РОЗДІЛ 13
СИНЕРГЕТИЧЕСКИЕ МОДЕЛИ ОЦЕНКИ БЕЗОПАСНОСТИ В АВТОМАТИЗИРОВАННЫХ БАНКОВСКИХ СИСТЕМАХ

Аннотация. *раскрыта сущность построения синергетической модели оценки безопасности банковской информации (БИн), предложены формальное математическое описание синергетической модели безопасности БИн на основе методологии и синергетическом подходе к обеспечению безопасности БИн и оцениванию безопасности информационных технологий автоматизированных банковских систем (АБС) организаций банковского сектора (ОБС) Украины, а также частных моделей: инфраструктурной модели АБС, синергетической модели угроз, модели нарушителя и модели проведения оценки защищенности АБС. Рассмотрена модель оценки экономической целесообразности внедрения того или иного механизма ТСЗИ в АБС ОБС в зависимости от ценности БИн.*

Ключевые слова: *синергетическая модель безопасности банковской информации, модель нарушителя, модель защищенности АБС.*

Abstract. *The article reveals the essence of building the synergetic model for assessing the security of banking information (BIn), offered a formal mathematical description of synergetic security model Bin based on the methodology and synergetic approach to security BIn and security evaluation of information technologies automated banking systems (ABS), banking organizations (BOs) in Ukraine, as well as special models: infrastructure ABS model, synergetic model threats, intruder's models and security assessment ABS models. The model of evaluation of the economic feasibility of the introduction of a mechanism TSZI in ABS OBS is considered depending on the value BIn.*

Keywords: *synergetic model of banking information security, intruder's model, ABS security model.*

Введение и постановка задачи. Анализ последних исследований и публикаций показал, что при построении защиты информации сложился подход, основанный на представлении процесса ее обработки в виде абстрактной вычислительной среды, в которой работают множество субъектов (пользователей и процессов) с множеством объектов (ресурсы и наборы данных). При этом построение системы защиты заключается в создании защитной среды в виде некоторого множества ограничений и процедур, способных под управлением ядра безопасности запретить несанкционированный и реализовать санкционированный доступ субъектов к объектам и защиту последних от преднамеренных и случайных внешних и внутренних угроз. Данный подход опирается на теоретические модели безопасности Хартсона, Белла –Лападулы, MMS Лендвера и Мак Лина, Биба, Кларка – Вилсона и др. Считается, что перечисленные модели являются

инструментарием при разработке политик безопасности, определяющих множество требований, которые должны быть выполнены в конкретной реализации системы. При построении защиты информации используют два подхода, использующих представление процесса ее обработки в виде абстрактной вычислительной среды, в которой работают множество субъектов (пользователей и процессов) с множеством объектов (ресурсы и наборы данных). При первом подходе используется модель на основе системы управления информационной безопасностью (СУИБ), второй основывается на использовании системы менеджмента информационной безопасности (СМИБ). В обоих подходах для оценки рисков используются теоретические модели безопасности, основанные на различных моделях разграничения доступа. Однако основными недостатками обоих подходов являются формирование моделей информационной безопасности на основе модели триады CIA (обеспечения конфиденциальности, целостности и доступности), отсутствие разграничений в понятиях “информационная безопасность” (ИБ) и “безопасность информации” (БИ), формальное комплексирование угроз, без учета их особенностей, что не позволяет получить синергетический выигрыш и эмерджентные свойства СБ АБС.

Целью исследования является раскрытие сущности построения синергетической модели безопасности БИн на основе методологии и синергетическом подходе к обеспечению Б БИн и оцениванию безопасности информационных технологий АБС ОБС Украины.

Основным результатом формирования методологических основ обеспечения безопасности ИП, в соответствии с системным подходом является идеализированная или эталонная модель (ЭМ) защищенной АБС ИКП, реализующая принципиально безопасные технологии циркуляции БИн. Кроме этого, ЭМ обеспечивает потенциальную возможность реализации решений стандартизации и унификации архитектурных подходов, путем разработки регламентов и стандартов в области безопасности БИн. Для построения модели безопасности на основе синергетического подхода к оценке угроз БИн, независимо от составляющей безопасности: информационной безопасности (ИБ), кибербезопасности (КБз), безопасности информации (БИ), целесообразно применять принципы Риск-менеджмента, который позволит при грамотном использовании основных его процедур своевременно определить и классифицировать угрозы, и, в соответствии с вероятностью наступления негативных последствий от их возможного проявления адекватно организовать систему обеспечения безопасности БИн.

Очевидно, что одной из важнейших задач оптимального построения комплексной системы защиты информации является выбор из множества средств такого их набора, который позволит обеспечить нейтрализацию всех потенциально возможных угроз с наилучшим качеством и минимально возможными затратами ресурсов. С этой целью используются модели безопасности, позволяющие синтезировать настройки параметров безопасности АБС, уменьшив трудозатраты и повысив степень соответствия нормативных документов на протяжении всего цикла использования ТСЗИ в АБС. На рис. 13.1 приведен обобщенный подход к построению синергетической модели безопасности БИн в АБС.

Анализ рис. 13.1 показывает, что основным отличием предлагаемого подхода моделирования модели безопасности от известных является, во-первых, использование синергетического подхода при построении модели угроз, что дает эмерджентный эффект получения комплексированной оценки угроз БИн, во-вторых, обеспечению успешности выполнения бизнес-процессов посредством функций безопасности БИн (ФББИн), выделенных элементов АБС, основанных на требованиях:

•обеспечение конфиденциальности информации;

•обеспечение доступности информации, сервисов и сетевых, и аппаратных подсистем;

•обеспечение целостности информации;

•обеспечение непрерывности бизнес-процессов.

