© Yevseiev S. Methodology for information technologies security evaluation for automated banking systems of Ukraine // Ukrainian Scientific Journal of Information Security, 2016, vol. 22, issue 3, p. 297-309.

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ / INFORMATION SECURITY MANAGEMENT

DOI: 10.18372/2225-5036.22.11103

МЕТОДОЛОГИЯ ОЦЕНИВАНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ АВТОМАТИЗИРОВАННЫХ БАНКОВСКИХ СИСТЕМ УКРАИНЫ

Сергей Евсеев

Харьковский национальный экономический университет им. С. Кузнеца, Украина

ЕВСЕЕВ Сергей Петрович, к.т.н.

Дата и место рождения: 1969, Харцызск, Донецкая обл., Украина.
Образование: Харьковский военный университет, 2002 р.
Должность: доцент кафедры информационных систем с 2007.
Научные интересы: информационная безопасность и кибербезопасность в банковских системах.
Публикации: более 180 научных публикаций включая монографии, книги, статьи и патенты.
E-mail: serhii.yevseiev@hneu.net

Аннотация. *Современные автоматизированные банковские системы (АБС) ежедневно подвергаются атакам как в киберпространстве, так и на различных уровнях технических систем защиты информации. Особенно остро стоят вопросы обеспечения безопасности не только критических транзакций и банковских операций, но и защиты всего комплекса банковской информации (БИн). Поэтому изобретение преступниками новых изощренных атак и техник их реализации на автоматизированные банковские системы обуславливает необходимость дальнейшего совершенствования правовой и методологический базы, посвященной вопросам оценивания безопасности информационных технологий (ИТ) АБС. Опираясь на научно-технический анализ лучших мировых и национальных стандартов, а также руководящих документов в области управления информационной безопасностью (ИБ), в статье впервые раскрывается совершенно новая методология оценивания безопасности ИТ АБС Украины. Характерной особенностью предложенной методологии является то, что в отличие от известных подходов, базисом оценивания безопасности ИТ АБС Украины является разработанная синергетическая модель угроз безопасности БИн. Предложенная методология позволяет учитывать практически весь спектр наиболее актуальных угроз кибербезопасности, информационной безопасности и безопасности информации ИТ АБС Украины, а на основе полученной синергетической оценки разрабатывать, внедрять и сопровождать безопасные ИТ АБС.*

Ключевые слова: *автоматизированная банковская система, банковская информация, информационная технология, методология, синергетическая модель угроз, информационная безопасность, кибербезопасность, безопасность информации.*

Введение

Развитие ИТ, базирующихся на последних достижениях науки и техники в области вычислительной техники и программирования, и внедрение их в банковскую сферу, значительно расширили спектр услуг и функций, предоставляемых современными АБС [1]. Поэтому повышение эффективности обеспечения безопасности БИн кроме всего прочего требует дальнейшего усовершенствования методологический базы, посвященной вопросам оценивания безопасности ИТ АБС адекватно к темпам их внедрения в банковскую сферу, и, как следствие, возникающего при этом расширенного спектра новых угроз. Особое значение в последнее десятилетие играет дальнейшее разделение функций и принципов обеспечения услуг в терминологии безопасности информации и информационной безопасности [1]. Под информационной безопасностью банковской информации (ИБ БИн) предлагается понимать состояние защищенности информационной среды банковского сектора, обеспечивающее ее

формирование, использование и развитие в интересах граждан и организаций банковского сектора, под безопасностью банковской информации (Б БИн) – состояние защищенности банковской информации, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность аутентичность и доступность БИн при ее обработке в автоматизированной банковской системе (АБС). Таким образом, дальнейшее развитие высоких технологий, вычислительной техники выдвигают новые требования к разграничению функций программно-аппаратных средств (программного обеспечения) обеспечения основных услуг ИБ и Б БИн.

Анализ существующих исследований

В современных условиях массовой доступности компьютерных систем и телекоммуникаций, увеличения оборотов электронного документооборота между банками и клиентами, перехода на электронную коммерцию проблемы безопасности БИн в силу природных и искусственных факторов только обостряются. Как следствие, ущерб от нарушения безопасности БИн становится все более дорогостоящим как для банков, так и для их клиентов [2]. Например, наибольшее количество угроз безопасности ИТ АБС Украины, как и в других государствах, исходит из сети Интернет при передаче БИн различными каналами связи [3]. Несовершенство стратегического управления безопасностью ИТ АБС Украины выливается для государственного банковского сектора в ряд проблем, основными из которых являются бессистемность в обеспечении безопасности, несогласованность механизмов обеспечения безопасности ИТ АБС, особенно в международном двух и многостороннем форматах и т.д. [4]. Анализ основных международных стандартов и стандартов Украины [7-24] показал, что рассмотренные отдельные составляющие методологии оценивания безопасности информационных технологий, применяемых в банковском секторе, основываются на модели безопасности – обеспечения целостности, конфиденциальности и доступности (модели ЦКД), при этом не учитывается неотъемлемая составляющая банковских транзакций – услуга аутентичности – состояние банковской информации, при котором информация обеспечивает подтверждение подлинности источника (авторизованного пользователя и/или процесса) информации. Отсутствие синергетического подхода к анализу рисков, единой методологии оценивания безопасности информационных технологий в стандартах банковского сектора не позволяет своевременно выработать соответствующие политики, новые подходы и меры по обеспечению банковской информации, что обусловлено несовершенством механизмов обеспечения ее информационной безопасности, безопасности информации и кибербезопасности в частности, неотъемлемой частью проблемы обеспечения безопасности банковской информации является проблема анализа рисков. Фактически риск представляет собой интегральную оценку того, насколько эффективно существующие средства защиты способны противостоять атакам на банковскую информацию [1, 2, 6, 22, 23, 34, 35].

Не взирая на то, что в настоящий момент разработано множество механизмов и средств защиты информации, теперь одной из самых приоритетных задач остается задача оценивания эффективности процесса обеспечения безопасности ИТ АБС на основе соответствующих метрик. Например, как показал анализ [6-14], среди самых распространенных метрик безопасности являются их следующие таксономии: Vaughn-Hennig-Siraj, NIST STS822, OCIPEP, OCTAVE, CISWG, Erkan Kahraman. Как установлено в результате изучения приведенных в качестве примера метрик безопасности их эффективное внедрение в банковский сектор Украины сдерживает: дефиниционная неопределенность – в силу несовершенства национальной законодательной базы и ее расхождения с лучшими мировыми практиками в этой сфере; низкая объективность получаемых оценок – в силу отсутствия международного опыта большей части банковского персонала, обеспечивающего безопасность ИТ АБС; методологические трудности – в силу проблематичности получения гармонизированных между собой количественных и качественных оценок и др. [5]. При этом последняя из приведенных проблем носит системообразующий ключевой характер, а поэтому требует глубокой научной и методической проработки и дальнейшего исследования.

Целью работы является усовершенствование методологии оценивания безопасности ИТ АБС Украины.

Для достижения поставленной цели были сформулированы и решены следующие частные задачи:

– уточнение требований передовых мировых практик в вопросах методологии оценивания безопасности ИТ АБС и установление на основе их анализа взаимосвязей между основными рисками безопасности и бизнес-процессами в АБС Украины;

– построение современной концепции стратегического управления безопасностью ИТ АБС Украины на основе принципиально новой синергетической модели угроз безопасности;

– разработка усовершенствованной методологии оценивания безопасности ИТ АБС Украины.

