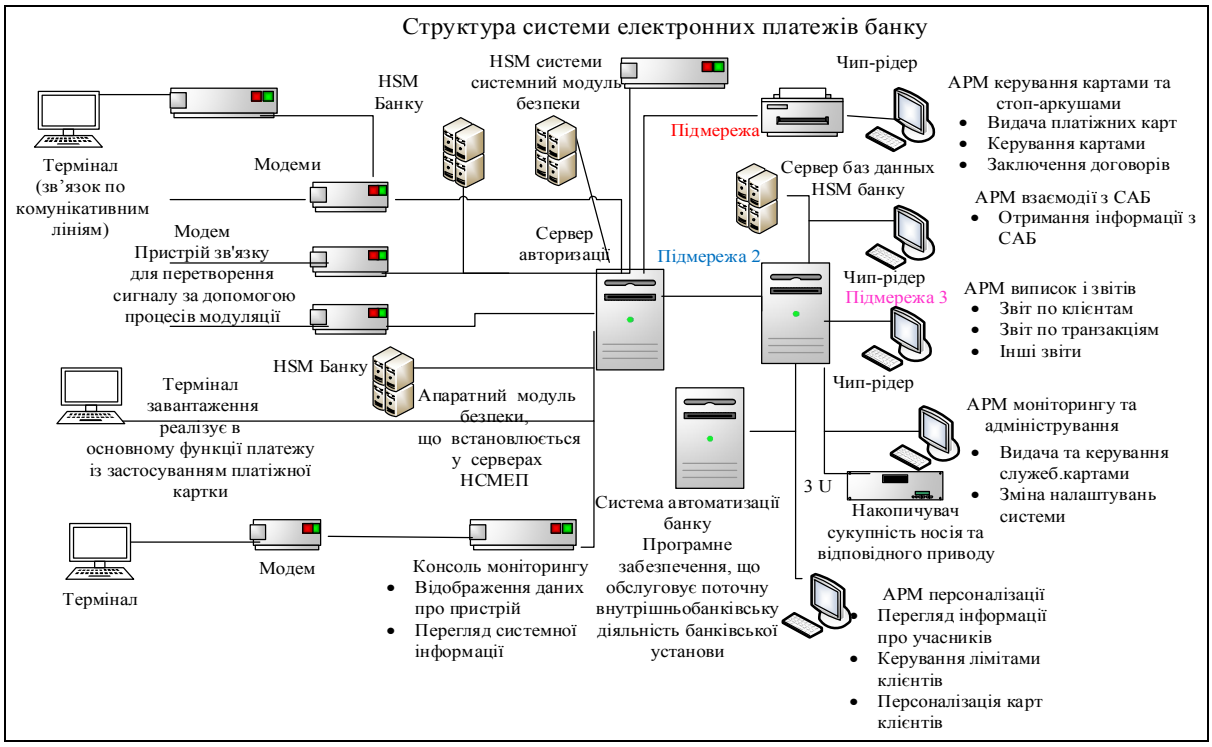


Рис. 1. Структурна схема електронних платежів

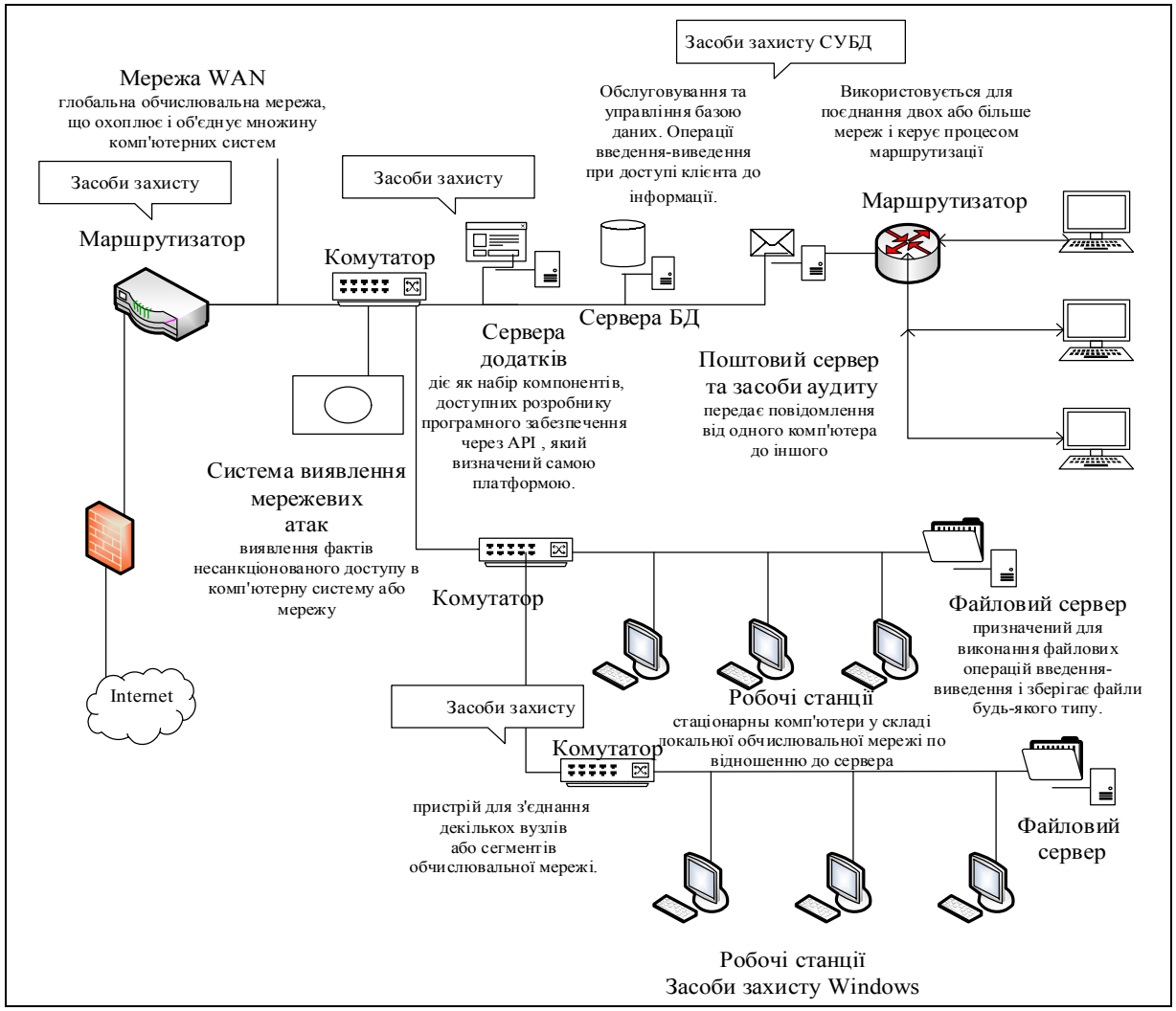


Рис. 2. Структурна схема підсистеми захисту інформації в СЕП

1. Центр системної ініціалізації та системної персоналізації (установа НБУ).

2. Розрахунковий банк (РБ) системи на базі Головного управління НБУ. Схема розрахунків – клірингова.

3. Головний та регіональні процесінгові центри (ГПЦ та РПЦ) в обласних управліннях НБУ або комерційних установах (до 25 РПЦ на всю Україну). Вони виконують обробку міжбанківських транзакцій, розрахунок клірингу, керування системою.

4. Банки-емітенти і банки-еквайєри НСМЕП із своїми банківськими системами, торгівельною інфраструктурою та інфраструктурою сфери послуг.

5. Користувачі карток – фізичні та юридичні особи.

6. Картки на інтегрованих схемах (або смарт-картки). Для забезпечення захисту банківської інформації в ВПБС на різних рівнях використовуються криптографічні механізми, однак, бурхливе зростання обчислювальної техніки, створення систем і технологій кібертерроризму призводить до появи нових загроз (активних і пасивних атак) і злому підсистеми захисту ВПБС.