Введем определения безопасности БИн, основных механизмов и процедур, в рамках построения модели безопасности БИн на основе синергетического подхода:

Банковская информация (БИн) – информация, возникшая в результате банковской деятельности, а также сведения, характеризующие сам банк, его финансовое положение, надёжность и выполнение требований законодательства.

Безопасность 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).

Информационная безопасность банковской информации (ИБ БИн) – состояние защищенности информационной среды банковского сектора, обеспечивающее ее формирование, использование и развитие в интересах граждан и организаций банковского сектора.

Кибербезопасность банковской информации (КБрБ БИн) – набор средств, стратегий, принципов обеспечения безопасности, гарантий безопасности, подходов к управлению рисками, действий, профессиональной подготовки, страхования и технологий, которые используются для защиты киберсреды АБС, ресурсов и пользователей ОБС;

Объектами угроз БИн выступают сведения о составе, состоянии и деятельности банка (персонала, материальных и финансовых ценностей, информационных ресурсов банка).

Угрозы безопасности БИн – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к банковским данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение БИн, а также иных НСД при их обработке в АБС.

Угрозы информации выражаются в нарушении ее доступности, целостности, аутентичности и конфиденциальности.

Синергетический показатель Б БИн в АБС – синергетическая оценка эффективности комплексного применения сил и средств обеспечения безопасности банковской информации в условиях антагонистического противодействия системы банковской защиты случайным и целенаправленным угрозам безопасности.

Источниками угроз выступают конкуренты, злоумышленники-хакеры, баккеры и инсайдеры. Источники угроз преследуют при этом следующие цели: ознакомление с банковской информацией, их модификация в корыстных целях и уничтожение для нанесения прямого материального ущерба.

Неправомерное овладение конфиденциальной информацией возможно за счет ее разглашения, утечки БИн через технические средства и несанкционированного доступа к БИн.

Источниками конфиденциальной информации являются персонал, банковские процессы, документы, технические носители БИн, технические средства обеспечения банковских транзакций.

Основными направлениями защиты информации являются правовая, организационная и инженерно-техническая защиты информации как выразители комплексного подхода к обеспечению информационной безопасности БИн.

Средствами защиты информации являются физические, аппаратные, программно-аппаратные средства и криптографические методы.

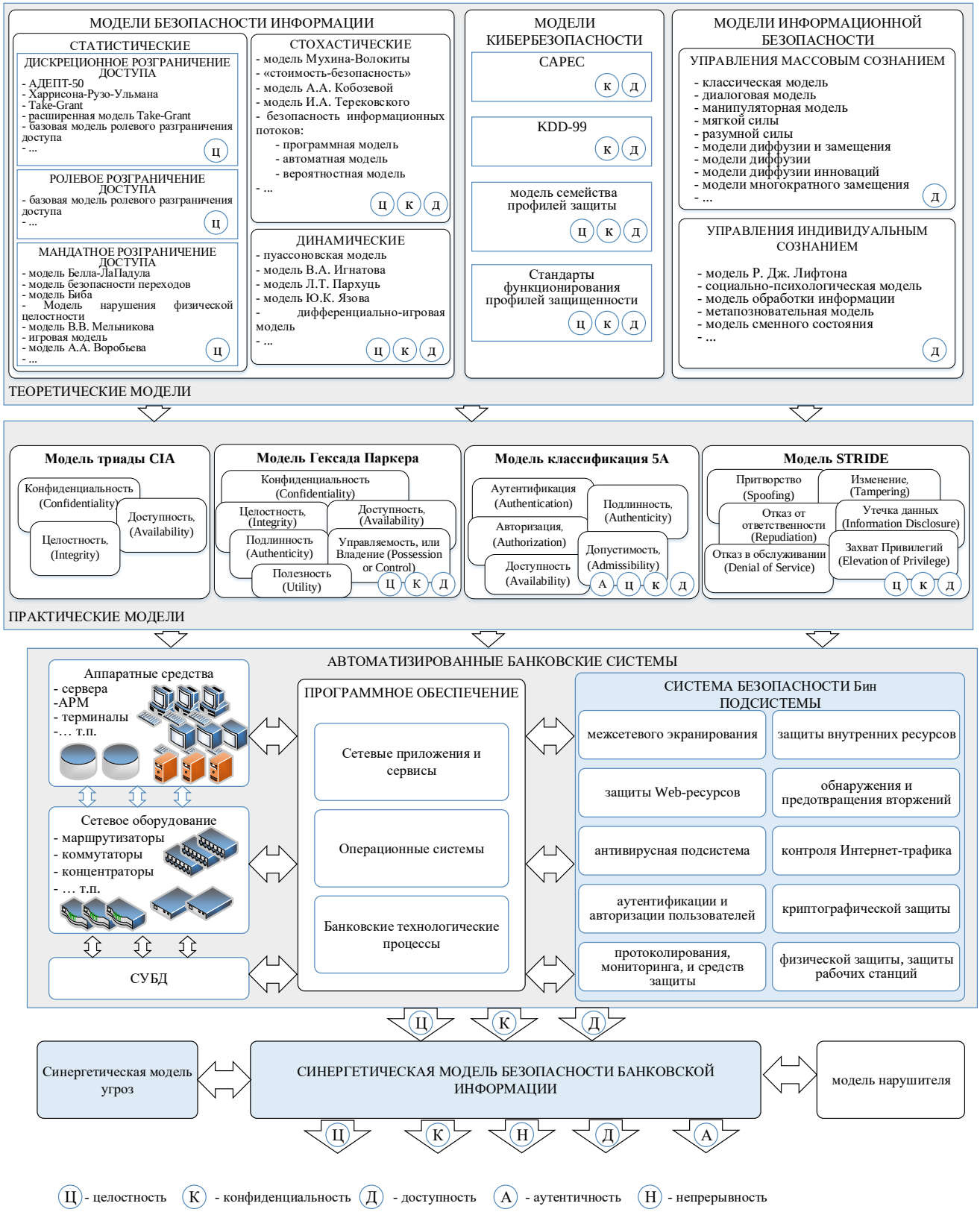

Рис. 13.1. Обобщенный подход формирования синергетической модели безопасности БИн