Основная часть. Уточнение требований передовых мировых практик в вопросах методологии оценивания безопасности ИТ АБС

Как известно, обоснованию критериев и созданию методологии оценивания информационной безопасности в мире уделено значительное внимание. В настоящее время можно выделить следующие основные документы, которые внесли серьезный теоретический и практический вклад в решение задач обеспечения информационной безопасности [6]: Критерии оценивания защищенности компьютерных систем [7], которые известны как «Оранжевая книга»; Европейские критерии оценивания безопасности ИТ [8]; Канадские критерии оценивания безопасности надежных компьютерных систем [9]; Федеральные критерии США [10]; Междуна-

родный стандарт ISO/IEC 15408 – «Критерии оценивания безопасности ИТ» [11-13]; Рабочий проект стандарта CEM-97/017 – «Общая методология оценивания безопасности ИТ» [24], ДСТУ ISO/IEC TR 13335. Інформаційні технології. Настанови з керування безпекою інформаційних технологій. ч. 1-5 [14-18], Стандарт України ГСТУ СУІБ 2.0/ISO/IEC 27002:2010 Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою (ISO/IEC 27002:2005, MOD) [23]. Анализ этих документов подтверждает тот факт, что для решения задач обеспечения информационной безопасности, наряду с формальными методами моделирования процессов и оценивания эффективности функционирования систем обеспечения безопасности, необходимо широко использовать методы декомпозиции и структуризации компонентов систем и процессов, неформальные методы оценивания эффективности функционирования и принятия решений. Это означает, что аппарат системного анализа необходимо использовать на всех этапах жизненного цикла систем защиты информации [6]. Особое место в разработке методологии оценивания безопасности информационных технологий в АБС занимает стандарт ISO/IEC 15408 «Общие критерии оценивания защищённости ИТ», «Общие критерии». Стандарт определяет общие критерии, которые используются в качестве основы для оценивания свойств безопасности информационных продуктов и технологий [11-13]. Единые критерии направлены на обеспечение сравнимости результатов оценок, полученных различными экспертами, путем введения общего множества требований к функциям безопасности продуктов и систем информационных технологий, а также к показателям этих функций. Используя анализируемый стандарт можно решить конкретную прикладную задачу выбора соответствующих требований и показателей безопасности ИТ [6]. Кроме того, потенциальные угрозы безопасности из Единых критериев, а именно целостности, доступности, конфиденциальности в дальнейшем предлагается положить как составляющие в новую синергетическую модель угроз безопасности.

Как известно, стандарты Национального банка Украины [22, 23], базирующиеся на международных стандартах ISO 27001 [19] и ISO 27002 [20] с добавлением к ним требований по защите информации [23], обусловлены конкретными потребностями сферы банковской деятельности и правовыми требованиями национального законодательства [26]. Ключевым моментом рассматриваемых документов является то, что они предписывают принципы управления информационной безопасностью банка, наиболее важным из которых является оценивание рисков [14 – 18, 22, 23, 26].

Практика показывает, что сегодня можно четко выделить две основные группы методов оценивания рисков безопасности [19, 20, 23, 28, 29]. Первая группа методов позволяет установить уровень риска путём оценивания степени соответствия определённому набору требований по обеспечению информационной безопасности. В качестве источников таких требований в банковском секторе Украины могут выступать как международные, так и национальные руководящие документы, систематизация которых в виде схемы подана на рис. 1.

Вторая группа методов оценивания рисков информационной безопасности базируется на определении вероятности реализации атак, а также уровней их ущерба. В данном случае значение риска вычисляется отдельно для каждой угрозы и, в общем случае, представляется как произведение вероятности реализации угрозы на величину потенциального ущерба от этой угрозы. Значение ущерба определяется собственником БИн, а вероятность реализации угрозы вычисляется группой экспертов, проводящих процедуру аудита.

Отличительной чертой методов первой и второй групп является применение различных шкал для определения величины риска. В первом случае риск и все его параметры выражаются в числовых, то есть количественных значениях. Во втором случае используются качественные шкалы.

В соответствии с требованиями стандартов Национального банка Украины согласно с предлагаемой концепцией стратегического управления безопасностью ИТ АБС Украины (рис. 1) сферой применения системы управления информационной безопасностью (СУИБ), которая должна быть внедрена, является банк в целом. Поэтому, очень важно в условиях увеличения количества угроз безопасности ИТ АБС уточнить бизнес-процессы/банковские продукты [26], которые работают с БИн, подлежащей защите. В нынешних условиях к такому перечню можно отнести [26]: платежные документы; внутренние платежные документы; кредитные документы; документы на денежные переводы; персональные данные клиентов и работников банка; статистические отчеты; другие документы, которые содержат информацию с ограниченным доступом. Кроме того, решение всего комплекса вопросов, связанных с обеспечением безопасности БИн и ИТ АБС Украины, а именно – кибербезопасности, информационной безопасности и безопасности информации в ИТ АБС должно решаться в комплексе и неразрывно один от другого, гармонично дополняя и восполняя, в случае необходимости, друг друга. Простое комплексирование сил и средств в каждом отдельном случае для обеспечения безопасности ИТ АБС является нецелесообразным как с практической, так и научной точек зрения. Отсутствие других альтернативных подходов обуславливает насущную необходимость в решении сложившейся проблемы – повышения защищенности ИТ АБС на основе разработки новых подходов.

Учитывая взаимосвязь угроз кибербезопасности, информационной безопасности и безопасности информации в ИТ АБС, в дальнейшем предлагается провести синтезирование описанных выше бизнес-продуктов с типовыми угрозами согласно синергетической модели угроз БИн [1] (рис. 2).