Під загрозою розуміється сукупність умов чинників, що створюють небезпеку несанкціонованого, в тому числі випадкового, доступу до інформації, результатом якого може стати знищення, зміна, блокування, копіювання, поширення інформації, загальна класифікація загроз наведена на рис. 4 [19].

Одним з найбільш вразливих місць в системі електронних платежів є пересилання платіжних та інших повідомлень між банками, між банком і банкоматом, між банком і клієнтом. Результати досліджень атак на сучасні КМ компанії "Arbor Networks" наведені на рис. 3.

У відповідності до Стандарту СОУ Н НБУ 65.1 СУІБ 1.0:2010 керівництву комерційних банків пропонується процесний підхід до управління інформаційною безпекою, заохочує його користувачів робити наголос наважливості:

a) розуміння вимог інформаційної безпеки організації і необхідності

розроблення політики та цілей інформаційної безпеки;

b) впровадження заходів безпеки та забезпечення їх функціонування

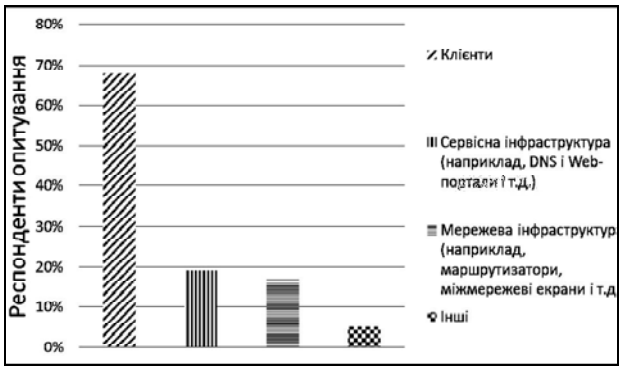
для управління ризиками інформаційної безпеки організації в контексті

загальних бізнес-ризиків організації;

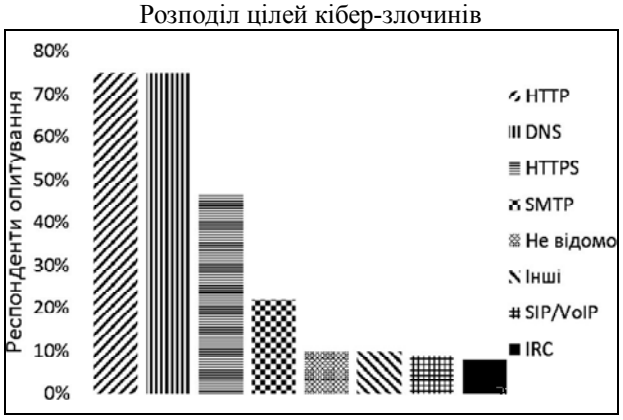
c) моніторингу та перегляді продуктивності та ефективності СУІБ (система управління інформаційної безпеки);

d) постійному вдосконаленні, основаному на об'єктивному вимірюванні.

Цей стандарт приймає модель "Плануй-Виконуй-Перевіряй-Дій" («Plan-Do-Check-Act»), надалі ПВПД (PDCA), яку застосовують для структуризації всіх процесів СУІБ. СУІБ забезпечує вибір адекватних і взаємопов'язаних заходів безпеки, які убезпечують інформаційні ресурси СУІБ та гарантують конфіденційність зацікавленим сторонам [14]. Основні етапи побудови СУІБ банку наведені на рис. 5. Проведений аналіз основних вимог стандарту визначає основні функції системи управління ІБ, які наведені на рис. 6 [14, 15].



Розподіл цілей кібер-злочинів



Цілі атак на прикладному рівні

Рис. 3. Типи атак
на послуги конфіденційності та цілісності

Механізми безпеки внутрішньоплатіжних системах комерційного банку України

Відповідно до міжнародних стандартів ISO 7498, ISO/IEC 10181 для забезпечення необхідних показників безпеки визначено п'ять базових загальноприйнятих послуг, основними з яких являються

лише дві: автентичність та цілісність, для їх забезпечення використовуються механізми безпеки, більшість з яких реалізується на основі криптографічних методів перетворення інформації.