В качестве *способов защиты* выступают организационно-технические меры, способы и действия, обеспечивающие упреждение противоправных действий, их предотвращение, пресечение и противодействие несанкционированному доступу к БИн. В обобщенном виде рассмотренные компоненты в виде *концептуальной синергетической модели безопасности БИн* приведены на рис. 13.2. Концептуальная синергетическая модель безопасности БИн предлагаемая автором формируется на основе предложенной автором методологии и синергетическом подходе к обеспечению безопасности БИн и оцениванию безопасности информационных технологий (ИТ) АБС Украины [**Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**], а также частных моделей: инфраструктурной модели АБС, синергетической модели угроз и модели проведения оценки защищенности АБС. Инфраструктурная модель АБС представляет собой следующую формальную модель:

$$G^{ABS} = \{\{O^{ABS}\}, \{L^{ABS}\}, \{I_A\}\}, \quad (1)$$

где O^{ABS} – множество объектов среды, описывающих элементы АБС и их принадлежность к уровням иерархии ИКП, L^{ABS} – множество связей между элементами, определяемое матрицей смежности $A^{ABS} = \left\| a_{ij}^{ABS} \right\|$.

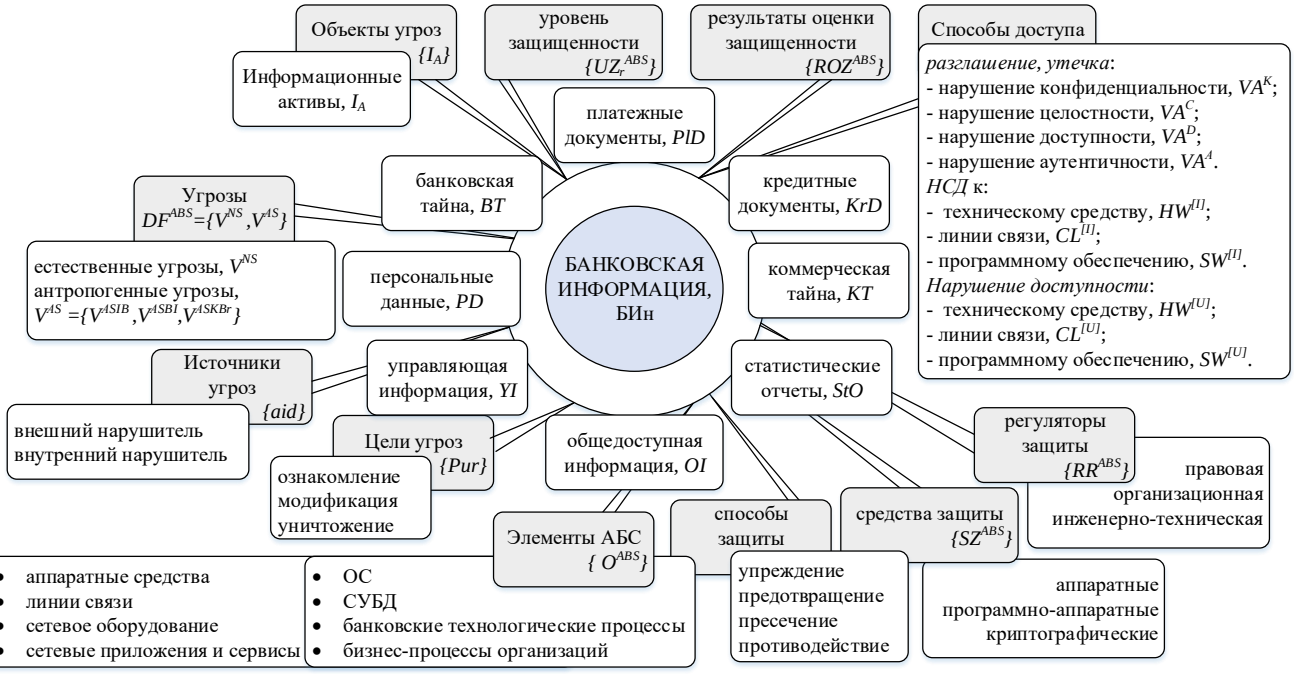

Рис. 13.2. Структурная схема концептуальной синергетической модели безопасности БИн

$\{I_A\}$ – множество элементов информационных активов. Каждый элемент $I_{A_i} \in \{I_A\}$ описывается вектором $I_{A_i} = (Type, A^C, A^D, A^A, A^K, C_Y)$. *Type* – тип информационного актива, описывается множеством базовых значений *Type = {BT, PID, RrD, KT, StO, Ol, YI, PD}*, где *BT* – банковская тайна, *PID* – платежные документы, *KrD* – кредитные документы, *KT* – коммерческая тайна, *StO* – статистические отчеты, *Ol* – общедоступная информация, *YI* – управляющая информация, *PD* – персональные данные. A^K – конфиденциальность, A^C – целостность, A^D – доступность, A^A – аутентичность, C_Y – непрерывность – свойства информации, которые необходимо обеспечивать. Принимают значение 1 – если свойство необходимо, 0 – в противном случае.