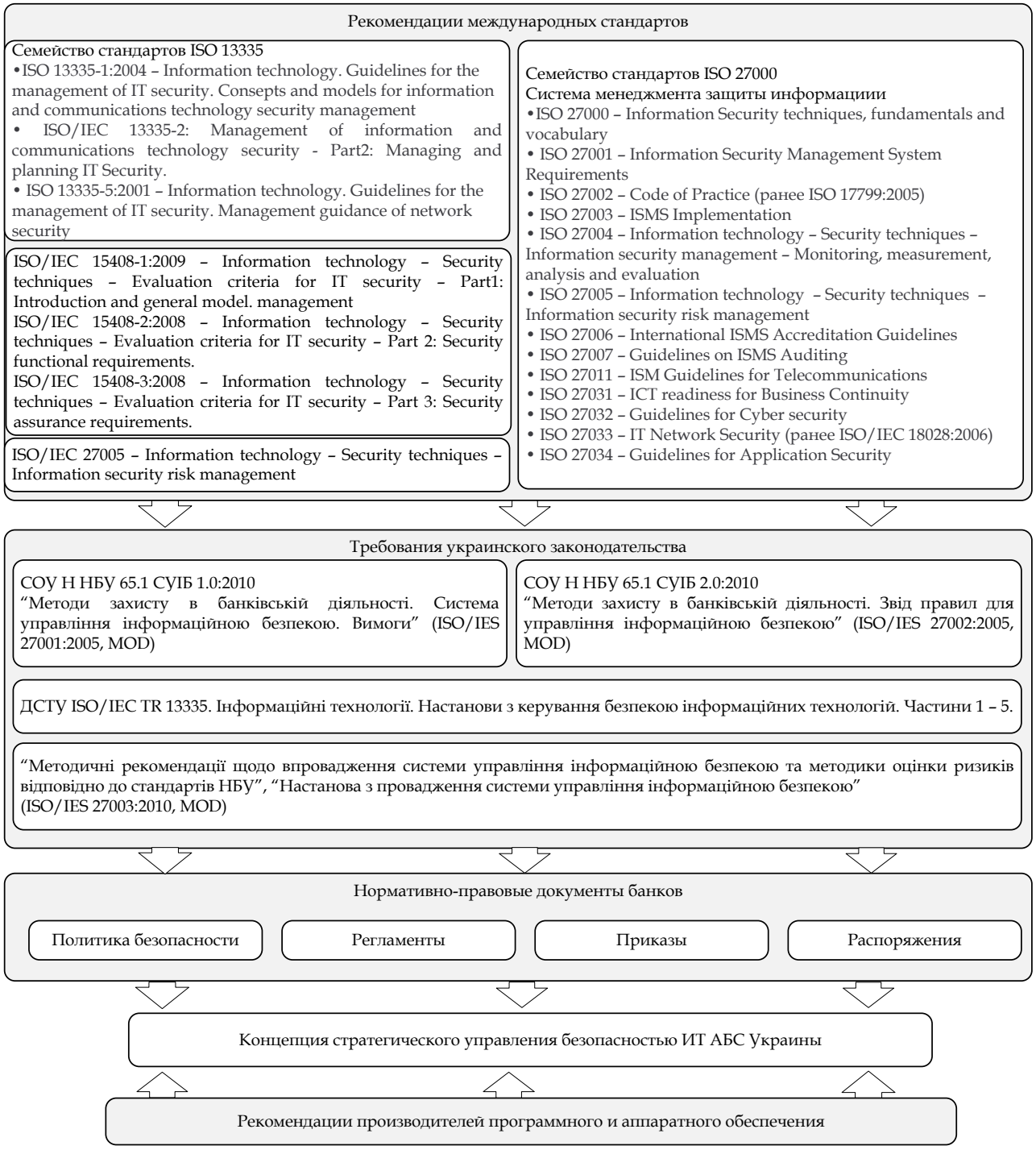

Рис. 1. Систематизация источников требований к безопасности ИТ АБС Украины

Отличительной чертой предлагаемого подхода (см. рис. 2) является то, что он закладывает необходимые и достаточные условия для разработки нового методологического базиса, направленного на достижение синергетического эффекта в сфере обеспечения безопасности ИТ АБС не только Украины, но и других развитых государств.

Таким образом, в результате уточнения требований передовых мировых практик в вопросах методологии оценивания безопасности ИТ АБС, впервые установлено взаимосвязи между основными рисками безопасности и бизнес-процессами, которые сегодня и в ближайшем будущем будут иметь место в АБС Украины.

Построение современной концепции стратегического управления безопасностью ИТ АБС Украины на основе принципиально новой синергетической модели угроз безопасности

Деятельность по обеспечению безопасности ИТ АБС во всех ее проявлениях не может сводиться только к удовлетворению краткосрочных потребностей по защите БИн. Поэтому, во избежание системных ошибок и противоречий при принятии решений на различных уровнях иерархии управления банком счита-

ется целесообразным доработать концепцию стратегического управления безопасностью ИТ АБС Украины. Опираясь на функционал трехуровневой модели стратегического набора типового предприятия [4] в контексте обеспечения безопасности ИТ АБС, предлагается современная концепция стратегического управления (рис. 3), базис которой составляет синергетическая модель угроз безопасности [1].

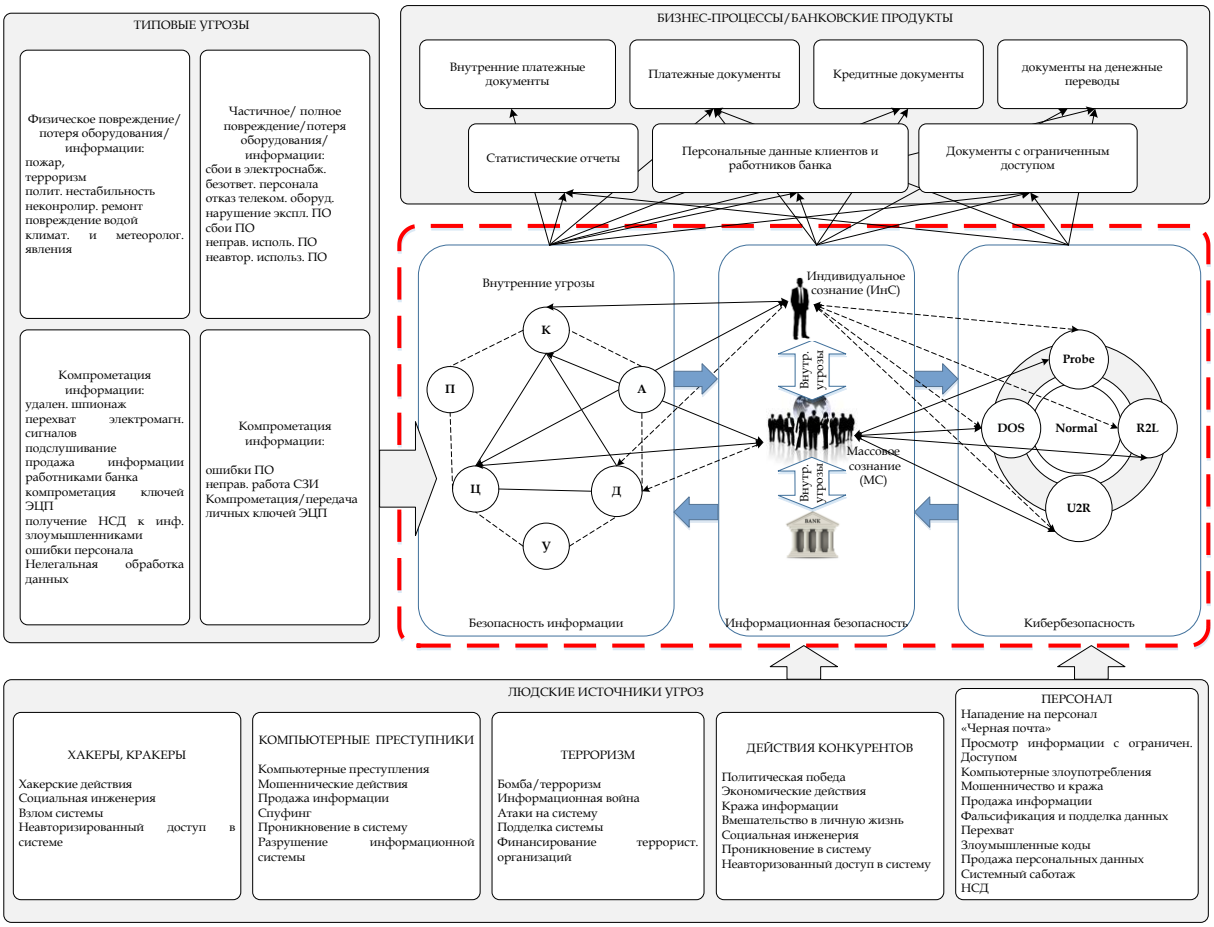

Рис. 2. Взаимосвязь бизнес-продуктов с типовыми источниками угроз согласно синергетической модели

Концептуально стратегический набор состоит из трех уровней (рис. 3 а, б, в). Первый уровень (рис. 3а) описывает общую корпоративную стратегию банка и его функциональные стратегии. Корпоративная стратегия описывает перспективы развития и способствует выполнению основной мисси банка. На данном уровне в соответствии с синергетическим подходом рассматривается общая концепция обеспечения безопасности ИТ АБС и формируются цели и задачи обеспечения кибербезопасности. Функциональные стратегии одного уровня обладают горизонтальными связями и согласуются на уровне целей, с последующей детализацией на следующем уровне стратегического набора.

На втором уровне (рис. 3б) формируется корпоративная стратегия информационной безопасности в АБС, определяются цели и задачи основных бизнес-процессов, связанных с защитой персональных данных юридических и физических клиентов банка. Корпоративная стратегия безопасности описывает каким образом следует управлять и координировать усилия по различным аспектам безопасности. Она развивается функциональными стратегиями: финансовой экономической, физической и информационной безопасностями.

На третьем уровне (рис. 3в) проводится детализация функциональных стратегий второго уровня стратегического набора, формируется корпоративная стратегия безопасности информации. Среди основных направлений по защите целесообразно выделить кадровую безопасность, физическую безопасность, сетевую и безопасность информации. Стратегия ИБ является важной функцией руководства банка в сфере безопасности и должна формироваться и проводится высшим руководством банка.

Концепция стратегического управления безопасностью ИТ АБС Украины на основе трехуровневой модели и синергетической модели угроз в отличие от известных охватывает все основные направления развития деятельности банка по обеспечению безопасности. Предложенная концепция подразумевает синергетический подход к выбору наиболее эффективных направлений достижения поставленных целей безопасности с учетом величины риска на каждом уровне модели стратегического управления банком. Подобный выбор позволяет комплексно производить отбор

альтернативных вариантов возможных стратегических решений по вопросам безопасности.