Рис. 4. Загальна класифікація загроз комерційного банку

Рис. 5. Етапи побудови СУІБ комерційного банку

Рис. 6. Основні функції СУІБ комерційного банку

Основні механізми забезпечення цілісності та автентичності інформації в ВПС на різних рівнях засновані на використанні стандартів блочно-симетричних шифрів (3DES, ГОСТ 28147-89).

Прикладом програмної реалізації розглянутих механізмів є програмні засоби криптографічного захисту інформації “Грифон-Б” та “Грифон-Л” призначених для криптографічного захисту конфіденційної інформації в автоматизованих банківських системах та застосовується для обміну інформацією всередині корпоративної мережі банку, з клієнтами, що працюють з системою “Клієнт-Банк”, в системах обслуговування пластикових карт [2 – 5, 16, 17]. Програмний засіб криптографічного захисту інфор-

мації “Грифон-Л” [16] призначене для використання у сфері банківської діяльності, зокрема, для обміну конфіденційною (у т.ч. фінансової) інформацією всередині корпоративної мережі банку, з клієнтами, які працюють за системою “Клієнт-Банк”, в системах обслуговування пластикових карт та ін.

Бібліотека процедур криптографічного захисту інформації “Тайфун-PKCS#11” містить процедури, призначені для забезпечення захисту цілісності й конфіденційності інформації, виконання автентифікації відправників повідомлень із використанням механізмів криптографічного захисту (електронний цифровий підпис, шифрування, вироблення імітовставок і геш-функцій) шляхом вбудовування в конкретні прикладні системи [10].

Процедури. які входять до складу бібліотеки реалізують:

шифрування/розшифрування даних за алгоритмом ГОСТ 28147-89;

вироблення/перевірка імітовставки за алгоритмом ГОСТ 28147-89;

вироблення/перевірка ЕЦП за алгоритмами ДСТУ 4145-2002, ГОСТ 34.310-95, 34.311-95;

вироблення ключів шифрування за схемою Діффі-Хеллмана (використовується відкритий розподіл ключів відповідно до вимог ISO 11166-94).

Швидкісні характеристики програмних засобів, що реалізують алгоритми криптографічних перетворень (для ПЕВМ на базі Intel Celeron 2,4 ГГц):

швидкість шифрування/ розшифрування даних у режимі простої заміни БСШ ГОСТ 28147-89 не менш 8 Мбайт/с;

швидкість обчислення геш-функції даних відповідно до ГОСТ 34.311-95 не менш 3 Мбайт/с;

час вироблення ЕЦП відповідно до ГОСТ 34.310-95 при довжині ключа 512 біт не більш 0,003 с;

час перевірки ЕЦП відповідно до ГОСТ 34.310-95 при довжині ключа 512 біт не більш 0,006 с;

час вироблення ЕЦП відповідно до ГОСТ 34.310-95 при довжині ключа 1024 біт не більш 0,01 с;

час перевірки ЕЦП відповідно до ГОСТ 34.310-95 при довжині ключа 1024 біт не більш 0,02 с;

час вироблення ЕЦП (з обчисленням предпідпису) згідно ДСТУ 4145-2002 для основного поля степеня 163 не більш 0,0068 с;

час перевірки ЕЦП згідно ДСТУ 4145-2002 для основного поля степеня 163 не більш 0,013 с.

Криптографічні перетворення в бібліотеці “Тайфун-PKI PKCS#11” реалізуються з використанням об’єктної бібліотеки програмних процедур криптографічного захисту інформації “Тайфун-W32” версії 2.01.