Каждый элемент $O_l \in \{O^{ABS}\}$, описывается вектором $O_l = \{Y^{ABS}, TO\}$, где Y^{ABS} – уровень иерархии информационной структуры, определяемое множеством

Y^{ABS} = {*FL, NL, OSL, DBL, BL*}, где *FL* – физический уровень, *NL* – сетевой уровень, *OSL* – уровень операционных систем (ОС), *DBL* – уровень систем управления базами данных, *BL* – уровень банковских технологических приложений и сервисов. Для указания типа связи и существующего отношения IO^R между информационными активами и объектами среды использования используется правило:

$$IO^R = \left\| IO_{il}^R \right\| \tag{2}$$

где IO_{il}^R – отображает наличие и тип связи между *i*-м информационным активом и *l*-м объектом среды. При этом $\forall i \in \{I_A\}$, а $\forall l \in \{O^{ABS}\}$:

$$IO_{il}^R = \begin{cases} 0, \text{связь отсутствует} \\ cs, \text{включает и хранит} \\ pt, \text{обрабатывает или передает} \\ so, \text{поддерживает функционирование} \end{cases}.$$

Синергетическая модель угроз формально может быть представлена в виде:

$$GR^{ABS} = \{\{DF^{ABS}\}, \{T_{risk}\}, \{T_P\}, \{T_U\}, \{VH\}\}. \tag{3}$$

Множество источников угроз безопасности АБС представлено кортежем $DF^{ABS} = \{V^{NS}, V^{AS}\}$, в котором V^{NS} – класс естественных источников угроз,

$V^{AS} = \{V^{ASIB}, V^{ASBI}, V^{ASKBr}\}$ – класс антропогенных угроз, где V^{ASIB} – множество угроз информационной безопасности, V^{ASBI} – множество угроз безопасности информации, V^{ASKBr} – множество угроз кибербезопасности. T_{risk} – качественный показатель риска, T_p – множество базовых термов вероятности реализации хотя бы одной угрозы *j*-му активу, T_U – множество базовых термов величины ущерба от реализации угрозы u_i, *VH* – множество деструктивные состояния элементов АБС, под которыми понимается нежелательное и незапланированное состояние компонента АБС, в котором он оказался в результате реализации одной или нескольких угроз [**Ошибка! Источник ссылки не найден.**].

Для получения синергетического эффекта повышения уровня защищенности БИн необходимо учитывать комплексирование угроз:

$$DF^{ABS} = \{V^{NS}\} \cup \{V^{AS}\}, \text{ где } \{V^{AS}\} = \{V^{ASBI}\} \cap \{V^{ASIB}\} \cap \{V^{ASKBr}\} \quad (4)$$

Каждый элемент из множества угроз $DF_i \in \{DF^{ABS}\}$, может быть представлен следующим вектором значений DF_i *(p,u,risk)*, где *p* – вероятность реализации угрозы, *u* – потенциальный ущерб, *risk* – риск, выраженный в качественной форме и принимающий одно из двух состояний T_{risk}={допустимый, недопустимый}={α_{r1},α_{r2}}.

Оценка вероятности реализации *i*-й угрозы к *j*-му активу определим на основе предложений авторов в работе [4]: для учета связей между источниками угроз и элементами АБС задается матрица $A^{DF} = \|a_{ij}^{DF}\|$, размерностью *n* на *m*, где *n* – количество угроз, *m* – количество активов. Для каждой *i*-й угрозы к *j*-му активу определяется вероятность реализации pr_{ij} на основе либо накопленных статистических данных, характерных для данного региона и условий эксплуатации (в количественной и/или качественной форме), либо экспертным путем.

Расчет вероятности реализации хотя бы одной угрозы для каждого актива выполняется по формуле:

$$p_{rj} = 1 - \prod_{i=1}^{m} (1 - pr_{ij}), \quad (5)$$

где p_{rj} – вероятность реализации хотя бы одной угрозы *j*-му активу.

Предполагается, что в случае реализации для *j*-го актива хотя бы одной из угроз из множества $V^{AS} = \{V^{ASIB}, V^{ASBI}, V^{ASKBr}\}$, ущерб равняется стоимости актива на основе детализации активов и тщательного выбора актуальных угроз:

$$q_j = u_j \quad (6)$$

Считается, что угрозы могут быть реализованы независимо друг от друга, тогда цена риска R_j для каждого *j*-го актива определяется по формуле:

$$R_j = pr_j \times q_j. \quad (7)$$

Цена полного риска равна сумме цен риска всех активов:

$$R_{полн} = \sum_{j=1}^{n} R_j . \quad (8)$$

Таким образом, вероятность реализации среды p_{rj}, с областью определения P = [0, 1] зададим множеством базовых термов T_p = {нереализуемая, минимальная, средняя, высокая, критичная} = $\{\alpha_{x1}, \alpha_{x2}, \alpha_{x3}, \alpha_{x4}, \alpha_{x5}\}$.

Оценка потенциально возможного ущерба от реализации угрозы тесно связано с капиталом (см. выражение (6)) и формируется на основе экспертных оценок. Величина ущерба от реализации угрозы u_i задается множеством базовых термов T_U = {минимальная, средняя, высокая, критичная} = $\{\alpha_{y1}, \alpha_{y2}, \alpha_{y3}, \alpha_{y4}, \alpha_{y5}\}$. Для перехода между качественными и количественными значениями используем правило, предложенное в [**Ошибка! Источник ссылки не найден.**].