Для полного раскрытия потенциала концепции стратегического управления необходим механизм способный качественно или количественно оценить эффективность достижения установленных стратегических целей. Так сформулированные в работе [27] основные требования к методике оценивания рисков согласно предложенной концепции позволяет сформулировать новые дополнительные требования. А именно, возникает потребность в: сопоставлении качественных и количественных показателей оценивания эффективности ИТ АБС; нахождении эмерджентных свойств создаваемой системы оценки безопасности информационных технологий автоматизированной банковской системы (СОБ ИТ АБС) на основе трехуровневой и синергетической моделей угроз; обязательном введении нового обобщенного синергетического показателя безопасности ИТ АБС.

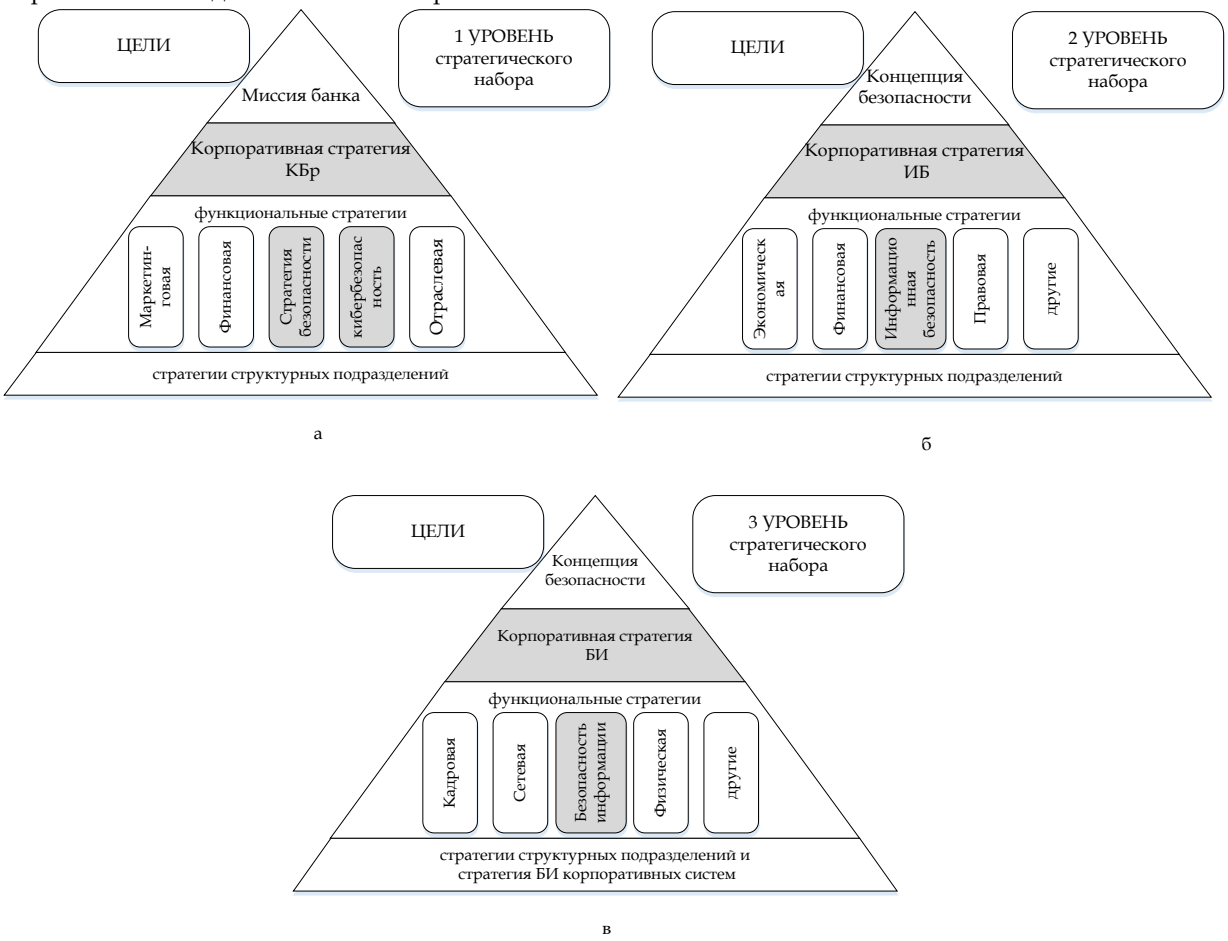

Рис. 3. Современная концепция стратегического управления безопасностью ИТ АБС Украины на основе трехуровневой модели и синергетической модели угроз

Анализ общей модели оценки объекта оценки (ОО) безопасности на основе контекста оценки

В стандарте [28] рассмотрен общий подход к процессу оценки объекта оценки безопасности, использующий системный подход к идентификации и анализу степени рисков.

Для оценки ОО безопасности в стандарте ISO/IEC 27005 определены основные принципы общей методологии оценки (ОМО) [28]:

– объективность – результаты оценки основываются на фактических свидетельствах и не зависят от личного мнения оценщика;

– беспристрастность – результаты оценки являются непредубежденными, когда требуется субъективное суждение;

– воспроизводимость – действия оценщика, выполняемые с использованием одной и той же совокупности данных для оценки, всегда приводят к одним и тем же результатам;

– корректность – действия оценщика обеспечивают точную техническую оценку;

– достаточность – каждый вид деятельности по оценке осуществляется до уровня, необходимого для удостоверения всех заданных требований и доверия;

– приемлемость – каждое действие оценщика способствует повышению доверия, по меньшей мере, пропорционально затраченным усилиям.

Использование общей методологии оценки позволяет достичь повторяемости и объективности результатов, но только этого недостаточно. Многие из критериев оценки требуют привлечения экспертных решений, добиться согласованности которых бывает нелегко. Для повышения согласованности выводов, полученных при оценке, ее конечные результаты могут быть представлены на сертифика-

цию. На рис. 4 представлена контекстная диаграмма общей модели оценки ОО в стандарте IDEF0.

Система оценки, методология и процедуры сертификации находятся в ведении органов оценки, управляющих системами оценки, и не входят в область действия критериев оценки (ОК). Среда безопасности включает все законы, политики безопасности организаций, опыт, специальные навыки и знания, для которых решено, что они имеют отношение к безопасности. Таким образом, она определяет контекст предполагаемого применения ОО. Среда безопасности включает также угрозы безопасности, присутствие которых в этой среде установлено или предполагается [29].