Система захищеної електронної пошти “Бриз” призначена для здійснення обміну електронними повідомленнями у форматі SMF-70, захищеними з використанням механізмів криптографічного захисту (електронний цифровий підпис, шифрування/розшифрування, вироблення імітовставок), між клієнтами електронної пошти (ЕП), зареєстрованими на вузлах ЕП, через мережу передачі даних довільного типу й відповідає критеріям НД ТЗІ 2.5-004-99 [9].

Проведений аналіз стандартів показав, що для забезпечення конфіденційності, автентичності та цілісності використовується БСШ Російський ГОСТ 28147-89 – застарілий алгоритм симетричного шифрування, розроблений в 1989 році, крім того крипостійкість БСШ, ґрунтується на крипостійкості S-боксів, які для даного шифру “надходять” з Російської Федерації, що істотно впливає на безпеку ВПС в цілому.

На сьогоднішній день в Україні немає національних стандартів на алгоритми БСШ та формування геш-функцій, які використовуються в електронних цифрових підписах.

Так національний стандарт ЕЦП ДСТУ 4145 використовується з Російським стандартом формування геш-коду ГОСТ 34.311-95.

Розроблені національні стандарти ДСТУ-7624-2014 “Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення” – встановлює криптографічний алгоритм симетричного блокового перетворення для забезпечення конфіденційності та цілісності (як додаткової послуги) інформації під час її обробки.

Стандарт пропонується використовувати під час розробки засобів криптографічного захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, а також при модернізації діючих систем для заміни ДСТУ ГОСТ 28147:2009 дозволять суттєво змінити рівень інформаційної безпеки в СЕП; національний стандарт ДСТУ 7564-2014 “Інформаційні технології. Криптографічний захист інформації. Функція ґешування” установлює алгоритм обчислення ґешзначення для послідовностей двійкових символів, що застосовують в криптографічних методах захисту, для забезпечення цілісності та автентичності інформації під час її передавання, оброблення і зберігання, зокрема під час використання електронного цифрового підпису, що визначений ДСТУ 4145.

Стандарт використовують під час розробки засобів криптографічного захисту інформації в інформаційно-телекомунікаційних системах, а також при модернізації діючих систем для заміни функції ґешування згідно з ГОСТ 34.311 [12, 13].

На рис. 7 наведений взаємозв’язок між механізмами і вживаними стандартами у підсистемі безпеки ВПС.