Для определения значения рисков воспользуемся правилом, предложенным в работе [18] на основе системы нечетких высказываний:

$$\tilde{L}^1 = \begin{cases} \tilde{L}_1^1 : \langle E_{11} \cup E_{12} \cup E_{13} \cup E_{14} \cup E_{21} \cup E_{22} \cup E_{23} \cup E_{31} \cup E_{32} : risk_i \text{ есть } \alpha_{r1} \rangle; \\ \tilde{L}_2^1 : \langle E_{24} \cup E_{33} \cup E_{34} \cup E_{42} \cup E_{43} \cup E_{44} \cup E_{51} \cup E_{52} \cup E_{53} \cup E_{54} : risk_i \text{ есть } \alpha_{r2} \rangle \end{cases}, \quad (9)$$

где E_{kj}: “p_{ri} есть α_{xk} и u_i есть α_{yj}”

В ходе анализа документов по моделированию угроз, оценке рисков и теории надежности определены следующие *деструктивные состояния элементов АБС* (множество $\{VH\}$):

а) *информационный актив*: недоступен (нарушена доступность), $I_A^{[D]}$; скомпрометирован (нарушена конфиденциальность), $IA^{[K]}$; изменен (нарушена целостность), $I_A^{[C]}$; нарушена метка безопасности (цифровая подпись) (нарушена аутентичность), $I_A^{[A]}$;

б) *программное обеспечение*: недоступно (произошел сбой), $SW^{[B]}$; взломано (получен несанкционированный доступ (НСД) злоумышленником или повышены привилегии пользователя), $SW^{[I]}$; нарушение доступности, $SW^{[U]}$; изменено (не санкционированно изменен код и/или конфигурация), $SW^{[M]}$;

в) *техническое средство*: недоступно (произошел временный сбой), $HW^{[B]}$; нарушение доступности, $HW^{[U]}$; неработоспособно (произошел отказ, требующий ремонт или замена), $HW^{[D]}$; утеряно (произошла потеря или кража у законного владельца), $HW^{[L]}$; взломано (получен несанкционированный доступ (НСД) злоумышленником или повышены привилегии пользователя), $HW^{[I]}$;

г) *линия связи*: недоступна (произошел сбой или отказ), $CL^{[D]}$; нарушение доступности, $CL^{[U]}$; взломана (получен НСД злоумышленником), $CL^{[I]}$.

Формальную модель злоумышленника определим с учетом предложений авторов [5] в которых определены категории и действия злоумышленников:

$$G_{IA}^{ABS} = \left\{ aid_i, pur_i, T_{IA}, S_{\max_i}, pr_j, MS_i^{ABS} \right\} \forall i \in n, \forall j \in m, \tag{10}$$

где $aid_i \in \{aid\}$ – идентификатор нарушителя, $pur_i \in \{pur_i\}$ – цель нарушителя, T_{IA} – время успешной реализации угрозы, $S_{\max_i}$ – вероятностный ущерб системы, $MS_i^{ABS} = \{ms_i\}_{i=1}^{N_{MS^{ABS}}}$ – рекомендации по выявлению, реагированию ТСЗИ, $N_{MS^{ABS}}$ – количество рекомендаций известных АБС, n – количество угроз, m – количество активов.

Под *источником угроз* понимается субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Множество источников угроз включает источники четырёх видов:

$$DF^{ABS} = \left\{ V^{NS}, V^{AS}, TS, PI, NI \right\}, \tag{11}$$

где DF^{ABS} – множество источников угроз безопасности АБС, в котором V^{NS} – класс естественных источников угроз, $V^{AS} = \left\{ V^{ASIB}, V^{ASBI}, V^{ASKBr} \right\}$ – класс антропогенных угроз, где V^{ASIB} – множество угроз информационной безопасности, V^{ASBI} – множество угроз безопасности информации, V^{ASKBr} – множество угроз кибербезопасности; TS – технические средства и системы; PI

– преднамеренные нарушители; *NI* – непреднамеренные нарушители (злоумышленники).

Сценарием реализации угроз называется один или несколько связанных переходов компонентов АБС в деструктивные состояния в результате воздействий источников угроз. Один или несколько сценариев реализации угроз могут быть представлены ориентированным графом *G(V,H)*, в котором: начальной вершиной (v_0) является множество, один из видов или конкретный источник угроз; промежуточными и конечными вершинами (v_n) являются деструктивные состояния компонентов АБС; дугами (h_{ij}) соединятся две вершины, одна из которых является причиной (v_i), а вторая – следствием и результатом перехода (v_j), Сценарий реализации угроз конфиденциальности рассмотрен в работе [**Ошибка! Источник ссылки не найден.**].

Для оценки показателей степени опасности нарушителей и степени реализации защитных мер определим наборы взвешенных метрик, принимающих значения в интервале [0; 1]. Каждая метрика характеризует степень соответствия некоторого признака нарушителя или защитной меры заданному целевому значению.Для оценки степени опасности нарушителя предлагается использовать следующие метрики, сформированные с учетом положений [**Ошибка! Источник ссылки не найден.**]: мотивация, оснащенность (имеющееся оборудование), техническая компетентность, знание информации о АБС и ТСЗИ, права доступа (до реализации угроз), время доступа (до момента обнаружения и реагирования).

