УДК 621.391
DOI: 10.15587/1729-4061.2015.51468

АНАЛИЗ ЗАКОНОДАТЕЛЬНОЙ БАЗЫ К СИСТЕМЕ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ НСМЭП

С. П. Евсеев, Г. П. Коц, О. Г. Король

АНАЛІЗ ЗАКОНОДАВЧОЇ БАЗИ ДО СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ НСМЭП

С. П. Євсєєв, Г. П. Коц, О. Г. Король

ANALYSIS OF THE LEGAL FRAMEWORK FOR INFORMATION SECURITY MANAGEMENT SYSTEM OF THE NSMEP

S. Evseev, G. Kotz, O. Korol

Розглядаються законодавчі акти у сфері захисту банківських транзакцій в національній системі масових електронних платежів (НСМЕП), її структура. Проводиться аналіз основних джерел загроз конфіденційності, цілісності та доступності даних, розглядаються основні вимоги стандартів до функцій системи управління інформаційною безпекою, програмні засоби технічних систем безпеки інформації в банківських інститутах Національного банку України.

Ключові слова: інформаційна безпека банківських транзакцій, загрози банківських даних.

Рассматриваются законодательные акты в области защиты банковских транзакций в национальной системе массовых электронных платежей (НСМЭП), ее структура. Проводится анализ основных источников угроз конфиденциальности, целостности и доступности данных, рассматриваются основные требования стандартов к функциям системы управления информационной безопасностью, программные средства технических систем безопасности информации в банковских институтах Национального банка Украины.

Ключевые слова: информационная безопасность банковских транзакций, угрозы банковских данных.

1. Введение

Развитие конкурентоспособной экономики любого государства тесно связано с вычислительными возможностями систем государственных и коммерческих банков. Банковский сектор в последнее десятилетие на основе стремительного роста цифровых технологий значительно расширил перечень услуг, предоставляемых институтам государства и населению. Появление

новых финансовых услуг связано с развитием Национальной системы электронных платежей – внутригосударственной банковской многоэмитентной платежной системой массовых платежей, выполняющей функции перевода средств по операциям, инициированным применением платежных карточек, обеспечением высокой безопасности, надежности, скорости и экономической эффективности выполнения операций с применением платежных карточек [1]. При этом решение вопросов обеспечения безопасности транзакций в банковских системах как в коммерческих банках Украины, так и в НСМЭП, остается актуальной и на сегодняшний день.

2. Анализ литературных данных и постановка проблемы

Компьютерные системы и телекоммуникации обеспечивают надежность функционирования огромного количества информационных систем самого разного назначения. Большинство таких систем несут в себе информацию, имеющую конфиденциальный характер. Таким образом, решение задачи автоматизации процессов обработки данных повлекло за собой новую проблему – проблему информационной безопасности [1]. Со времени своего появления банки неизменно вызывали преступный интерес. И этот интерес был связан не только с хранением в кредитных организациях денежных средств, но и с тем, что в банках сосредотачивалась важная и зачастую секретная информация о финансовой и хозяйственной деятельности многих людей, компаний, организаций и даже целых государств. Компьютеризация банковской деятельности позволила значительно повысить производительность труда сотрудников банка, внедрить новые финансовые продукты и технологии. Однако прогресс в технике преступлений шел не менее быстрыми темпами, чем развитие банковских технологий. В настоящее время свыше 90% всех преступлений связана с использованием автоматизированных систем обработки информации банка (АСОИБ) [2]. Защита собственно банковской системы должна использовать мощные средства аутентификации и контроля действий как внутренних пользователей, так и клиентов. Общепринято, что наиболее надежную защиту могут обеспечить средства двухфакторной аутентификации, будь то электронные ключи (токены) или генераторы одноразовых паролей. Безопасность данных при хранении требует использования средств шифрования, которые смогут работать либо на уровне хранилищ данных, либо на уровне отдельных компонентов системы, например, таблиц баз данных. Безопасность банкоматов и платежных терминалов должна обеспечиваться с использованием традиционных средств – антивирусной защиты. Но в то же время специфика таких устройств требует применения дополнительных средств защиты, включая создание “замкнутой программно-аппаратной среды”, полностью исключающей установку любого стороннего ПО и подключение внешних устройств [3]. Для обеспечения адекватности системы защиты информации целесообразно применять принципы Риск-менеджмента. Данный метод позволит, при грамотном подходе определить и классифицировать угрозы и, в соответствии с вероятностью наступления негативных последствий и их возможной тяжестью для Банка, организовывать Систему защиты. К

сожалению, на сегодня принципы Риск-менеджмента в сфере защиты информации еще не очень совершенны [4]. На практике обеспечение информационной безопасности происходит в условиях случайного воздействия факторов, которые в полной мере сложно предусмотреть заранее при проектировании системы защиты информации, но в дальнейшем они способны снизить эффективность предусмотренных проектом мер информационной безопасности или полностью скомпрометировать их.

Одной из существенных проблем при проектировании и эксплуатации систем защиты информации является игнорирование методологии системного анализа в отношении средств и инструментов для их защиты. Следует признать сложность, а иногда и невозможность объективного подтверждения эффективности системы защиты информации, что во многом определяется неполнотой нормативно-методического обеспечения информационной безопасности, прежде всего в области показателей и критериев [5]. Международный стандарт для операций по банковским картам с чипом (EMV), введенный в 2005 году, определяет физическое, электронное и информационное взаимодействие между банковской картой и платёжным терминалом для финансовых операций на основе стандартов ISO/IEC 7816 для контактных карт, и ISO/IEC 14443 для бесконтактных карт. Интернет-банкинг широко распространился среди банков и клиентов. Использование Интернет-ресурсов в качестве альтернативного средства передачи пин-кода клиента в банк не только приводит к снижению затрат на передачу, но и позволяет улучшить банковскую конкурентоспособность и увеличить гибкость работы банка с клиентами. Главными препятствиями на пути интернет-банкинга являются безопасность системы, отсутствие доверия и правовой поддержки [6]. В работе [7] отмечается, что безопасность информации может быть обеспечена лишь при комплексном использовании всего арсенала имеющихся средств защиты во всех структурных элементах производственной системы и на всех этапах технологического цикла обработки информации. Наибольший эффект достигается тогда, когда все используемые средства, методы и меры объединяются в единый целостный механизм — систему защиты информации (СЗИ). При этом функционирование системы должно контролироваться, обновляться и дополняться в зависимости от изменения внешних и внутренних условий.

3. Цели и задачи исследования

Целью работы является анализ основных законодательных актов в сфере защиты банковских транзакций в национальной системе электронных платежей (НСМЭП), ее структуры, определение основных источников угроз конфиденциальности и целостности данных, рассмотрение основных требований национальных стандартов к функциям системы управления информационной безопасностью (СУИБ).

Для достижения поставленной цели были поставлены следующие задачи:

– провести анализ законодательных актов в сфере защиты банковских

транзакций в национальной системе электронных платежей (НСМЭП), ее структуры;

– анализ основных источников угроз безопасности данных в НСМЭП;

– проанализировать основные требований национальных стандартов к функциям системы управления информационной безопасностью (СУИБ);

– анализ основных механизмов безопасности информации в НСМЭП.

4. Анализ основных законодательных актов в сфере защиты банковских транзакций в национальной системе электронных платежей (НСМЭП), ее структуры

Национальный банк Украины на основе стандарта СОУ Н НБУ 65.1 СУИБ 1.0: 2010, который соответствует стандарту ISO / IEC 27001: 2005 Information technology – Security techniques – Information security management systems – Requirements в 2010 году создал национальную систему массовых электронных платежей (НСМЭП НБУ). НСМЭП действует в соответствии с Законами Украины “О Национальном банке Украины”, “О банках и банковской деятельности”, “О платежных системах и переводе средств в Украине”, другими законодательными актами Украины и нормативно-правовыми актами Национального банка Украины и определена как внутригосударственная банковская многоэмитентная платежная система массовых платежей [8–10].

Деятельность НСМЭП обеспечивается и регулируется организационной структурой АПК (аппаратно-программный комплекс – совокупность составляющих компонентов (подсистем, блоков, элементов), функционально определенных на уровне информационной структуры, взаимодействующих в соответствии с информационными технологиями и определенными правилами (регламентами, инструкциями и т.п.) обеспечивает реализацию основных функций НСМЭП), нормативной базой, представленной на рис. 1.

Для проведения платежей в системе используется специальное платежное средство – платежная карточка НСМЭП, обеспечивающая взаимозачет на основе клиринга (процедура финансовых оборотов, в которой клиринговый субъект работает в качестве посредника, и принимает на себя роль покупателя и продавца в данной транзакции с целью обеспечения заказов между двумя сторонами) [1, 10].

Основным нормативно-правовым актом Национального банка Украины, определяющим общие требования по функционированию в Украине НСМЭП и порядка выполнения межбанковского перевода средств через корреспондентские счета банков-резидентов в национальной валюте Украины является "Инструкция о межбанковском переводе средств в Украине в национальной валюте", утвержденной постановлением Правления Национального банка Украины от 16.08.2006 № 320 и зарегистрированной в Министерстве юстиции Украины 06.09.2006 за № 1035/12909 (с изменениями).

НСМЭП обеспечивает осуществление расчетов в пределах Украины между банками как по поручениям клиентов банков, так и по обязательствам банков. СЭП выполняет межбанковский перевод в файловом режиме и в режиме реального времени. Осуществление банком начальных платежей в файловом

режиме является обязательным, а в режиме реального времени – по его выбору. Вместе с тем, банк, работающий в НСМЭП в файловом режиме, обеспечивает прием платежей в режиме реального времени.