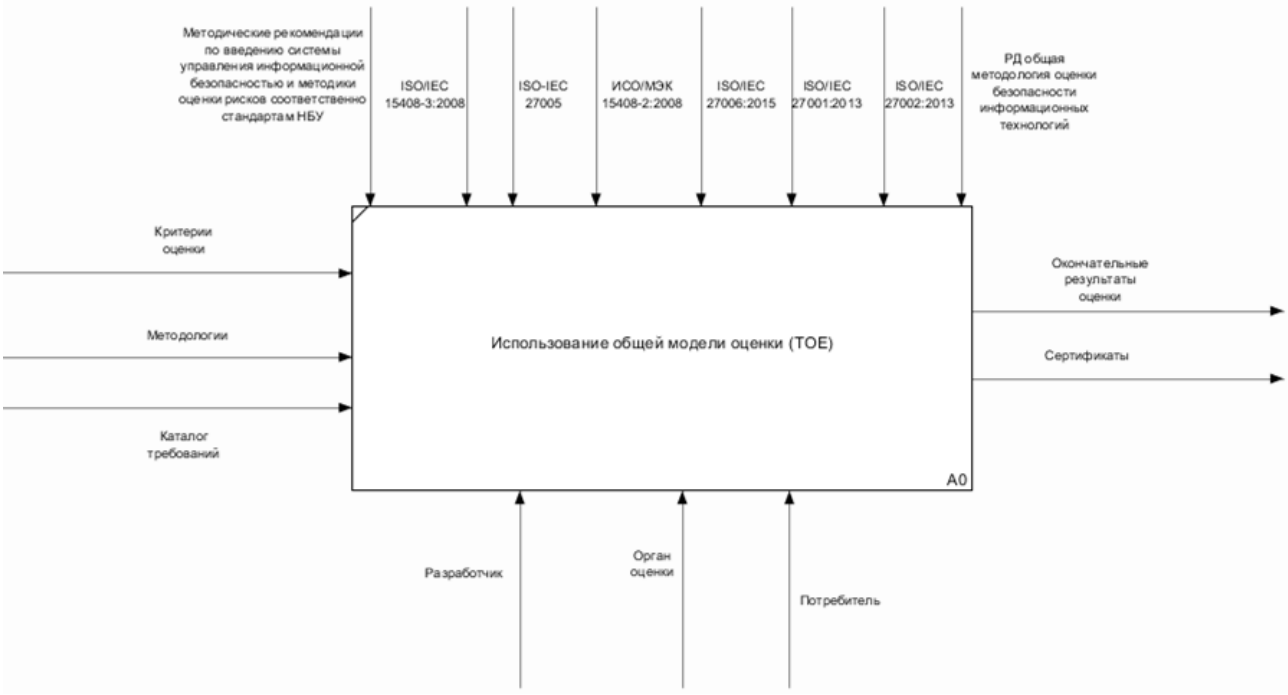

Рис. 4. Контекстная диаграмма использования общей модели оценки ОО

Безопасность связана с защитой активов от угроз, где угрозы классифицированы на основе потенциала злоупотребления защищаемыми активами. Во внимание следует принимать все разновидности угроз, но в сфере безопасности наибольшее внимание уделяется тем из них, которые связаны с действиями человека, злонамеренными или иными [29]. Системы ИТ приобретаются и создаются для выполнения определенных требований, и при этом, по экономическим причинам, могут максимально использоваться имеющиеся коммерческие продукты ИТ, такие как операционные системы, компоненты прикладного программного обеспечения общего назначения и аппаратные платформы. Анализ стойкости функций безопасности в ОК и ОМО основывается на применении количественных показателей, реализованных вероятностными и/или перестановочными механизмами [30] и не позволяет получить экономическую составляющую затрат на использование механизмов защиты или контрмеры безопасности ИТ, реализованные в системе, могут использовать функции, имеющиеся во включаемых продуктах ИТ, и, следовательно, зависят от правильного выполнения функций безопасности продуктов ИТ. Поэтому продукты ИТ могут подлежать оценке в качестве составной части оценки безопасности системы ИТ. На рис. 5 представлена декомпозиция первого уровня общей модели ОО. Процесс оценки ОО, как показано на рис. 5, может проводиться параллельно с разработкой или следом за ней. Основными исходными материалами для оценки ОО являются: совокупность свидетельств, характеризующих ОО, включая прошедшее оценку задания по безопасности (ЗБ), в качестве основы оценки ОО; ОО, безопасность которого требуется оценить; критерии, методология и система оценки.

Кроме того, в качестве исходных материалов для оценки возможно также использование вспомогательных материалов (таких, как замечания по применению ОК) и специальных знаний в области безопасности ИТ, которыми располагает оценщик и сообщество участников оценок.

В ОК используются различные формы представления, что показано на рис.6, который иллюстрирует возможный способ последовательного формирования требований безопасности и спецификаций при разработке профиля защиты (ПЗ) или ЗБ. Все требования безопасности ОО, в конечном счете, следуют из рассмотрения предназначения и контекста ОО. Приведенная схема не предназначена для ограничения способов разработки ПЗ и ЗБ, а лишь иллюстрирует, каким образом результаты некоторых аналитических подходов связаны с содержанием ПЗ и ЗБ.