Степень опасности *i*-го нарушителя определяется по формуле:

$$d_i = \prod \left(M_{ih}^{DF^{ABS}} \right)^{w_{ih}^{DF^{ABS}}} \tag{12}$$

где $M_{ih}^{DF^{ABS}}$ – значение *h*-ой метрики *i*-го нарушителя;

$w_{ih}^{DF^{ABS}}$ – весовой коэффициент *h*-ой метрики *i*-го нарушителя, $\sum_h w_{ih}^{DF^{ABS}} = 1.$

Метрики степени реализации защитных мер, подразделяемых на превентивные (предотвращение перехода элемента АБС в деструктивное состояние) ψ_j и корректирующие (снижающие величину ущерба от перехода) $\psi_j^{/}$ определим по формуле:

$$\psi_j = \prod_g \left(\sum_l w_{gl}^{SZ^{ABS}} \times M_{gl}^{SZ^{ABS}} \right)^{w_{jg}^K}, \tag{13}$$

где $M_{gl}^{SZ^{ABS}}$ – значение метрики *l*-ой защитной меры *g*-ой категории;

$w_{gl}^{SZ^{ABS}}$ – весовой коэффициент *l*-ой защитной меры *g*-ой категории, $\sum_{l} w_{gl}^{SZ^{ABS}} = 1.$

w_{jg}^{K} – весовой коэффициент *g*-ой категории, $\sum_{g} w_{jg}^{K} = 1.$

Степень реализации корректирующих защитных мер $\psi_j^{/}$ по аналогии с ψ_j определяется по формуле (6). Вектор весовых коэффициентов *W* определяется путем нормирования результирующего вектора приоритетов, определяемого экспертным путем:

$$w_i = \overline{b_i} \Big/ \sum_{i=1}^{m} \overline{b_i}, \forall i \in [1;m], \quad \overline{b_i} = \sqrt[K_E]{\prod_k b_{ik}}, \tag{14}$$

где $\overline{b_i}$ – результирующий приоритет *i*-го элемента;

b_{ik} – приоритет *i*-го элемента, оцененный *k*-м экспертом;

m – размерность матрицы парных сравнений;

K_E – число экспертов.

Формирование экспертной группы (количество экспертов) вычислим за формулой:

$$K_E \geq 0{,}5\left(0{,}33/\beta + 5\right), \tag{15}$$

где β – ошибка результата экспертного анализа или допустимая вероятность ошибки.

Согласованность полученных оценок определяется дважды. Сначала оценивается индекс согласованности оценок эксперта:

$$C_E = \frac{\lambda_{k_{\max}} - m}{m-1}, \tag{9}$$

где $\lambda_{k_{\max}}$ – максимальное собственное число матрицы парных сравнений *k*-го эксперта; *m* – размерность матрицы парных сравнений.

Оценки эксперта считаются согласованными, если отношение согласованности $CR = C_E/CIS$, где *CIS* – среднее значение индекса согласованности, определяемый в диапазонах (табл. 13.1).

Согласованность мнений группы экспертов определяется по правилу трех сигм. несогласованные оценки не учитываются при расчете результирующего вектора приоритетов $\overline{B} = \left(\overline{b_1}, \overline{b_2}, ..., \overline{b_m}\right)^T$.

Таблица 13.1

Значения *CIS* и *CR* от *m*

m	3	4	5	6	7	8	9	10	11	12
CIS	0,58	0,90	1,12	1,24	1,32	1,41	1,45	1,49	1,51	1,48
CR	[0;0,05]	[0;0,08]	[0;0,1]							

Доверительный интервал δ_i определяется по формуле:

$$\delta_i = t_{cm} \times \sigma_{gi} / \sqrt{K_E}\,, \tag{16}$$

где t_{cm}=0,95 – критерий Стьюдента;

σ_{gi} – геометрическое стандартное отклонение.

Для построения метрик угроз на основе синергетического подхода, предложенного в работе [**Ошибка! Источник ссылки не найден.**] воспользуемся подходом построения классификатора угроз на основе информационно-аналитической модели метода двойных троек, предложенного авторами в работе [**Ошибка! Источник ссылки не найден.**]. В отличие от известного при построении классификатора содержательная часть каждой из четырех платформ включает в себя соответственно: *первая платформа* – классификация угроз по отношению к составным обеспечения безопасности БИн в АБС ОБС: информационная безопасность (ИБ) (01), безопасность информации (БИ) (02), кибербезопасность (КБр) (03).

вторая платформа – классификация угроз по характеру направлений: нормативно-правовое (01), организационное (02), инженерно-техническое (03);

третья платформа – классификация угроз в соответствии с основными особенностями информации: конфиденциальность (01), целостность (02), доступность (03), аутентичность (04);

четвертая платформа – классификация угроз по уровням иерархии инфраструктуры АБС: *FL* – физический уровень (01), *NL* – сетевой уровень (02), *OSL* – уровень операционных систем (ОС) (03), *DBL* – уровень систем управления базами данных (04), *BL* – уровень банковских технологических приложений и сервисов (05). На рис. 13.3 приведена взаимосвязь структурной схемы классификатора угроз с АБС ОБС.

Впервые методологию построения классификатора угроз, принципы и методику представления, семантику и систему кодирования различных классов угроз государственных информационных ресурсов (ГИР), а также классификатор для первого широкого класса угроз ГИР, сформированных на основе нормативно-правового направления представлены в работах Юдина О.К., Бучика С.С. В работе [**Ошибка! Источник ссылки не найден.**] предлагается

модифицированный классификатор, основанный на синергетическом подходе к формированию моделей нарушителя и оценки угроз, с учетом специфики угроз и инфраструктуры в АБС ОБС.