В *файловом режиме обмен* платежными документами организовано в пакетном режиме технологическими циклами путем приема-передачи соответствующих документов. Продолжительность цикла составляет 15 – 20 минут. В *режиме реального времени* средства зачисляются на счет получателя немедленно, в момент поступления платежа от отправителя НСМЭП. Именно это является главным признаком платежных систем класса RTGS согласно международной классификации.

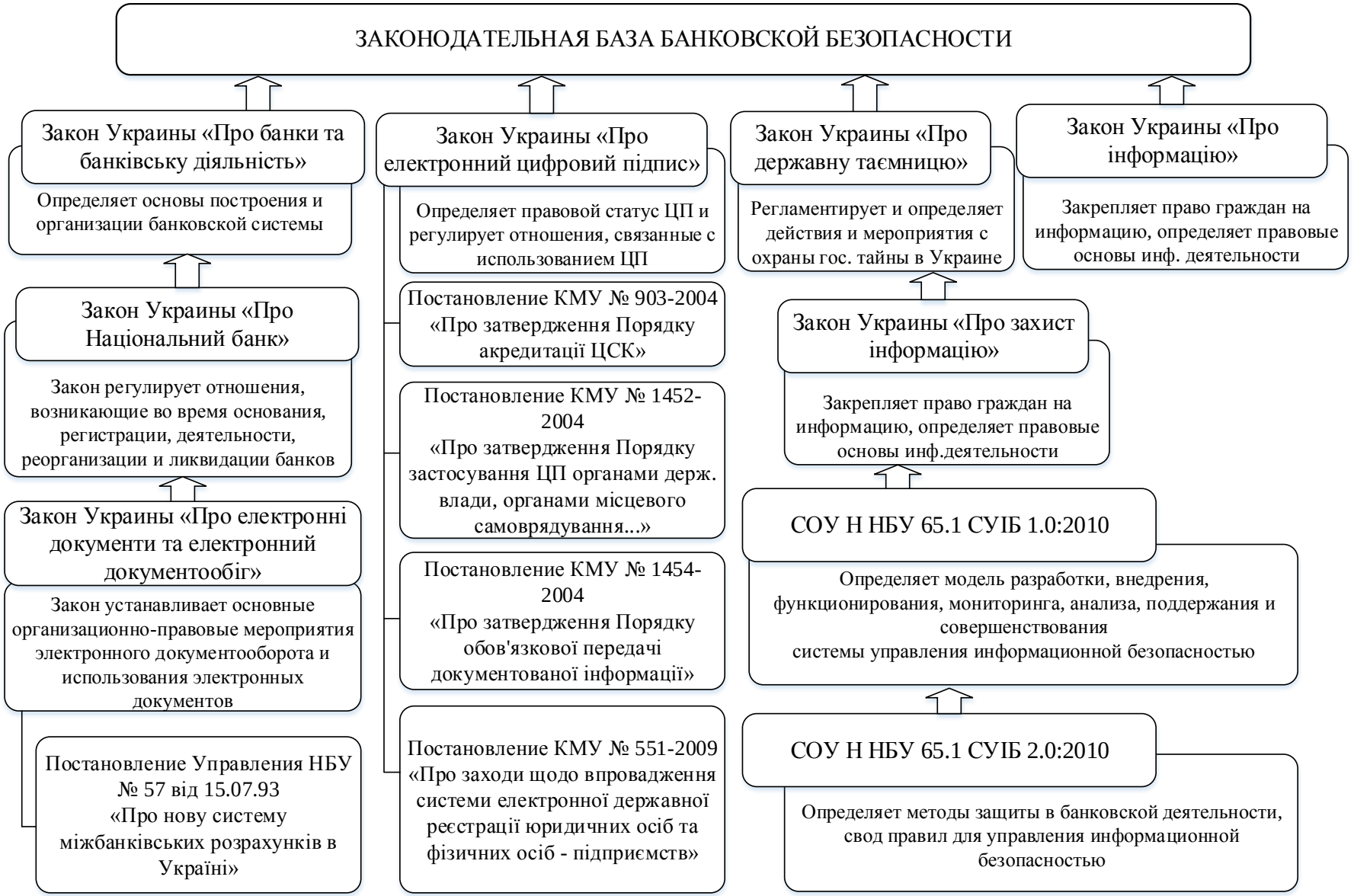


Рис. 1. Нормативная база НСЭП

За 9 месяцев 2009 года в среднем за день обрабатывалось 1239 тысяч начальных платежей и электронных расчетных сообщений на сумму 24 139 млн. гривен, в том числе среднесуточная загруженность:

в *файловом режиме* составила за количество 1 238 000 начальных платежей и электронных расчетных сообщений на сумму 22 345 млн. Гривен,

что соответственно меньше на 12% по количеству и на 29 % по сумме, чем за 9 месяцев 2008 года;

в *режиме реального времени* составляла 1000 начальных платежей и электронных расчетных сообщений на сумму тысячу семьсот девяносто четыре млн. грн., что на 67% меньше по количеству и в 2 раза больше по сумме, чем в соответствующем периоде 2008 года.

Среднедневной остаток средств на счетах участников системы составил 23 млрд. гривен. Среднесуточный коэффициент оборота средств по счетам участников системы составил 1,06.

Анализ статистических данных работы системы электронных платежей Национального банка по переводу средств между банками свидетельствует о том, что система в течение 9 месяцев 2009 года успешно выполняла возложенные на нее функции государственной системы межбанковских расчетов, удовлетворяла потребности его участников в переводе средств, обеспечивала максимальную скорость, прозрачность, высокий уровень безопасности и надежности проведения платежей [22].

Организационная структура НСМЭП – совокупность определенных Платежной организацией субъектов, их функций, прав и обязанностей, а также совокупность отношений, возникающих между ними при проведении перевода средств и обеспечения деятельности НСМЭП [1].

В состав НСМЭП входят:

– *Платежная организация НСМЭП* – юридическое лицо, являющееся владельцем или, получила право на использование знака для товаров и услуг НСМЭП (и других знаков, идентифицирующих принадлежность платежных карточек к НСМЭП, и которая определяет правила работы НСМЭП, а также выполняет другие функции по обеспечению деятельности НСМЭП и несет ответственность в соответствии с законодательством Украины и заключенным ею договорам);

– *Члены НСМЭП* – эмитенты и эквайры;

– *Участники НСМЭП*:

Расчетный банк НСМЭП (Национальный банк Украины выполняет функции Платежной организации и Расчетного банка НСМЭП и осуществляет контроль над ее функционированием)

– *Главный процессинговый центр НСМЭП (ГПЦ)* – юридическое лицо, которое на основании надлежащим образом оформленного права (заключенного с Платежной организацией договора, полученного от нее разрешения, лицензии и т.п.) осуществляет процессинг, а также выполняет функции клирингового учреждения НСМЭП;

– *Региональный процессинговый центр НСМЭП (РПЦ)* – юридическое лицо, которое на основании надлежащим образом оформленного права

(заключенного с Платежной организацией договора, полученного от нее разрешения, лицензии и т.п.) осуществляет процессинг и выполняет клиринг для отдельной группы членов НСМЭП, определенных Платежной организацией по соответствующему признаку (территориальное расположение, организационная структура и т.д.);

– *Процессинговый центр банковского уровня (БПЦ)* – юридическое лицо, которое на основании надлежащим образом оформленного права (заключенного с Платежной организацией договора, полученного от нее разрешения, лицензии и т.п.) осуществляет процессинг и выполняет по договору (ам) с эмитентом (ами) и/или эквайром (ами) их информационное обслуживание.

– *Технические эквайры* (эквайринговые компании)

– *Предприятия торговли и сферы услуг* (торговцы)

– *Держатели платежных карточек*.

Структурная схема НСМЭП представлена на рис. 2.