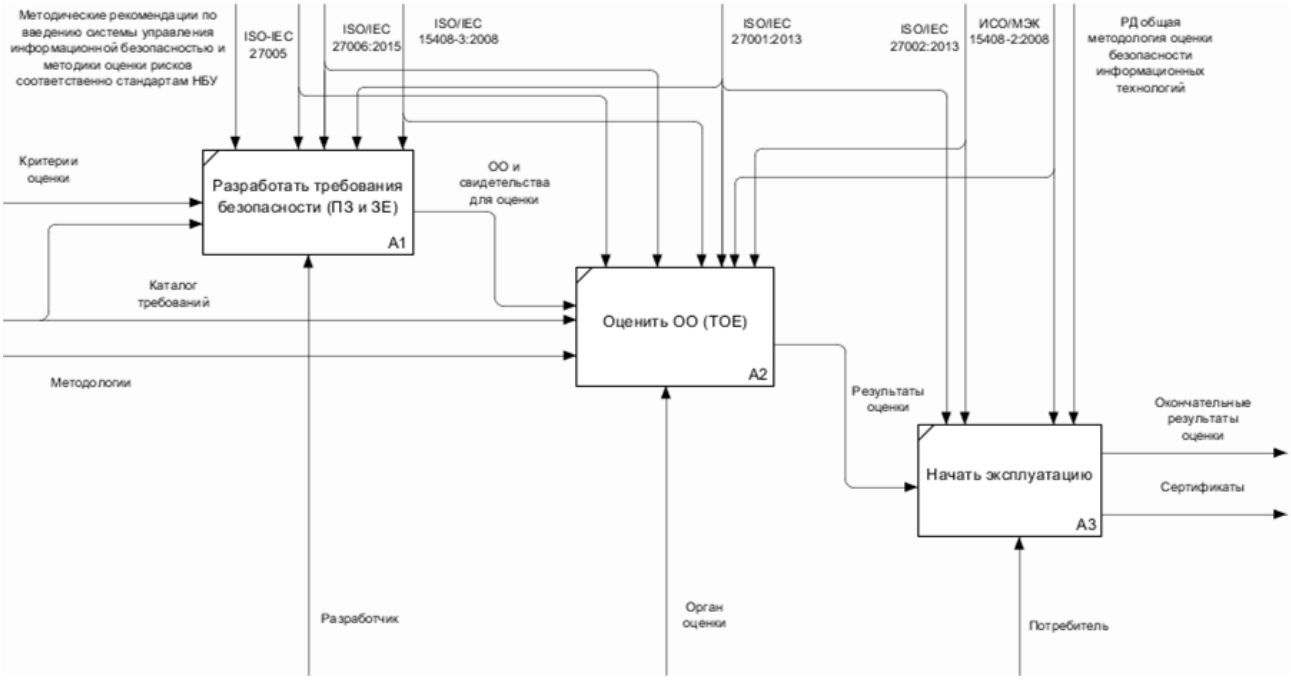

Рис. 5. Диаграмма декомпозиции использования общей модели оценки ОО 1 уровня

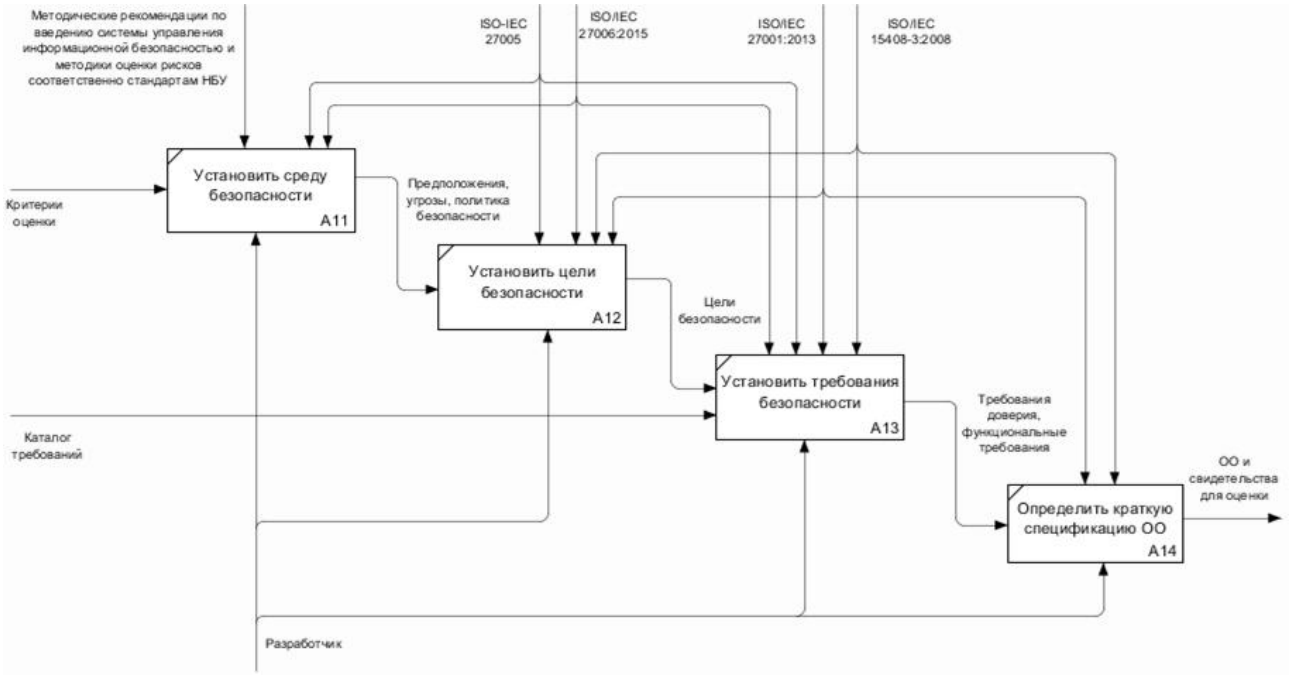

Рис. 6. Диаграмма декомпозиции использования общей модели оценки ОО 2 уровня

Результаты анализа среды безопасности могут использоваться для установления целей безопасности, которые направлены на противостояние установленным угрозам, а также проистекают из установленной политики безопасности организации и сделанных предположений. Необходимо, чтобы цели безопасности были согласованы с определенными ранее целями применения или предназначением ОО как продукта, а также со всеми известными сведениями о физической среде ОО. Требования безопасности ИТ являются результатом преобразования целей безопасности в совокупность требований безопасности для ОО и требований безопасности для среды, которые, в случае их удовлетворения, обеспечат для ОО способность достижения его целей безопасности.

Таким образом, проведенные исследования общей модели оценки ОО показали, что использование основных подходов стандартов и руководящих документов [26-31] позволяют в целом определить основные цели, задания по безопасности, политику и профиль защиты, однако без учета стремительного роста и модификации угроз на классические механизмы средств защиты информации (СЗИ), и появления новых угроз

в различных аспектах киберпространства. Именно последние угрозы несут непоправимые последствия на критические коммуникационные системы к которым относятся АБС.

Усовершенствование методологии оценивания безопасности ИТ АБС Украины

Для формализации методологии оценивания безопасности ИТ АБС Украины воспользуемся предлагаемой последовательностью этапов при определении необходимых средств обеспечения безопасности (рис. 7) и некоторыми основными положениями из известных методик [26, 32].

При этом отметим, что в дальнейшем нижеследующие термины «информационный актив», «источник угрозы информационной безопасности», «модель угроз информационной безопасности», «объект среды информационного актива», «оценка риска нарушения информационной безопасности» и др. понимаются в смысле, определённом в [32].

Рис. 7. Основные этапы методологии обеспечения безопасности ИТ АБС Украины

В соответствии с общим подходом к оценке рисков в предлагаемой методологии на первом и втором этапах банковские информационные активы АБС рассматриваются в совокупности с соответствующими им объектами среды. При этом результаты анализа среды безопасности могут использоваться для установления целей безопасности, направленных на противостояние установленным угрозам, а также проистекают из установленной политики безопасности организации и сделанных предположений. Необходимо учитывать, чтобы цели безопасности были согласованы с определенными ранее целями применения или предназначением ОО, как продукта, а также со всеми известными сведениями о физической среде ОО. Требования безопасности ИТ являются результатом преобразования целей безопасности в совокупность требований безопасности для ОО и требований безопасности для среды, которые, в случае их удовлетворения, обеспечат для ОО способность достижения его целей безопасности. Обеспечение свойств безопасности ИТ АБС для информационных активов выражается в создании необходимой защиты соответствующих им объектов среды.

На третьем и четвертом этапах проводится оценка рисков нарушения безопасности ИТ АБС для типов банковских информационных активов (типов банковской информации), входящих в предварительно определенную область оценки. Для оценки рисков нарушения безопасности ИТ АБС предварительно определяются и документально оформляются: полный перечень типов информационных активов, входящих в область оценивания; полный перечень типов объектов среды, соответствующих каждому из типов информационных активов области оценивания; модель угроз безопасности ИТ АБС, описывающую угрозы безопасности ИТ АБС для всех выделенных в АБС типов объектов среды на всех уровнях иерархии информационной инфраструктуры АБС.

Риск нарушения безопасности ИТ АБС предлагается определять на основании качественных оценок: степени возможности реализации угроз безопасности ИТ АБС (СВР угроз Б ИТ АБС) выявленными и/или предполагаемыми источниками угроз безопасности ИТ АБС в результате их воздействия на объекты среды рассматриваемых типов банковских информационных активов; степени тяжести последствий от потери свойств безопасности ИТ АБС для рассматриваемых типов банковских информационных активов (СТП нарушения Б ИТ АБС).

Оценку СВР угроз Б ИТ АБС и СТП нарушения Б ИТ АБС предлагается базировать на экспертной оценке, выполняемой сотрудниками службы безопасности ИТ банка с привлечением сотрудников подразделений информатизации.

На пятом этапе предлагается использовать синергетическую модель угроз безопасности, позволяющую, как доказано в [1], обеспечить максимальное количество эмерджентных свойств АБС при минимальных ресурсных затратах, направленных на возбуждение в системе синергетического эффекта. Этот подход позволит получить комплексную оценку угроз на основе их пересечения в трех плоскостях защиты банковской информации: кибербезопасности, безопасности информации и информационной

безопасности, с последующим объединением полученных результатов анализа типовых атак.

На последних этапах на основе полученных результатов оценки формируется политика безопасности и профили защиты для каждого уровня стратегической модели управления.

Основным этапом в предлагаемой усовершенствованной методологии оценки является оценка рисков нарушения безопасности ИТ АБС. Основными процедурами данного этапа являются:

– формирование перечня типов банковских информационных активов с определением перечня свойств безопасности ИТ АБС, поддержание которых необходимо обеспечивать в рамках системы оценки безопасности ИТ АБС;

– формирование для каждого типа банковских информационных активов перечня типов объектов среды;

– формирование для типов объектов среды перечня источников угроз в трех плоскостях защиты банковской информации, воздействие которых может привести к потере свойств безопасности ИТ АБС и соответствующих типов банковских информационных активов. Перечень источников угроз формируется на основе синергетической модели угроз;

– оценка СВР угроз Б ИТ АБС на основе предыдущих процедур. Анализ возможности потери каждого из свойств безопасности ИТ АБС для каждого из типов банковских информационных активов в результате воздействия на соответствующие им типы объектов среды выделенных источников угроз;

– оценка СТП нарушения Б ИТ АБС на основе предыдущих процедур. Анализ последствий потери каждого из свойств безопасности ИТ АБС для каждого из типов банковских информационных активов в результате воздействия на соответствующие им типы объектов среды выделенных источников угроз;

– оценка рисков нарушения безопасности ИТ АБС на основании сопоставления оценок СВР угроз Б ИТ АБС и оценок СТП нарушения Б ИТ АБС вследствие реализации соответствующих угроз;

– оценка рисков нарушения безопасности ИТ АБС в количественной (денежной) форме.

На рис. 8 представлена структурная схема модели оценивания информационных технологий на основе предложенной методологии.