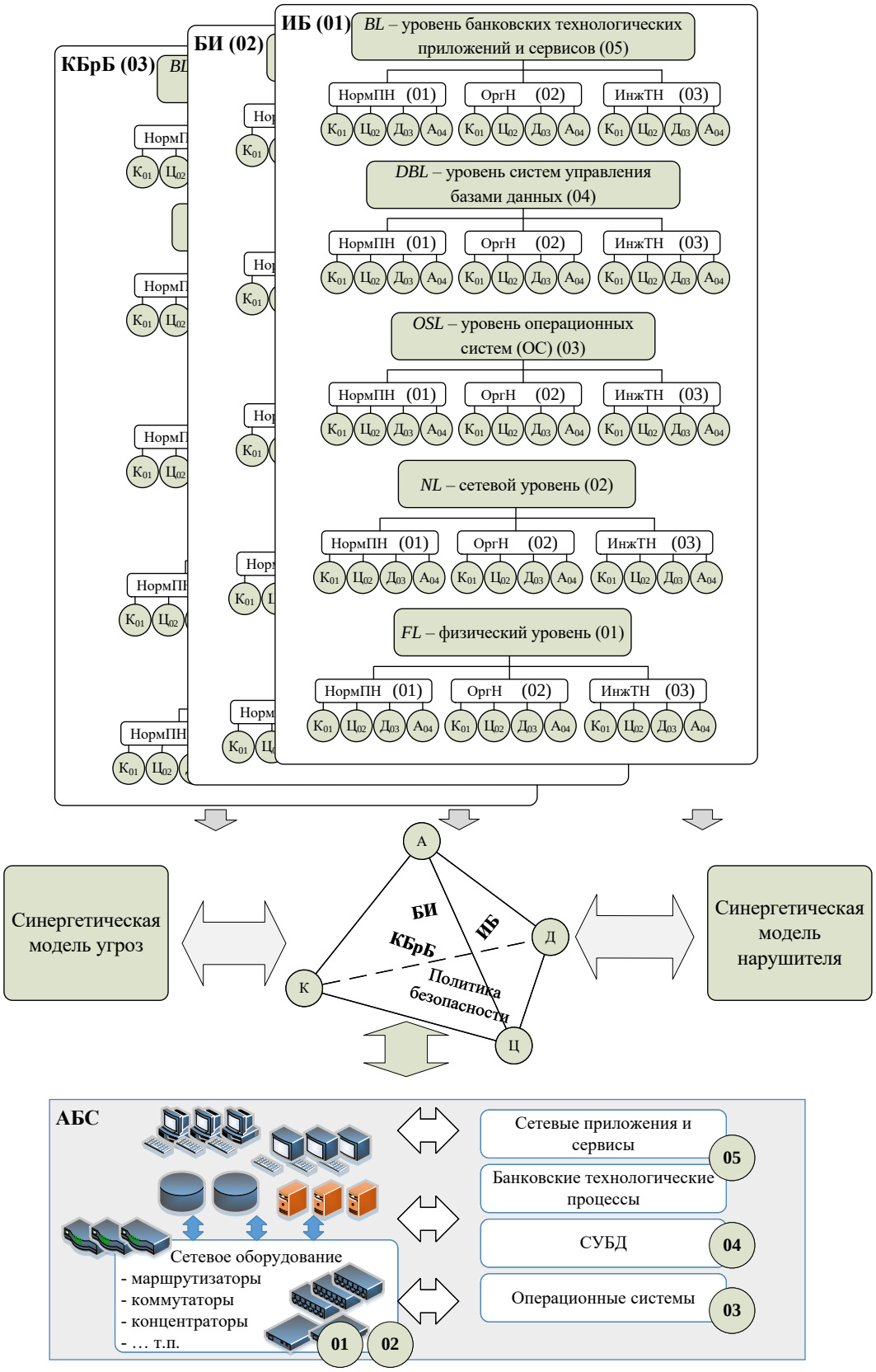

Рис. 13.3. Взаимосвязь структурной схемы классификатора угроз с АБС ОБС

Описание модифицированного классификатора угроз состоит из четырех числовых величин:

– составная обеспечения безопасности БИн в АБС ОБС: информационная безопасность (ИБ) (01), безопасность информации (БИ) (02), кибербезопасность (КБр) (03);

– характер направлений: нормативно-правовое (01), организационное (02), инженерно-техническое (03);

– основные особенности информации: конфиденциальность (01), целостность (02), доступность (03), аутентичность (04);

– уровни иерархии инфраструктуры АБС: *FL* – физический уровень (01), *NL* – сетевой уровень (02), *OSL* – уровень операционных систем (ОС) (03), *DBL* – уровень систем управления базами данных (04), *BL* – уровень банковских технологических приложений и сервисов (05). Части классификатора разделяются точкою и имеют вид, представленный на рис. 13.4.

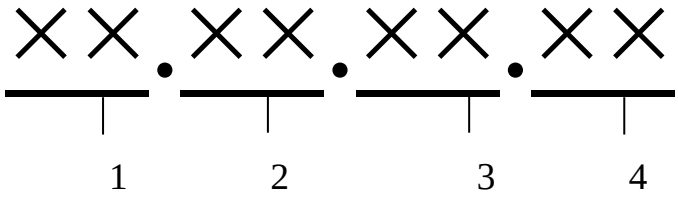

Рис. 13.4. Части классификатора

(1 – синергетическая составная обеспечения безопасности БИн, 2 – характер направлений; 3 – особенности информации; 4 – уровни иерархии инфраструктуры АБС).

Представленная классификация позволяет сформировать соответствующие метрики угроз и превентивных защитных мер.