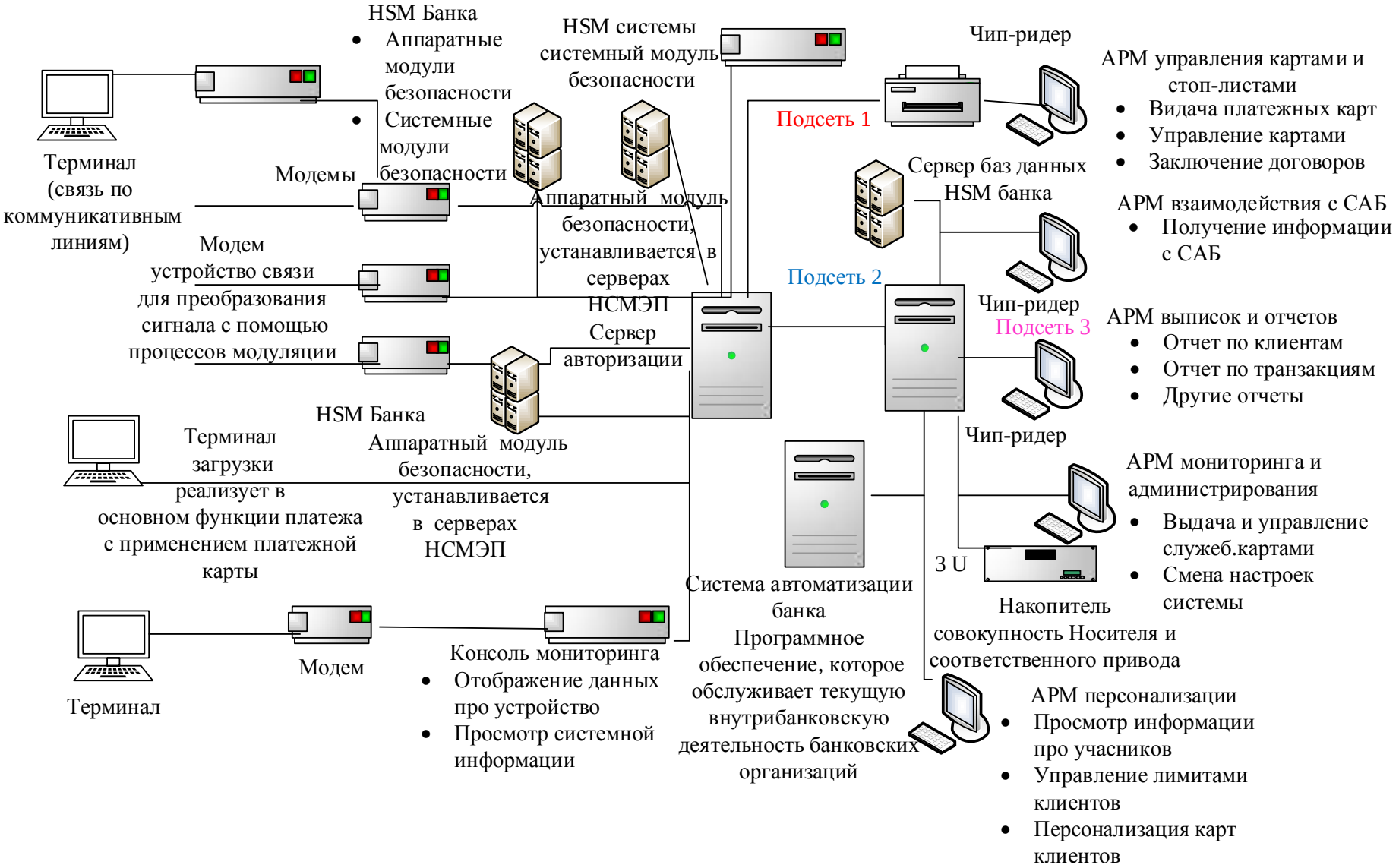


Рис. 2. Структура НСЭП

Проведенный анализ организационной структуры НСМЭП показал, что в основе выполнения функций ее работы используется *автоматизированная карточная система (АКС)* – программно-технический комплекс, с помощью которого обеспечивается выполнение функций членом(ами) или участником(ами) НСМЭП относительно эмиссии карточек, обработки информации по операциям с их применением, управления терминалами и банкоматами и т. д.). Такая система относится к сложным многоуровневым системам управления критического применения (СУКП), в которых передача информации требует контроля безопасности на каждом уровне[1].

Данная система интегрируется в банковские системы и множество типов терминалов, в том числе переносные, работающие в автономном режиме, и банкоматы, выполняющие более широкий спектр функций. НСМЭП управляет потоками электронных денег, связью терминалов и локальных сетей. Для обеспечения надежной работы электронная платежная система должна быть надежно защищена. С точки зрения информационной безопасности в НСМЭП существуют следующие уязвимые места:

– пересылка платежных и других сообщений между банком и клиентом и между банками;

– обработка информации внутри организаций отправителя и получателя сообщений;

– доступ клиентов к средствам, аккумулированным на счетах.

5. Анализ основных источников угроз безопасности данных в НСМЭП

Несмотря на широкое применение различных криптографических алгоритмов на различных уровнях защиты НСМЭП подвержена различным угрозам, общая классификация угроз приведена на рис. 3 [10].

Проведенный анализ показал, что одним из наиболее уязвимых мест в системе электронных, платежей является пересылка платежных и других сообщений между банками, между банком и банкоматом, между банком и клиентом, связанная со следующими особенностями:

– внутренние системы организаций отправителя и получателя должны быть приспособлены для отправки и получения электронных документов и обеспечивать необходимую защиту при их обработке внутри организации (защита оконечных систем);

– взаимодействие отправителя и получателя электронного документа осуществляется опосредовано через канал связи.

Эти особенности порождают следующие проблемы:

– взаимное опознавание абонентов (проблема установления взаимной подлинности при установлении соединения);

– защита электронных документов, передаваемых по каналам связи (проблемы обеспечения конфиденциальности и целостности документов);

– защита процесса обмена электронными документами (проблема доказательства отправления и доставки документа);

– обеспечение исполнения документа (проблема взаимного недоверия между отправителем и получателем из-за их принадлежности к разным

организациям и взаимной независимости) [3].