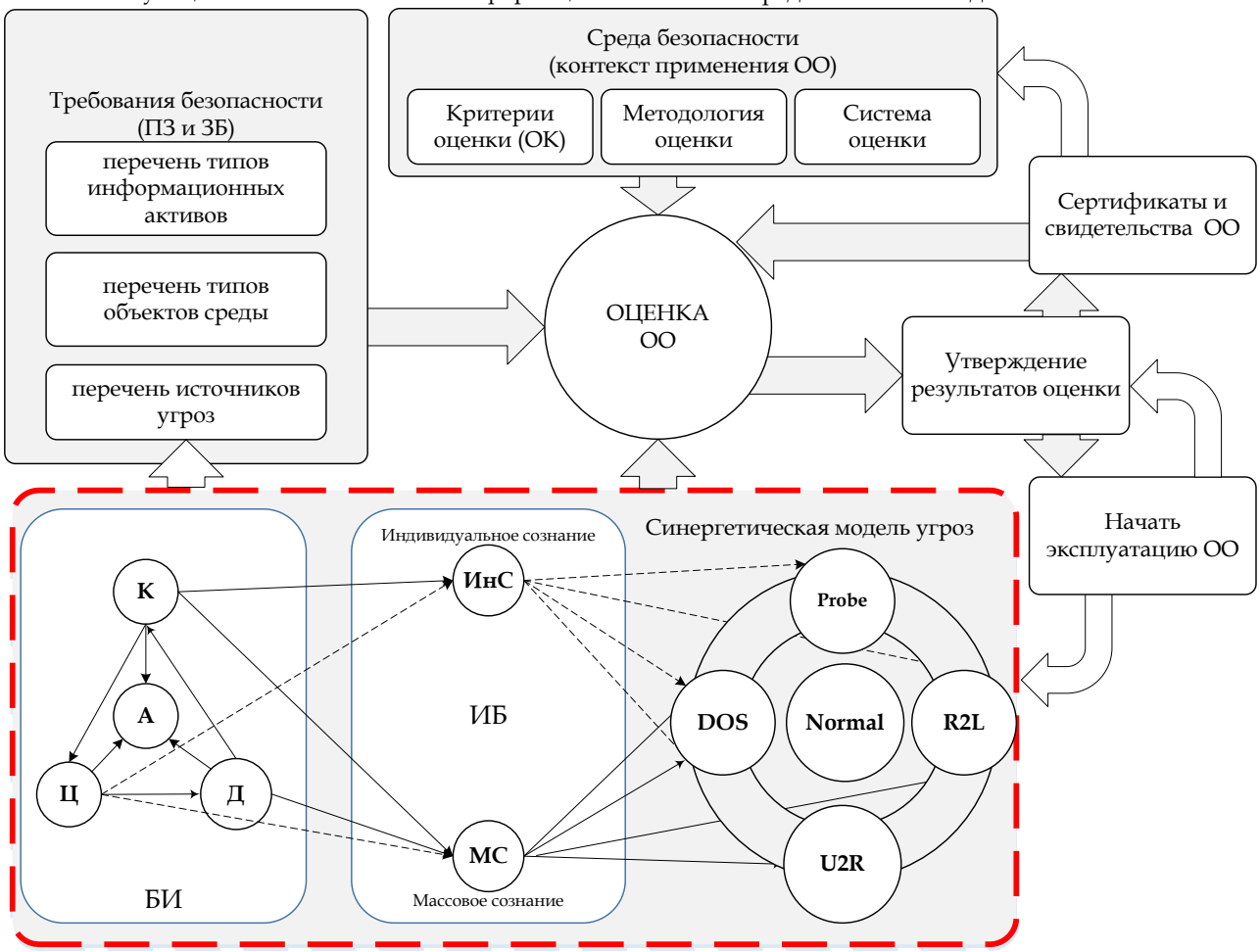

Рис. 8. Структурная схема модели оценки информационных технологий на основе синергетической модели угроз безопасности

Выводы

Прогрессивное развитие ИТ и объединение большинства из них в единый контур обмена информационными потоками кроме всего прочего требует надежных систем обеспечения их кибербезопасности, информационной безопасности и безопасности информации. Не взирая на существенные успехи в борьбе с киберпреступностью вопросы обеспечения безопасности ИТ особенно остро стоят в

банковском секторе не только Украины, но и АБС мирового уровня. Как показывает практика применение международного опыта в обеспечении безопасности ИТ АБС Украины требует дальнейшего усовершенствования не только нормативной и законодательной базы, а также гармонизации ее с лучшими мировыми практиками в этой области, но и собственно научного сопровождения процесса оценивания безопасности ИТ с учетом новых угроз безопасности. Именно поэтому современная методология оценивания безопасности ИТ АБС Украины должна базироваться на синергетической основе, что позволит неразрывно друг от друга дополнять и восполнять, в случае необходимости, различные аспекты обеспечения безопасности. Отсутствие других альтернативных подходов побуждает насущную необходимость в решении сложившейся проблемы – повышения защищенности ИТ АБС на основе новых предлагаемых в работе подходов.

С этой целью разрешения сложившегося противоречия в статье предложена Концепция стратегического управления безопасностью ИТ АБС Украины на основе трехуровневой модели и синергетической модели угроз. Она, в отличие от известных концепций, охватывает все основные направления развития деятельности банка по обеспечению кибербезопасности, информационной безопасности и безопасности информации. Кроме того, она закладывает основы синергизма при выборе наиболее эффективных направлений достижения поставленных целей безопасности с учетом величины риска на каждом уровне модели стратегического управления банком, что является новым в банковской сфере. Разработанная Концепция послужила базисом для создания методологии оценивания безопасности ИТ АБС Украины. В отличие от известных, предложенная методология учитывает целенаправленное или случайное пересечение угроз безопасности ИТ АБС, что позволяет предпринимать адекватные меры защиты БИн, а на основе полученных синергетических оценок безопасности разрабатывать, внедрять и сопровождать новые защищенные ИТ для банковского сектора.

Литература

[1] Hryshchuk R. The synergetic approach for providing bank information security: the problem formulation // R. Hryshchuk, S. Yevseiev / Безпека інформації. – 2016. – № 22 (1). – С. 64 – 74. – doi:10.18372/2225-5036.22.10456

[2] Грищук Р. В. Основи кібернетичної безпеки : Монографія / Р.В. Грищук, Ю.Г. Даник; за заг. ред. проф. Ю.Г. Даника. – Житомир : ЖНАЕУ, 2016. – 636 с.

[3] Sun L., Srivastava R. P., Mock T. J. An Information Systems Security Risk Assessment Model under Dempster-Shafer Theory of Belief Functions // [Электронный ресурс]. – Режим доступа к ресурсу: http://www.tandfonline.com/doi/abs/10.2753/MIS0742-1222220405. – doi: 10.2753/mis0742-1222220405

[4] Потий А.В. Концепция стратегического управления информационной безопасностью // А. В. Потий, Д.Ю. Пилипенко / Радіоелектронні і комп'ютерні системи. 2010. – № 6 (47). – С. 53 – 58.

[5] Потий А.В. Классификация показателей безопасности информации // А.В. Потий, Д.Ю. Пилипенко / Системи обробки інформації, 2010. Вип. 3(84). – С. 53 – 56.

[6] Горбенко И.Д. Критерии и методология оценки безопасности информационных технологий// И.Д. Горбенко, А.В. Потий, П.И. Терещенко / [Электронный ресурс]. – 2000. – Режим доступа к ресурсу: http://www.bezpeka.com/ru/lib/spec/infsys/art108.html.

[7] Trusted Computer Systems Evaluation criteria, US DoD 5200.28-STD, 1985.

[8] Information Technology Security Evaluation Criteria, v. 1.2. Office for Official publications of the European Communities, 1991.

[9] Canadian Trusted Computer Product Evaluation Criteria, v. 3.0. Canadian System Security Centre, Communications Security Establishment, Government of Canada, 1993.

[10] Federal Criteria for Information Technology security. – NIST, NSA, US Government, 1993.