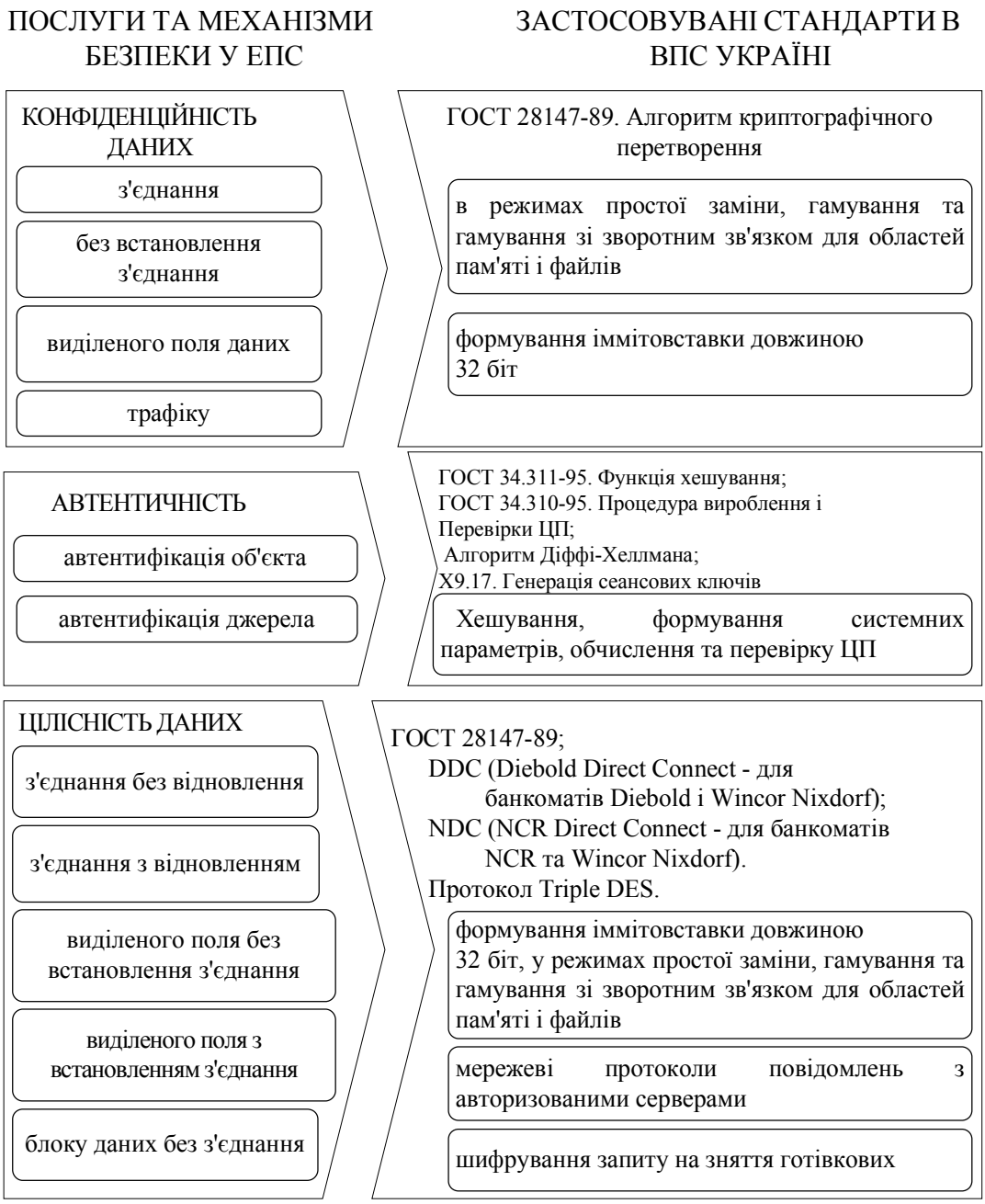


Рис. 7. Взаємозв'язок між механізмами і стандартами безпеки ВПС

Висновки

Таким чином, проведені дослідження показали, що подальший розвиток обчислювальних і ІТ-технологій приводять не тільки до збільшення зростання грошового обігу через банкомати та інші СЕП, розширенню послуг, які надаються через глобальну мережу Internet населенню, але й до модернізації старих, і появі нових видів загроз на елементи СЕП.

Для забезпечення безпеки банківської інформації у ВПС використовуються криптографічні симетричні й асиметричні алгоритми шифрування, що стандартизовані й сертифіковані Національним банком України.

Поява національних стандартів за спеціальними механізмами забезпечення інформаційної безпеки СЕП (шифрування, ЦП, цілісність даних, автентифікація) може суттєво вплинути на рівень забезпечення інформаційної безпеки банківських транзакцій і надійності СЕП у цілому.

Список літератури

1. Правила Національної системи масових електронних платежів, затверджені постановою Правління Національного банку України від 10.12.2004 № 620.

2. 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.

3. ГОСТ 34.311-95. Межгосударственный стандарт. Информационная технология. Криптографическая защита информации. Функция хеширования. Киев. Госстандарт Украины. 1998

4. ГОСТ Р 34.10-94. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма.

5. ГОСТ Р34.11-94. Информационная технология. Криптографическая защита информации. Функция хэширования.

6. Криптография в банковском деле. / М.И. Анохин, Н.П. Варновский, В.М. Сидельников, В.В. Ященко. – М.: МИФИ. 1997. – 274 с.

7. Аволио Ф.М. Защита информации на предприятии / Ф.М. Аволио, Г. Шипли // Сети и системы связи. – 2000. − № 8. – С. 91−99.

8. Диффи У. Защищенность и имитостойкость / У. Диффи, М. Хеллман // Введение в криптографию. – 1979. – № 3. − С. 79–109.