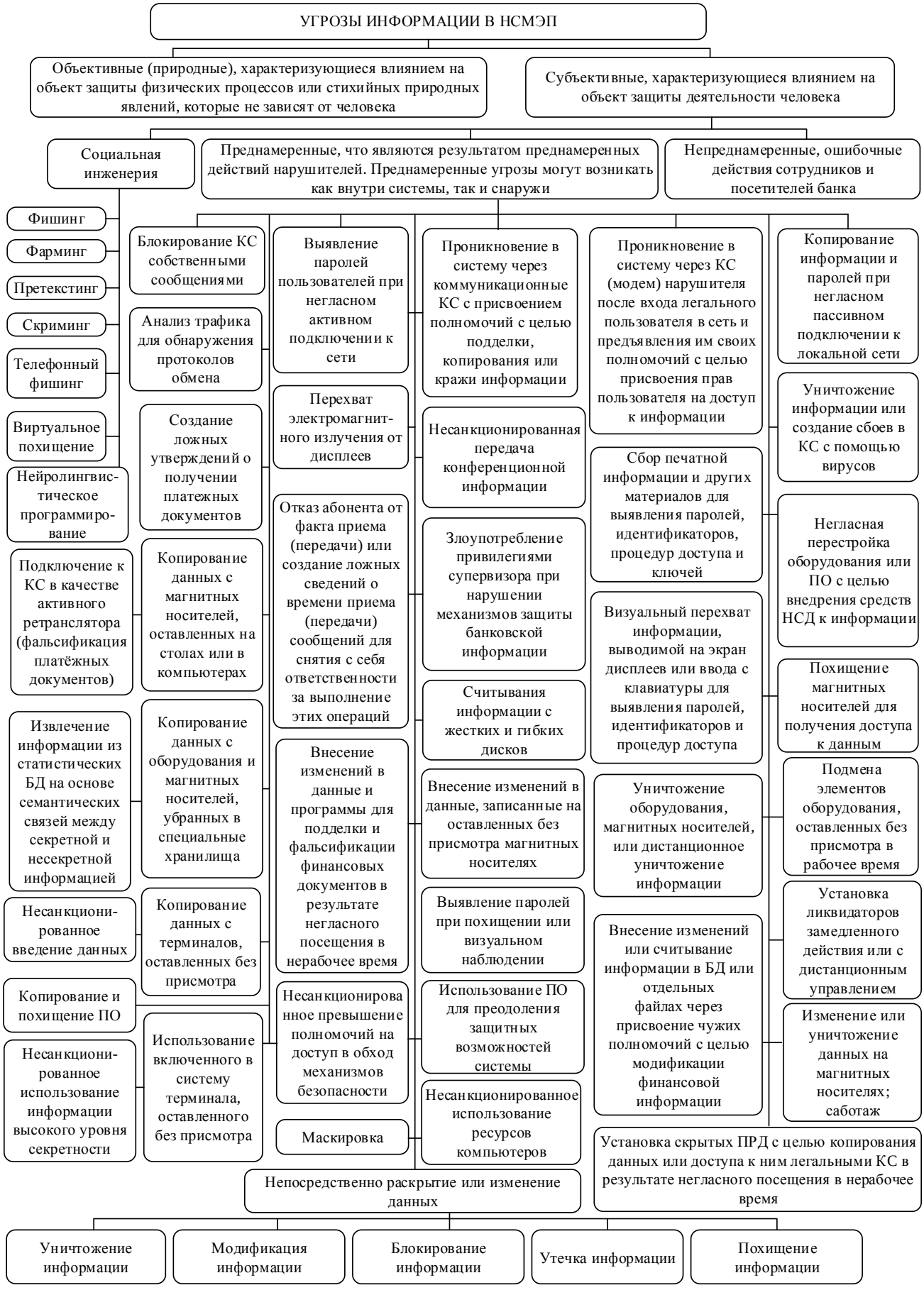
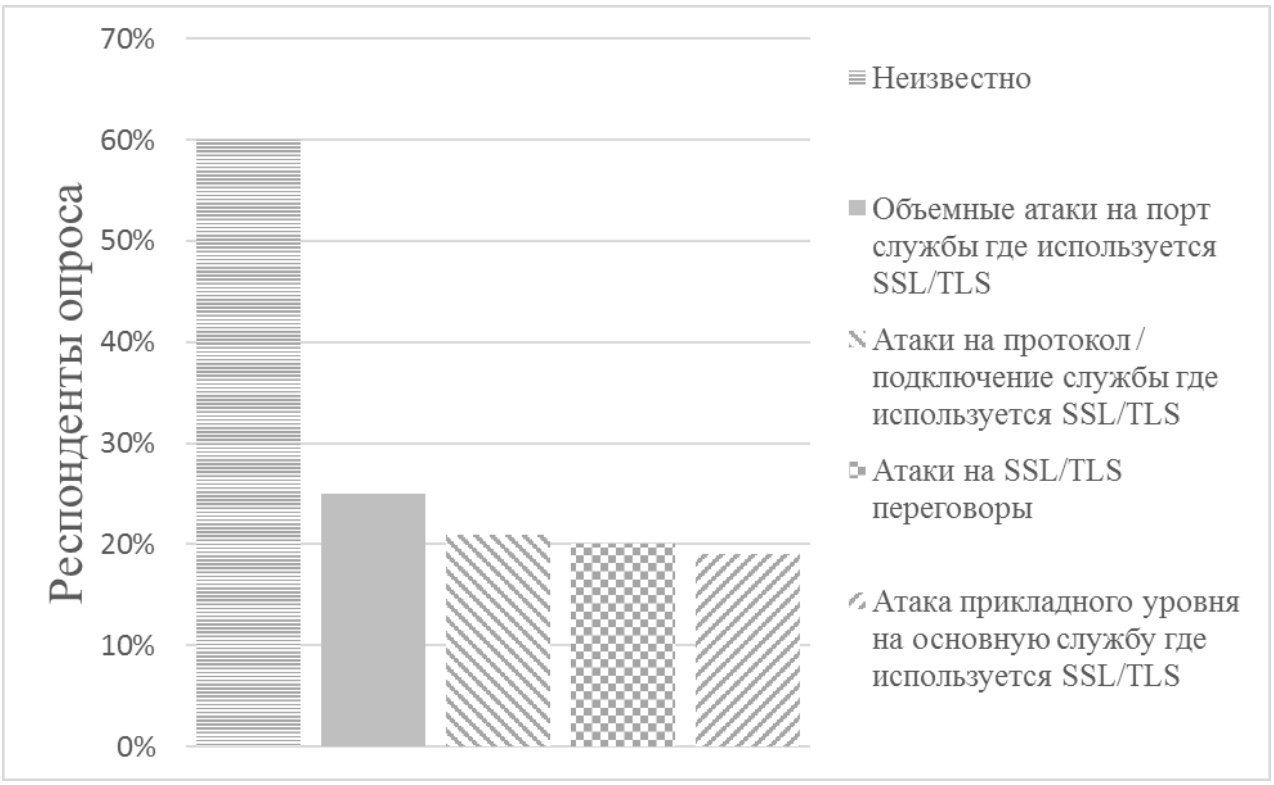
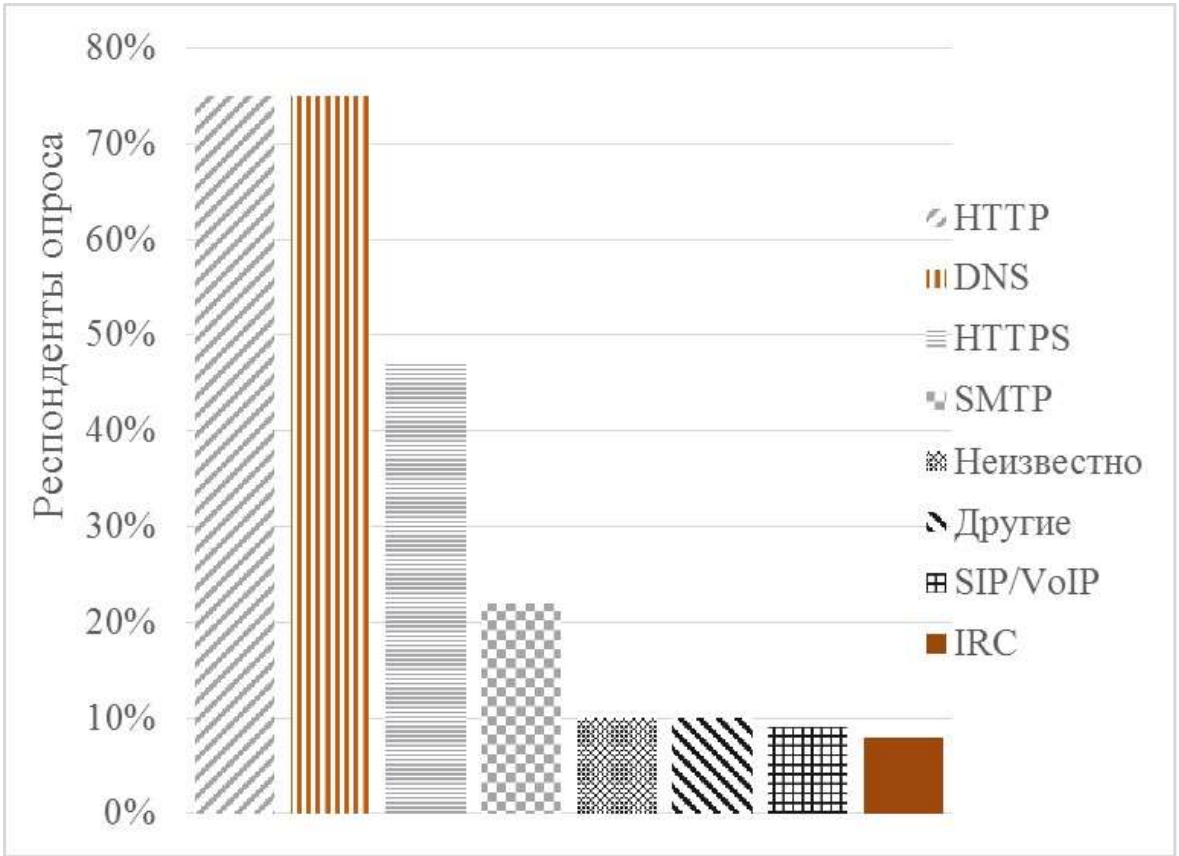


Рис. 3. Основные виды угроз

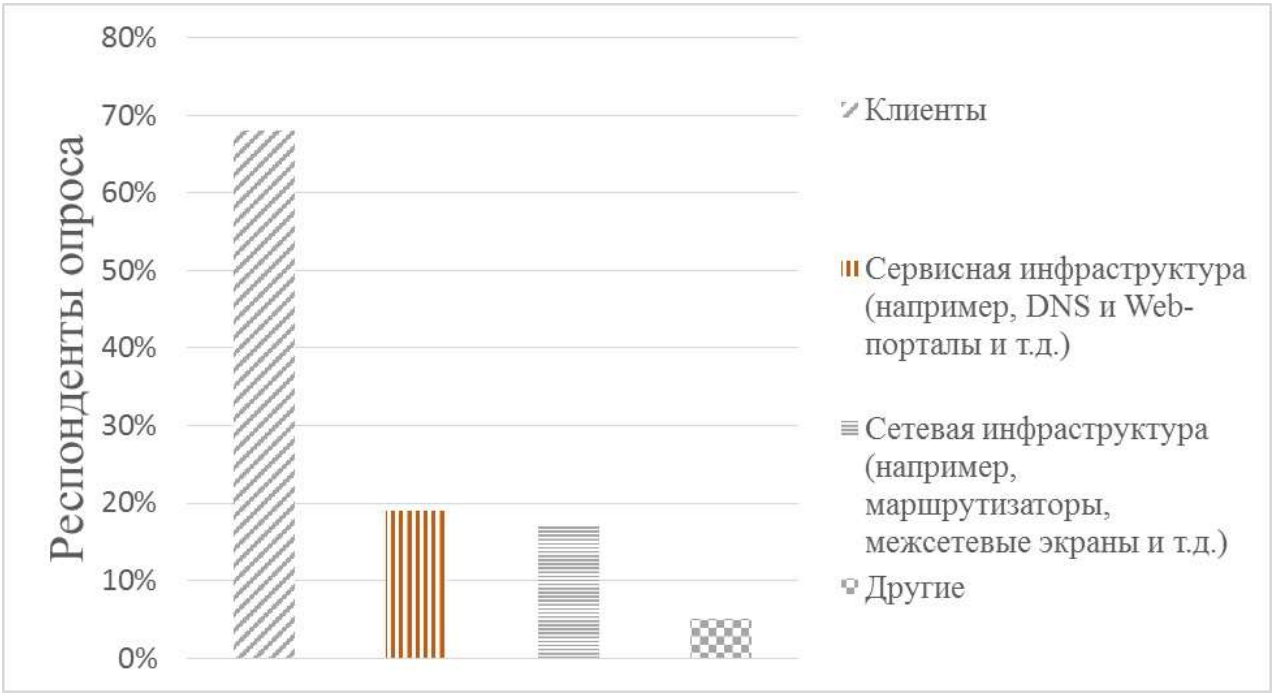
Результаты исследований компании “Arbor Networks” атак на компьютерные сети приведены на рис. 4, а-в.



а



б



в

Рис. 4. Анализ атак на компьютерные сети: а – типы атак на услуги конфиденциальности и целостности (респонденты опроса: 0,6 – неизвестно; 0,25 – объемные атаки на порт службы с использованием протоколов SSL/TLS; 0,21 – атаки на протокол/подключение службы с использованием протоколов SSL/TLS; 0,2 – атаки на протоколы SSL/TLS переговоров; 0,19 – атака прикладного уровня на основную службу где используется протоколы SSL/TLS); б – цели атак на прикладном уровне (респонденты опроса: 0,75 – HTTP; 0,75 – DNS; 0,47 – HTTPS; 0,22 – SMTP; 0,1 – другие; 0,1 – неизвестно; 0,09 – SIP/VoIP; 0,08 – IRC); в – распределение целей кибер-преступлений (респонденты опроса: 0,68 – клиенты; 0,19 – сервисная инфраструктура (DNS и Web-порталы и т.д.); 0,17 – сетевая инфраструктура (маршрутизаторы, межсетевые экраны и т.д.); 0,05 – другие

На рис. 5 представлен анализ первоочередных целей злоумышленников при атаках на элементы банковских систем и на элементы НСМЭП.