[11] ISO/IEC 15408-1:2009 – Information technology – Security techniques – Evaluation criteria for IT security – Part1: Introduction and general model. management [Электронный ресурс]. – Режим доступа: http://www.iso.org/iso/catalogue_detail.htm?csnumber=50341

[12] ISO/IEC 15408-2:2008 – Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements. [Электронный ресурс]. – Режим доступа: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=46414

[13] ISO/IEC 15408-3:2008 – Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements. [Электронный ресурс]. – Режим доступа: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=46413

[14] ДСТУ ISO/IEC TR 13335-1:2003 Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 1. Концепції та моделі безпеки інформаційних технологій. [Электронный ресурс]. – Режим доступа: ttp://lindex.net.ua/ua/shop/bibl/500/doc/11423

[15] ДСТУ ISO/IEC TR 13335-2:2003 Інформаційні технології. Частина 2. Настанови з керування безпекою інформаційних технологій. [Электронный ресурс]. – Режим доступа: http://www.premier-hs.com.ua/ru/content/dstu-isoiec-tr-13335-22003-nastanovi-z-kieruvannia-biezpiekoiu-informatsiinikh-tiekhnologhii

[16] ДСТУ ISO/IEC TR 13335-3:2003 Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 3. Методи керування захистом інформаційних технологій. [Электронный ресурс]. – Режим доступа: http://lindex.net.ua/ua/shop/bibl/500/doc/11425

[17] ДСТУ ISO/IEC TR 13335-4:2005 Інформаційні технології. Настанови з управління безпекою інформаційних технологій. Частина 4.

Вибирання засобів захисту. [Электронный ресурс]. – Режим доступа http://metrology.com.ua/download/iso-iec-ohsas-i-dr/61-iso/290-dstu-iso-iec-tr-13335-4-2005.

[18] ДСТУ ISO/IEC TR 13335-5:2005 Інформаційні технології. Настанови з управління безпекою інформаційних технологій. Частина 5. Настанова з управління мережною безпекою. [Электронный ресурс]. – Режим доступа: http://lindex.net.ua/ua/shop/bibl/500/doc/11427.

[19] ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements. [Электронный ресурс]. – Режим доступа: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534.

[20] ISO/IEC 27002:2013 – Information technology -- Security techniques – Code of practice for information security controls. [Электронный ресурс]. – Режим доступа: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54533

[21] ISO/IEC 27006:2015 – Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems [Электронный ресурс]. – Режим доступа к ресурсу: http://www.iso.org/iso/home/search.htm?qt=ISO%2FIEC+27006%3A2015+&sort=rel&type=simple&published=on.

[22] 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). [Электронный ресурс]. – Режим доступа: https://kyianyn.files.wordpress.com/2010/12/nbu-27001.pdf

[23] Стандарт України СОУ Н НБУ 65.1 СУІБ 1.0:2010. Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою (ISO/IEC 27002:2005, MOD) [Электр. ресурс]. – Режим доступа: http://s-byte.com/useful/27002.pdf

[24]. CEM-97/017. Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model.

[25] Зегжда Д. Как построить защищенную информационную систему / Д. Зегжда, А. Ивашко. – СПб : Мир и семья - 95, 1997. – 312 с.

[26] Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України [Текст]: лист департаменту інформатизації Національного банку України банкам України від 03 березня 2011 р. № 24-112/365. – К.: НБУ, 2011.

[27] Потій О.В. Дослідження методів оцінки ризиків безпеці інформації та розробка пропозицій з їх вдосконалення на основі системного підходу // О.В. Потій, А.В. Лєншин / Збірник наукових праць ХУПС, 2010. Вип. 2(24). – С.85 –91.

[28] ISO/IEC 27005:2011 – Information technology – Security techniques – Information security risk management [Электр. ресурс]. – Режим доступа: http://www.iso.org/iso/ru/catalogue_detail?csnumber=56742

[29] Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. ГОСТ Р ИСО/МЭК 15408-2-2008 [Электронный ресурс]. – Режим доступа к ресурсу:http://primorsky.ru/authorities/executive-agencies/departments/informationsecurity/Documents/doki-po-ib/

[30] Кобзарь М. Методология оценки безопасности информационных технологий по общим критериям // М. Кобзарь, А. Сидак / Информационный бюлетень Jet Info. 2004. Вып. 6(133). – С. 2 – 16.

[31] Руководящий документ. Безопасность информационных технологий. Общая методология оценки безопасности информационных технологий. Проект [Электронный ресурс]. – Режим доступу к ресурсу: http://fstec.ru/component/attachments/293

[32] РС БР ИББС-2.2-2009. Методика оценки рисков нарушения информационной безопасности. [Электронный ресурс]. – Режим доступа к ресурсу: http://www.cbr.ru/credit/gubzi_docs/st22_09.pdf

[33] Постанова Правління Національного банку України від 18 червня 2003 року № 254 «Про затвердження Положення про організацію операційної діяльності в банках України», К: НБУ., 2003. – 28 с.

[34] Корченко А. О. Банківська безпека. / А.О. Корченко, Л.М. Скачек, В.О. Хорошко. – К. : ПВП «Задруга». – 2014. – 185 с.

[35] Іванченко І. С. Забезпечення інформаційної безпеки держави. / І.С. Іванченко, В.О. Хорошко, Ю.Є. Хохлачова, Д.В. Чирков. – К. : ПВП «Задруга», 2013. – 170 с.

УДК 681.3.06 (045)

Євсеев С.П. Методологія оцінювання безпеки інформаційних технологій автоматизованих банківських систем України

Анотація. *Сучасні автоматизовані банківські системи (АБС) щодня піддаються атакам як в кіберпросторі, так і на різних рівнях технічних систем захисту інформації. Особливо гостро стоять питання забезпечення безпеки не тільки критичних транзакцій і банківських операцій, але і захисту всього комплексу банківської інформації (БІн). Тому винахід злочинцями нових витончених атак і технік їх реалізації на автоматизовані банківські системи обумовлює необхідність подальшого вдосконалення правової та методологічний бази, присвяченій питанням оцінювання безпеки інформаційних технологій (ІТ) АБС. Спираючись на науково-технічний аналіз кращих світових і національних стандартів, а також керівних документів в галузі управління інформаційною безпекою (ІБ), в статті вперше розкривається зовсім нова методологія оцінювання безпеки ІТ АБС України. Характерною особливістю запропонованої методології є те, що на відміну від відомих підходів, базисом оцінювання безпеки ІТ АБС України є розроблена синергетична модель загроз безпеки БІн. Запропонована методологія дозволяє враховувати практично весь спектр найбільш актуальних загроз кібербезпеки, інформаційної безпеки та безпеки інформації ІТ АБС України, а на основі отриманої синергетичної оцінки розробляти, впроваджувати та супроводжувати безпечні ІТ АБС.*

***Ключові слова**: автоматизована банківська система, банківська інформація, інформаційна технологія, методологія, синергетична модель загроз, інформаційна безпека, кібербезпека, безпека інформації.*

Yevseiev S. Methodology for information technologies security evaluation for automated banking systems of Ukraine

***Abstract.** Modern automated banking systems (ABS) are daily exposed to attacks in cyberspace and in the different levels of technical protection of information systems. Particularly acute security issues not only of critical transactions and banking operations, but also protection the full range of banking information (BIn). Therefore, the invention of new sophisticated attacks by criminals and techniques to implement them on the automated banking systems necessitates further improvement of legal and methodological base, devoted to security assessment of information technologies (IT) ABS. Based on the scientific and technical analysis of the best international and national standards and guidelines in the field of information security management, in an article for the first time disclosed a completely new methodology for security evaluation of Ukraine's IT security ABS. A characteristic feature of the proposed methodology is that, in contrast to conventional approaches, the basis of security assessment of Ukraine's IT ABS is developed synergetic model of security threats BIn. The proposed methodology allows to consider all spectrum of the most pressing threats to cyber security, information security and information security of Ukraine's IT ABS and on the basis of the synergistic evaluation to design, implement and maintain secure IT ABS.*

***Key words**: automated banking system, banking information, information technology, methodology, synergetic model of threats, information security, cyber security, information security.*

Отримано *3 жовтня 2016 року*, затверджено редколегією *27 жовтня 2016 року*