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

10. Задірака В.К. Методи захисту банківської інформації. / В.К. Задірака, О.С. Олесюк, Н.О. Недашковський. – К.: Вища школа, 1999. – 264 с.

11. Корченко А.О. Банківська безпека / А.О. Корченко, Л.М. Скачек, В.О. Хорошко; за загальним ред. д.т.н. проф. В.О. Хорошка. – К: ПВП "Задруга", 2014. – 185 с.

12. Національний Стандарт України ДСТУ 7624-2014. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. К:. 2014. – 235 с.

13. Національний Стандарт України ДСТУ 7564-2014. Інформаційні технології. Криптографічний захист інформації. Функція гешування. К:. 2014. – 41 с.

14. Стандарт України СОУ Н НБУ 65.1 СУІБ 1.0:2010. Методи захисту в банківській діяльності система управління інформаційною безпекою. Вимоги. (ISO/IEC 27001:2005, MOD).К: НБУ., 2010. – 67 с.

15. Стандарт України СОУ Н НБУ 65.1 СУІБ 1.0:2010. Звід правил для управління інформаційною безпекою (ISO/IEC 27002:2005, MOD)).К: НБУ., 2010. – 209 с.

16. Программное средство криптографической защиты информации "Грифон-Б" [Електронний ресурс]. – Режим доступу: http://www.banksoft.com.ua/index.php?id=28.

17. Программное средство «Библиотека функций криптографической защиты информации "Грифон-Л" Електронний ресурс]. – Режим доступу: http://www.banksoft.com.ua/index.php?id=27.

18. 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

19. Worldwide Infrastructure Security Report. 2014. Arbor Networks, Inc Електронний ресурс]. – Режим доступу: https://www.google.com.ua/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CB8QFjAA&url=http%3A%2F%2Fpages.arbornetworks.com%2Frs%2Farbor%2Fimages%2FWISR2014_EN2014.pdf&ei=DyR2VfznJOPgyQOghoN4&usg=AFQjCNGP0_ZTliItqCtofJ-cXfZT9QHRiQ&sig2=4hgA_vIye1idQyQgsTIZXg&bvm=bv.95039771,d.bGQ.

Надійшла до редколегії 19.05.2015

Рецензент: д-р техн. наук, проф. В.А. Хорошко, Національний авіаційний університет, Київ.

АНАЛИЗ УГРОЗ И МЕХАНИЗМОВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В СИСТЕМЕ ЭЛЕКТРОННЫХ ПЛАТЕЖЕЙ КОММЕРЧЕСКОГО БАНКУ УКРАИНЫ

О.Г. Король

Рассматриваются основные угрозы и механизмы обеспечения безопасности банковских транзакций в системах электронных платежей (СЭП) коммерческих банков Украины. Проводится анализ основных требований стандарта СОУ Н НБУ 65.1 СУИБ 1.0: 2010 соответствующего стандарту ISO / IEC 27001: 2005 Information technology - Security techniques - Information security management systems - Requirements по формированию основных требований и функций построения системы управления информационной безопасностью (СУИБ).

Ключевые слова: *механизмы обеспечения безопасности, аутентичность, целостность, конфиденциальность, внутриплатежные системы коммерческого банка Украины.*

ANALYSIS OF THREATS AND SECURITY ARRANGEMENTS INFORMATION IN ELECTRONIC PAYMENT SYSTEMS UKRAINIAN COMMERCIAL BANKS

O.G. Korol

The main threats and security mechanisms of banking transactions in the electronic payment system (EPS) of commercial banks in Ukraine. The analysis of the main requirements of the standard SDA H NBU 65.1 ISMS 1.0: 2010 quality standard ISO / IEC 27001: 2005 Information technology - Security techniques - Information security management systems - Requirements for the formation and functions of the basic requirements of building information security management system (ISMS).

Keywords: *security arrangements, authenticity, integrity, confidentiality, commercial banking system of Ukraine.*