Рис. 5. Первоочередные цели злоумышленников при атаках на элементы НСМЭП

Результаты исследований показывают, что основные атаки направлены на получение злоумышлениками конфиденциальной (коммерческой) информации на всех промежуточных узлах корпоративных систем с использованием взлома основных протоколов обеспечения услуг конфиденциальности, целосности и доступности.

6. Основные требований национальных стандартов к функциям системы управления информационной безопасностью (СУИБ)

В соответствии со стандартом СОУ Н НБУ 65.1 СУИБ 1.0: 2010 руководству коммерческих банков предлагается процессный подход к

управлению информационной безопасностью, поощряет его пользователей делать упор на важности [8, 9]:

– понимания требований информационной безопасности организации и необходимости разработки политики и целей информационной безопасности;

– осуществления безопасности и обеспечения их функционирования для управления угрозами информационной безопасности организации в контексте общих бизнес-угроз банка;

– мониторинга и просмотра производительности и эффективности СУИБ (система управления информационной безопасности);

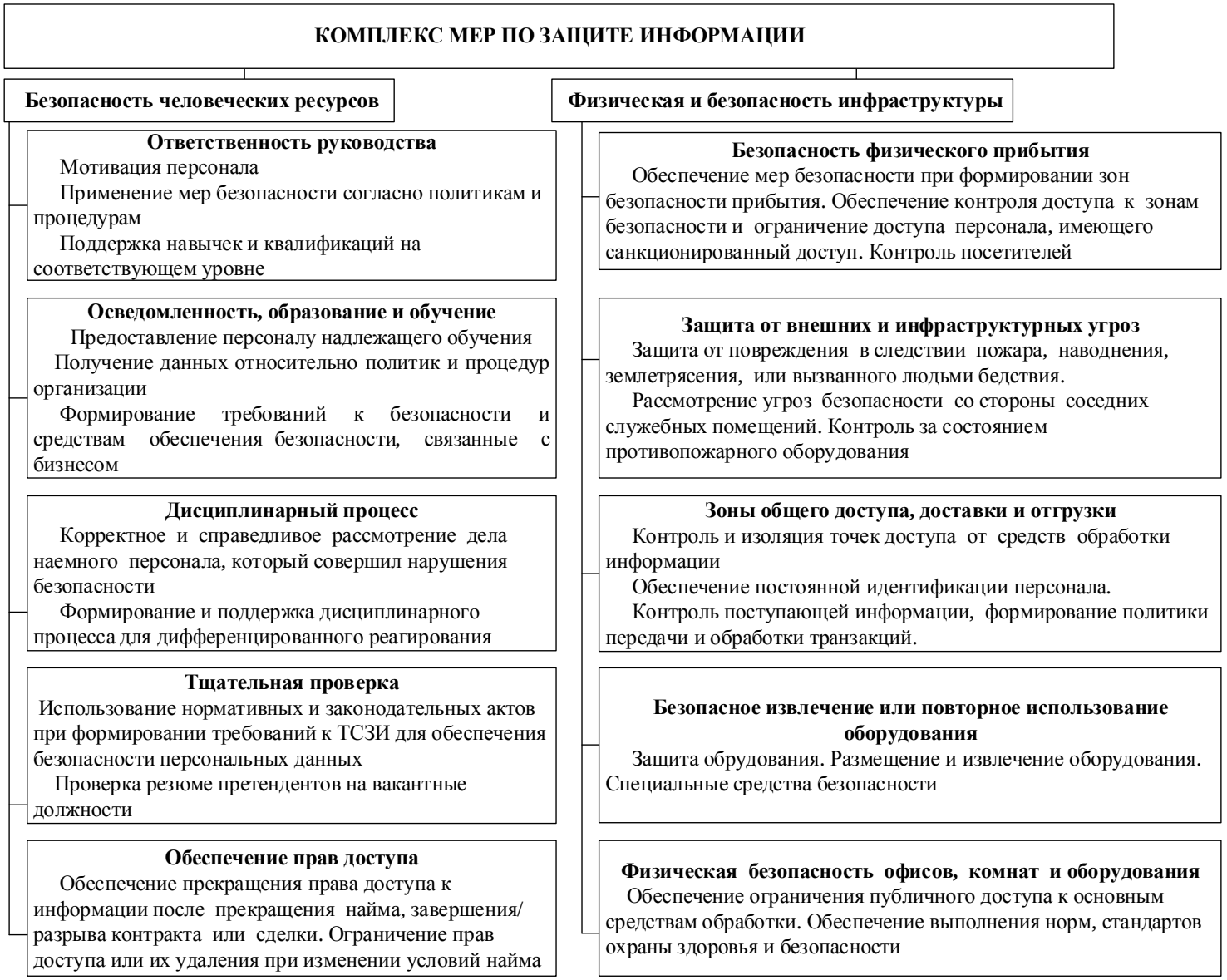
– постоянном совершенствовании, основанном на объективном измерении. Стандарт принимает модель “Планируй-Выполняй-Проверяй-Действуй” (“Plan-Do-Check-Act”), в дальнейшем ПВПД (PDCA), которую применяют для структуризации всех процессов СУИБ. СУИБ обеспечивает выбор адекватных и взаимосвязанных мер безопасности, которые защищают информационные ресурсы СУИБ и гарантируют конфиденциальность заинтересованным сторонам [8]. Основные этапы построения СУИБ банка приведены на рис. 6.

Рис. 6. Этапы построения СУИБ коммерческого банка

Принятие модели ПВПД (PDCA) отображает принципы, установленные Руководством ОЕСР, регулирующих безопасность информационных систем и сетей. Этот стандарт предоставляет надежную модель для внедрения принципов этой установки, влияющие на оценку рисков, проектирование и внедрение безопасности, управление безопасностью и повторную ее оценку.

Проведенный анализ основных требований стандарта определяет основные функции системы управления ИБ, которые приведены на рис. 7 [8, 9], а также на основе рекомендаций стандарта СОУ Н НБУ 65.1 СУИБ 2.0: 2010 определить основные методы защиты в банковской деятельности, приведенные на рис. 8 а, б.

Рис. 7. Основные функции СУИБ коммерческого банка


КОМПЛЕКС МЕР ПО ЗАЩИТЕ ИНФОРМАЦИИ
Безопасность человеческих ресурсов
Ответственность руководства
Мотивация персонала
Применение мер безопасности согласно политикам и процедурам
Поддержка навычек и квалификаций на соответствующем уровне
Осведомленность, образование и обучение
Предоставление персоналу надлежащего обучения
Получение данных относительно политик и процедур организации
Формирование требований к безопасности и средствам обеспечения безопасности, связанные с бизнесом
Дисциплинарный процесс
Корректное и справедливое рассмотрение дела наемного персонала, который совершил нарушения безопасности
Формирование и поддержка дисциплинарного процесса для дифференцированного реагирования
Тщательная проверка
Использование нормативных и законодательных актов при формировании требований к ТСЗИ для обеспечения безопасности персональных данных
Проверка резюме претендентов на вакантные должности
Обеспечение прав доступа
Обеспечение прекращения права доступа к информации после прекращения найма, завершения/ разрыва контракта или сделки. Ограничение прав доступа или их удаления при изменении условий найма
Физическая и безопасность инфраструктуры
Безопасность физического прибытия
Обеспечение мер безопасности при формировании зон безопасности прибытия. Обеспечение контроля доступа к зонам безопасности и ограничение доступа персонала, имеющего санкционированный доступ. Контроль посетителей
Защита от внешних и инфраструктурных угроз
Защита от повреждения в следствии пожара, наводнения, землетрясения, или вызванного людьми бедствия.
Рассмотрение угроз безопасности со стороны соседних служебных помещений. Контроль за состоянием противопожарного оборудования
Зоны общего доступа, доставки и отгрузки
Контроль и изоляция точек доступа от средств обработки информации
Обеспечение постоянной идентификации персонала.
Контроль поступающей информации, формирование политики передачи и обработки транзакций.
Безопасное извлечение или повторное использование оборудования
Защита обрудования. Размещение и извлечение оборудования. Специальные средства безопасности
Физическая безопасность офисов, комнат и оборудования
Обеспечение ограничения публичного доступа к основным средствам обработки. Обеспечение выполнения норм, стандартов охраны здоровья и безопасности

а

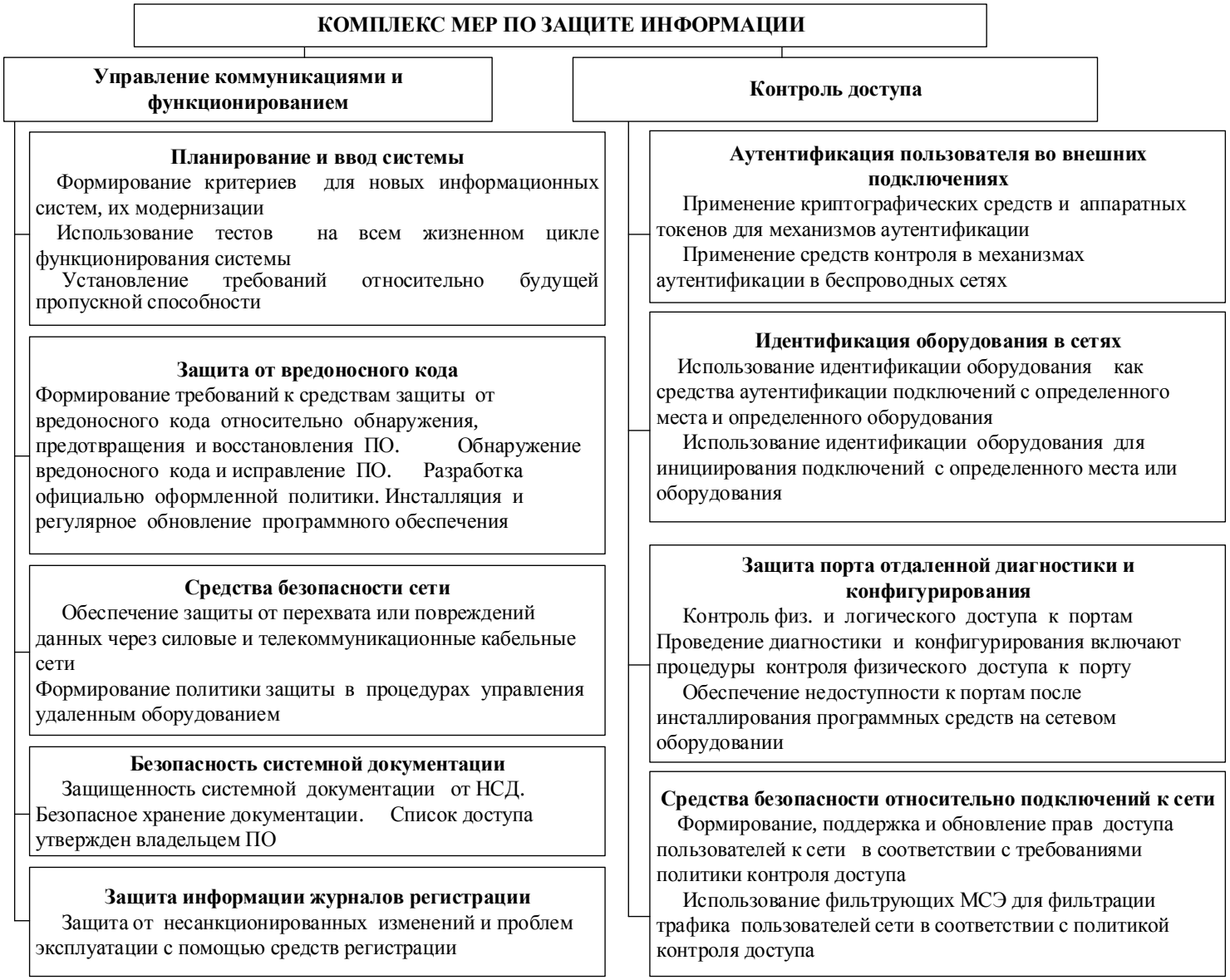


Рис. 8. Комплекс мер по защите банковских транзакций: а – безопасность человеческих ресурсов, физическая безопасность инфраструктуры; б – администрирование и контроль доступа

НСМЭП использует информационные технологии, обеспечивающие формирование, обработку, передачу и хранение документов по операциям с применением платежных карточек и формирования соответствующих документов на перевод средств в электронной форме, а также систему защиты информации, обеспечивающую непрерывную защиту информации относительно осуществления операций с применением платежных карточек на всех этапах ее формирования, обработки, передачи и хранения [1]. Структурная схема СУИБ НСМЭП представлена на рис. 9.

7. Анализ основных механизмов безопасности информации в НСМЭП

Система защиты электронных банковских документов в вычислительной сети НБУ состоит из комплекса аппаратно-программных средств криптографической защиты и ключевой системы к ним, технологических и организационных мероприятий по защите информации в сети. Согласно Концепции системы электронного денежного обращения в Украине, утвержденной Правлением НБУ 02.10.92, разработаны и изготовлены аппаратно-программные средства криптографической защиты электронных банковских документов в вычислительной сети НБУ, в составе [1]:

– аппаратуры защиты банковских данных (АЗБД);

– аппаратуры защиты электронного денежного обращения (АЗЭДО)

– ключевая система, с генерацией ключей в НБУ и защищенными электронными носителями ключей (шифров);

– электронные карточки (ЭК).

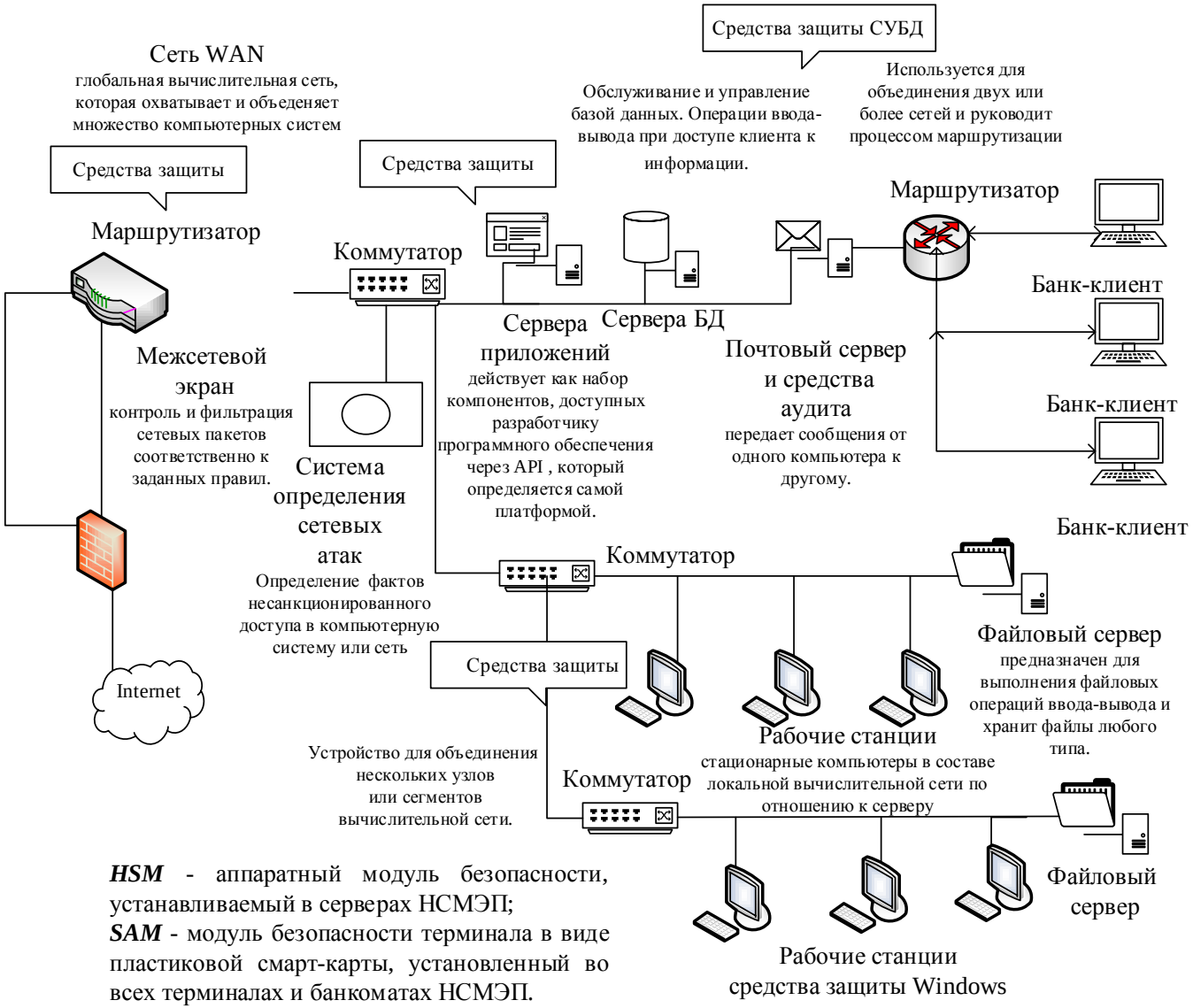


Рис. 9. Структурная схема СУИБ НСМЭП

Аппаратура защиты соответствует стандарту ГОСТ 28147-89 на алгоритмы шифрования и имеет сертификат Государственной службы Украины по вопросам технической защиты информации, удовлетворяет все требования вычислительной сети “Банк”.

Качество решения указанных выше проблем в значительной мере определяется рациональным выбором криптографических средств, при реализации механизмов защиты.

В соответствии с международными стандартами ISO 7498, ISO/IEC 10181 для обеспечения необходимых показателей безопасности определены пять базовых общепринятых услуг, основными из которых являются только две: аутентичность и целостность, для их обеспечения используются механизмы безопасности, большинство из которых реализуется на основе криптографических методов преобразования информации. Основные механизмы обеспечения целостности и подлинности информации в банковских системах на различных уровнях основаны на использовании стандартов блочно-симметричных шифров (3DES, ГОСТ 28147-89).

На рис. 10 приведена взаимосвязь между механизмами и применяемыми стандартами в СУИБ НСМЭП.

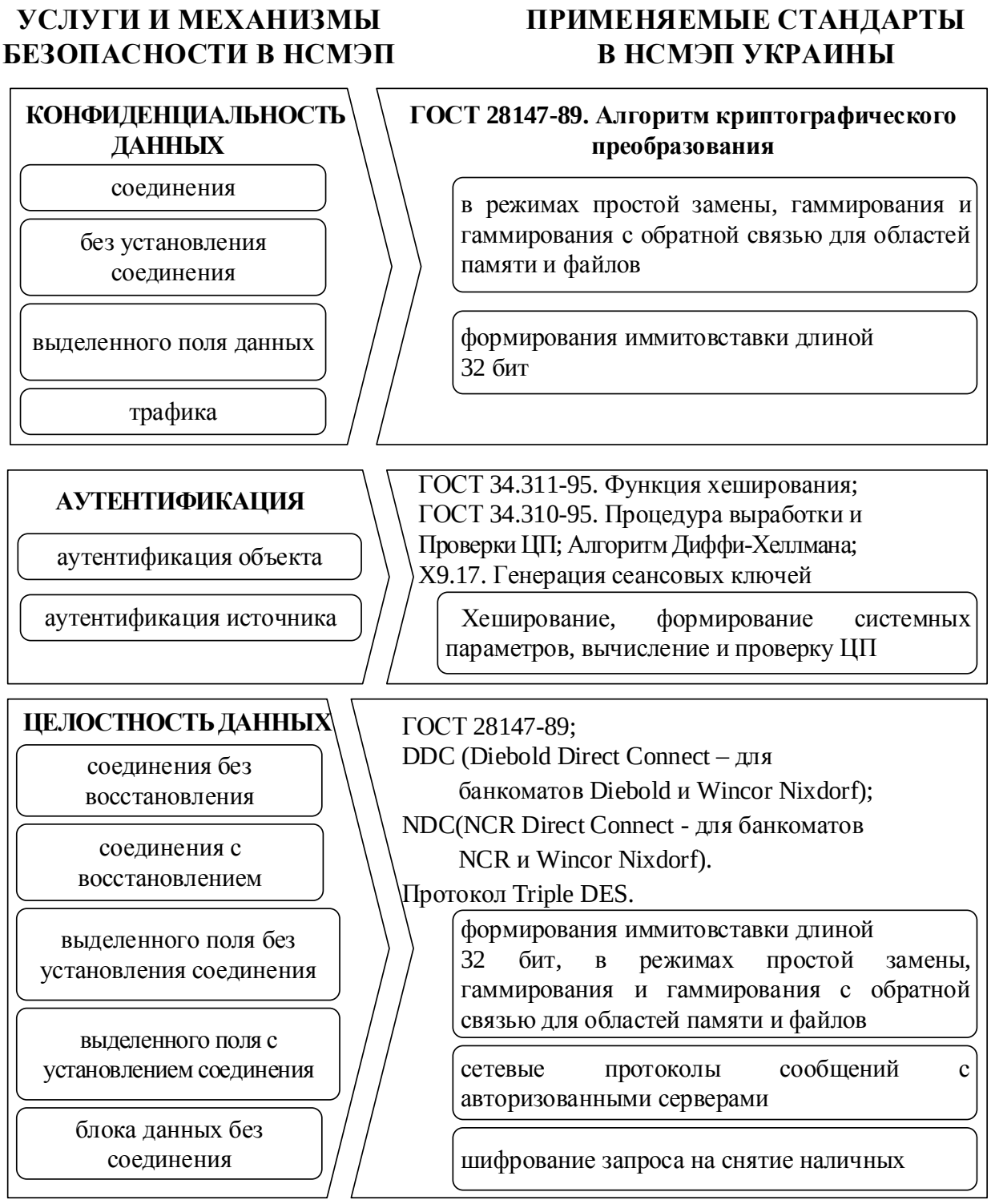


Рис. 10. Взаимосвязь между механизмами и применяемыми стандартами в СУИБ НСМЭП

Примерами 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 и применяется для обмена информацией внутри корпоративной сети банка, с клиентами, работающими с системой “Клиент-Банк”, в системах обслуживания

пластиковых карт [13, 14, 16, 17]. Программное средство криптографической защиты информации “Грифон-Л” [17] предназначено для использования в сфере банковской деятельности, в частности, для обмена конфиденциальной (в т.ч. финансовой) информации внутри корпоративной сети банка, с клиентами, которые работают по системе “Клиент- Банк”, в системах обслуживания пластиковых карт и др.

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 [15].

Процедуры, входящие в состав библиотеки реализуют:

– шифрование/расшифрование данных по алгоритму ГОСТ 28147-89;

– выработку/проверку имитовставки по алгоритму ГОСТ 28147-89;

– выработку/проверку ЭЦП по алгоритмам 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 ПК на базе Intel Celeron 2,4 ГГц):

– скорость шифрование/расшифрование данных в режиме простой замены БСШ ГОСТ 28147-89 не менее 8 Мбайт/с;

– скорость вычисления хэш-функции данных в соответствии с ГОСТ 34.311-95 не менее 3 Мбайт/с;

– выработке ЭЦП в соответствии с ГОСТ 34.310-95 при длине ключа 512 бит не более0,003 с;

– время проверки ЭЦП в соответствии с ГОСТ 34.310-95 при длине ключа 512 бит не более 0,006 с;

– выработке ЭЦП в соответствии с ГОСТ 34.310-95 при длине ключа 1024 бит не более 0,01 с;

– время проверки ЭЦП в соответствии с ГОСТ 34.310-95 при длине ключа 1024 бит не более 0,02 с;

– выработке ЭЦП (с вычислением предподписи) согласно ДСТУ 4145-2002 для основного поля степени 163 не более 0,0068 с;

При проверке 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, шифрование/расшифрование, выработка имитовставок), между клиентами электронной почты (ЭП), зарегистрированными на узлах ЭП через сеть передачи данных произвольного типа и отвечает критериям НД ТЗИ 2.5-004-99 [18].

В 2014 году в Украине приняты национальные стандарты, введенные в действие в 2015 году [20, 21]:

– ДСТУ-7624-2014 “Информационные технологии. Криптографическая защита информации. Алгоритм симметричного блочного преобразования” – устанавливает криптографический алгоритм симметричного блочного преобразования для обеспечения конфиденциальности и целостности (как дополнительной услуги) информации во время ее обработки. Стандарт предлагается использовать при разработке средств криптографической защиты информации в информационных, телекоммуникационных и информационно-телекоммуникационных системах, а также при модернизации действующих систем для замены ГОСТ 28147: 2009, что позволит существенно изменить уровень информационной безопасности в СУИБ;

– ДСТУ 7564-2014 “Информационные технологии. Криптографическая защита информации. Функция хеширования” – устанавливает алгоритм вычисления хеш-значения для последовательностей двоичных символов. Стандарт предлагается использовать при разработке средств криптографической защиты информации в информационно-телекоммуникационных системах, а также при модернизации действующих систем для замены функции хеширования в соответствии со стандартом ГОСТ 34.311. Однако для их использования в банковских системах необходимо дополнительное разрешение НБУ.

8. Выводы

Проведенные исследования показали, что развитие вычислительных ресурсов позволили расширить спектр банковских услуг на основе использования Интернет-ресурсов. Одной из существенных проблем при проектировании и эксплуатации систем защиты банковской информации является игнорирование методологии системного анализа в отношении средств и инструментов для их защиты

Задача защиты банковской информации, как правило, включает решение частных задач по обеспечению надежной и безопасной работы АБС (автоматизированной банковской системы), безопасного доступа сотрудников и клиентов к банковской системе в территориально распределенной сети, доступа сотрудников к внешним информационным сетям (Интернет-ресурсам), защиту банкоматов и терминалов, возможности контроля всех процессов в системе и своевременного обнаружения любых нарушений.

Прогресс в технике преступлений идет не менее быстрыми темпами, чем развитие банковских технологий. В настоящее время свыше 90% всех преступлений связано с использованием АБС на основе синтеза “классических атак” грубой силы и методов социальной инженерии.

Анализ законодательной базы банковской деятельности показал, что она в

целом основывается на мировые стандарты, определяющие основные принципы построения системы управления информационной безопасностью, рекомендации противодействию кибератак на банковские системы. Неполнота нормативно-методического обеспечения информационной безопасности, прежде всего в области показателей и критериев существенно усложняет, а иногда не позволяет объективно оценить эффективность системы защиты информации. Сегодня в Украине помимо крупнейших игроков банковского сектора существует множество небольших банков, которые в силу финансовых ограничений не могут позволить себе вкладывать значительные суммы в информационную безопасность. Тем не менее, обеспечить безопасность автоматизированных банковских систем и информационных систем банков, является необходимостью для банков любого масштаба.

Для обеспечения безопасности банковской информации в НСМЭП используются криптографические симметричные и несимметричные алгоритмы шифрования, разработанные в конце прошлого столетия и не удовлетворяющие, в первую очередь, по оперативности обработки данных (особенно критично в пиковые нагрузки на АБС). Отсутствие Доктрины информационной безопасности; несовершенство законодательной базы не позволяет использовать национальные стандарты в автоматизированных банковских системах.

Литература !!+DOI

1. Химка, С. С. Разработка моделей и методов для создания системы информационной безопасности корпоративной сети предприятия с учетом различных критериев [Электронный ресурс] / С. С. Химка. – Режим доступа: http://masters.donntu.org/2009/fvti/khimka/diss/index.htm

2. Украинский ресурс по безопасности [Электронный ресурс]. – Режим доступа: http://kiev-security.org.ua

3. Слободенюк, Д. Банковские технологии, Средства защиты информации в банковских системах [Электронный ресурс] / Д. Слободенюк. – 2013. – Режим доступа: http://www.arinteg.ru/about/publications/press/sredstva-zashchity-informatsii-v-bankovskikh-sistemakh-131107.html

4. Симаков, М. Н. V Съезд директоров по информационной безопасности [Электронный ресурс] / М. Н. Симаков. – Москва, 2012. – Режим доступа: http://www.cso-summit.ru/data/2012/presentations/cso2012_013_express-tula_simakov.pdf

5. Ревенков, П. В. Защита информации в банке: основные угрозы и борьба с ними [Электронный ресурс] / П. В. Ревенков. – Режим доступа: http://www.crmdaily.ru/novosti-rynka-crm/568-zashhita-informacii-v-banke-osnovnye-ugrozy-i-borba-s-nimi.html

6. Security of Internet Banking - A Comparative Study of Security Risks and Legal Protection in Internet Banking in Thailand and Germany [Electronic resource]. – Available at: http://www.thailawforum.com/articles/internet-banking-thailand.html

7. Ярочкин, В. И. Информационная безопасность [Текст]: учебник / В. И. Ярочкин; 2-е изд. – М.: Академический Проект; Гаудеамус, 2004. – 544 с.

8. 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) [Текст]. – К.: НБУ., 2010. – 67 с.

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

10. Корченко, А. А. Банківська безпека [Текст] / А. А. Корченко, Л. Н. Скачек, В. А. Хорошко. – Київ, 2014. – 185 с.

11. ГОСТ 34.310-95. Информационная технология. Криптографическая защита информации. Процедура выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма [Текст]. – К.: Госстандарт Украины, 1998.

12. ГОСТ 34.311-95. Информационная технология. Криптографическая защита информации. Функция хеширования [Текст]. – К.: Госстандарт Украины, 1998.

13. ГОСТ Р34.10-94. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма [Текст]. – Национальный стандарт.

14. ГОСТ Р34.11-94. Информационная технология. Криптографическая защита информации. Функция хеширования [Текст]. – Национальный стандарт.

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

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

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

18. Євсеев, С. П. Механизмы обеспечения аутентичности банковских данных во внутриплатежных системах комерческого банка [Текст]: зб. наук. ст. / С. П. Євсеєв, В. Е. Чевардин, С. А. Радковский // Х.: ХНЕУ. – 2008. – Вип. 6. – С. 40–44.

19. ДСТУ 4145–2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка [Текст]. – К.: Держстандарт України, 2002. – 40 с.

20. ДСТУ 7564–2014. Інформаційні технології. Криптографічний захист інформації. Функція ґешування [Текст]. – К. : Держстандарт України, 2014. – 39 с.

21. ДСТУ 7624–2014. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення [Текст]. – К.: Держстандарт України, 2014. – 235 с.

22. Міжбанківські розрахунки в Україні [Електронний ресурс]. – Режим доступу: http://www.bank.gov.ua/control/uk/publish/

References !!+DOI

1. Khymka, S. S. Razrabotka modelej y metodov dlia sozdanyia systemy ynformatsyonnoj bezopasnosty korporatyvnoj sety predpryiatyia s uchetom razlychnykh kryteryev [Development of models and methods for the creation of a system of information security corporate network , taking into account various criteria]. Available at: http://masters.donntu.org/2009/fvti/khimka/diss/index.htm [in Russian]

2. Ukraynskyj resurs po bezopasnosty [Ukrainian security resource] [Elektronnyj resurs]. Available at: http://kiev-security.org.ua [in Russian]

3. Slobodeniuk, D. (2013). Bankovskye tekhnolohyy, Sredstva zaschyty ynformatsyy v bankovskykh systemakh [Banking Technologies: means of information security in banking systems]. Available at: http://www.arinteg.ru/about/publications/press/sredstva-zashchity informatsii-v-bankovskikh-sistemakh-131107.html [in Russian]

4. Symakov M. N. (2012). V S'ezd dyrektorov po ynformatsyonnoj bezopasnosty [V Congress Chief Security]. Moscow. Available at: http://www.csosummit.ru/data/2012/presentations/cso2012_013_express-tula_simakov.pdf [in Russian]

5. Revenkov, P. V. Zaschyta ynformatsyy v banke: osnovnye uhrozy y bor'ba s nymy [Data protection in the bank : the main threats and control of them]. Available at: http://www.crmdaily.ru/novosti-rynka-crm/568-zashhita-informacii-v-banke-osnovnye-ugrozy-i-borba-s-nimi.html [in Russian]

6. Security of Internet Banking – A Comparative Study of Security Risks and Legal Protection in Internet Banking in Thailand and Germany. Available at: http://www.thailawforum.com/articles/internet-banking-thailand.html [in English].

7. Yarochkyn, V. Y. (2004). Ynformatsyonnaia bezopasnost' [Information security]. Second edition. Moscow: Akademycheskyj Proekt; Haudeamus, 544. [in Russian]

8. Standart Ukrainy SOU N NBU 65.1 SUIB 1.0:2010. Metody zakhystu v bankivs'kij diial'nosti systema upravlinnia informatsijnoiu bezpekoiu. [Vymohy Methods of protection in the banking system of information security management. Requirements]: (ISO/IEC 27001:2005, MOD) (2010). Kyiv: NBU., 67. [in Ukrainian]

9. Zvid pravyl dlia upravlinnia informatsijnoiu bezpekoiu (ISO/IEC 27002:2005, MOD) [Set of rules for information security management]: SOU N NBU 65.1 SUIB 1.0:2010 (2010). Kyiv: NBU, 209. [in Ukrainian]

10. Korchenko, A. A., Skachek, L. N., Khoroshko, V. A. (2014). Bankivs'ka bezpeka [Banking security]. Kyiv, 185. [in Ukrainian]

11. Ynformatsyonnaia tekhnolohyia. Kryptohrafycheskaia zaschyta ynformatsyy. Protsedura vyrabotky y proverky elektronnoj tsyfrovoj podpysy na baze asymmetrychnoho kryptohrafycheskoho alhorytma [Interstate standard. Information technology. Cryptographic protection of information. The procedure of development and verification of digital signatures based on asymmetric cryptographic algorithm]: HOST 34.310-95 (1998). Kyiv: Hosstandart Ukrayny. [in Russian]

12. GOST 34.311-95. Ynformatsyonnaia tekhnolohyia. Kryptohrafycheskaia

zaschyta ynformatsyy. Funktsyia kheshyrovanyia [Interstate standard. Information technology. Cryptographic protection of information. Hashing function] (1998). Kyiv: Hosstandart Ukrayny. [in Russian]

13. GOST R34.10-94. Ynformatsyonnaia tekhnolohyia. Kryptohrafycheskaia zaschyta ynformatsyy. Protsedury vyrabotky y proverky elektronnoj tsyfrovoj podpysy na baze asymmetrychnoho kryptohrafycheskoho alhorytma [Information technology. Cryptographic protection of information. Procedure of generation and verification of electronic digital signatures based on asymmetric cryptographic algorithm]. Natcionalnyj standart. [in Russian]

14. GOST R34.11-94. Ynformatsyonnaia tekhnolohyia. Kryptohrafycheskaia zaschyta ynformatsyy. Funktsyia kheshyrovanyia [Information technology. Cryptographic protection of information. Hashing function]. Natcionalnyj standart. [in Russian].

15. Zadiraka, V. K., Olesiuk, O. S., Nedashkovs'kyj, N. O. (1999). Metody zakhystu bankivs'koi informatsii [Methods of bank information protection]. Kyiv: Vyscha shkola, 264. [in Ukrainian]

16. Prohrammnoe sredstvo kryptohrafycheskoj zaschyty ynformatsyy "Hryfon-B" [Software for cryptographic information protection "Griffin-B"]. Available at: http://www.banksoft.com.ua/index.php?id=28 [in Russian]

17. Prohrammnoe sredstvo «Byblyoteka funktsyj kryptohrafycheskoj zaschyty ynformatsyy "Hryfon-L"[The software "Library of cryptographic information protection functions " Griffin-L"]. Available at: http://www.banksoft.com.ua/index.php?id=27 [in Russian]

18. Yevseiev, S. P., Chevardyn, V. E., Radkovskyj, S. A. (2008). Mekhanyzmy obespechenyia autentychnosty bankovskykh dannykh vo vnutryplatezhnykh systemakh komercheskoho banka [Mechanisms for provodong bank data authenticity to the payment systems within the commercial bank]. Kharkiv: KhNEU, 6, 40–44. [in Russian]

19. DSTU 4145–2002. Informatsijni tekhnolohii. Kryptohrafichnyj zakhyst informatsii. Tsyfrovyj pidpys, scho gruntuiet'sia na eliptychnykh kryvykh. Formuvannia ta perevirka [Information Technology. Cryptographic protection of information. Digital signature based on elliptic curves. Generation and verification] (2002). Kyiv: Derzhstandart Ukrainy, 40. [in Ukrainian]

20. DSTU 7564–2014. Informatsijni tekhnolohii. Kryptohrafichnyj zakhyst informatsii. Funktsiia geshuvannia [Information Technology. Cryptographic protection of information. Hashing function] (2014). Kyiv: Derzhstandart Ukrainy, 39. [in Ukrainian]

21. DSTU 7624–2014. Informatsijni tekhnolohii. Kryptohrafichnyj zakhyst informatsii. Alhorytm symetrychnoho blokovoho peretvorennia [Cryptographic protection of information. The algorithm of symmetric block conversion] (2014). Kyiv: Derzhstandart Ukrainy, 235. [in Ukrainian]

22. Mizhbankivs'ki rozrakhunky v Ukraini [Interbank settlements in Ukraine]. Available at: http://www.bank.gov.ua/control/uk/publish/