На основании полученных от модели угроз данных осуществляется соотношение угроз с возможностями нарушителя той или иной категории. Перечень угроз классифицируется на основе уровней иерархии информационной структуры *(DF_i).* Для определения связей между категориями нарушителей уровнями иерархии АБС задается матрица $A^{DF} = \left\| a_{ij}^{DF} \right\|$, в которой $a_{ij}^{DF} = 1$, если источник угроз DF_i может реализовать угрозу в отношении *j*-го

актива АБС $O_l \in \{O^{ABS}\}$, а иначе $a_{ij}^{DF} = 0$. Для описания модели оценки защищенности АБС воспользуемся методологией оценивания безопасности ИТ АБС [**Ошибка! Источник ссылки не найден.**], формально предлагается следующая модель:

$$G_{OZ}^{ABS} = \{\{I_A\}, \{O^{ABS}\}, \{DF^{ABS}\}, \{RR^{ABS}\}, \{SZ^{ABS}\}, \{ROZ^{ABS}\}, \{UZ_r^{ABS}\}\}, \quad (17)$$

где $\{I_A\}$ – множество элементов информационных активов;

- $\{O^{ABS}\}$ – множество объектов среды, описывающих элементы АБС и их принадлежность к уровням иерархии ИКП;
- $\{DF^{ABS}\}$ – множество источников угроз безопасности АБС;
- $\{RR^{ABS}\}$ – множество требований регуляторов к обеспечению безопасности БИн;
- $\{SZ^{ABS}\}$ – множество возможных ТСЗИ;
- $\{ROZ^{ABS}\}$ – данные учета о результатах оценки защищенности АБС;
- $\{UZ_r^{ABS}\}$ – уровень защищенности АБС.

Для определения связей между угрозами и информационными активами используется матрица бинарных отношений $A^{DF} = \|a_{ij}^{DF}\|$, при этом $\forall j \in \{I_A\}$, а $\forall i \in \{DF_i\}$.

$$\|A^{DF}\| = \begin{cases} 1, \text{если для } j\text{-го информационного актива существует } i \text{ угроза} \\ 0, \text{если для } j\text{-го информационного актива не существует } i \text{ угроза} \end{cases}. \quad (18)$$

Каждый механизм защиты БИн в АБС $SZ_i \in \{SZ^{ABS}\}$ характеризуется вектором $SZ_i = (T_{SZ}, T_V, C_{SZ})$, где T_{SZ} – тип средства защиты, T_V – время внедрения, C_{SZ} – стоимость. Для описания связи между угрозами и ТСЗИ используется матрица $A^{DFSZ} = \|a_{ij}^{DFSZ}\|$, где a_{ij}^{DFSZ} – отображает наличие связи между i-й угрозой нарушения безопасности $DF_i \in \{DF^{ABS}\}$ и j-м ТСЗИ $SZ_i \in \{SZ^{ABS}\}$. В модели предлагается использовать следующие типы связей:

MZ – имеется механизм защиты, обеспечивающий противодействие ее деструктивному воздействию $VH_i \in \{VH\}$;

NMZ – нет механизма защиты, для обеспечения противодействия i-й угрозы.

При этом $a_{ij}^{DFSZ} \in \{MZ, NMZ\}$, MZ, NMZ – наличие связи типа, определенного между i-й угрозой и j-м ТСЗИ. Для элементов матрицы значения определяются по правилу:

$$\left\| a_{ij}^{DFSZ} \right\| = \begin{cases} MZ, \text{если } i \text{ угроза рззакрываеся } j\text{-}м \text{ ТСЗИ} \\ NMZ, \text{если } i \text{ угроза рззакрываеся } j\text{-}м \text{ ТСЗИ} \end{cases}. \quad (19)$$

Если для всех $i = m$ $a_{mj}^{DFSZ} = NMZ$, то делается вывод что ТСЗИ АБС не способны защитить БИн от данного деструктивного воздействия, и для повышения уровня защищенности АБС необходимо внедрить дополнительные средства и механизмы защиты.

Множество требований регуляторов $\{RR^{ABS}\}$ включает в себя требования к обеспечению безопасности БИн – $\{R_{BBI}\}$, определенных в международных и национальных стандартах, систематизация источников представлена в работе [**Ошибка! Источник ссылки не найден.**], множества оценок степени выполнения требований безопасности – $\{OV_{BBI}\}$, итоговый уровень соответствия безопасности БИн требованиям из множества $\{R_{BBI}\}$ – $\{IU_{BBI}\}$ и определяется:

$$\{RR^{ABS}\} = \{R_{BBI}\} \cup \{OV_{BBI}\} \cup \{IU_{BBI}\}. \quad (20)$$

Общий показатель уровня защищенности АБС, позволяющий оценить, уровень соответствия ТСЗИ требованиям регуляторов, на основе комплексного подхода оценки рисков и синергетической модели угроз определяется по формуле:

$$OPZ^{ABS} = \sum_{i=1}^{k} OPZ_i, \quad (21)$$

где k – количество частных показателей безопасности, OPZ_i – частный показатель, принимающий значения из множества $\{0, 1\}$, принимающий значения в соответствии с правилами [**Ошибка! Источник ссылки не найден.**]:

OPZ_1 – отсутствие недопустимых рисков, в случае если в организации банковского сектора (ОБС) при составлении модели угроз/модели нарушителя и оценки рисков выявлены недопустимые по своему уровню риски, то $OPZ_1 = 0$, в противном случае – $OPZ_1 = 1$;

OPZ_2 – отсутствие опасных угроз, незакрытых механизмами и ТСЗИ, $OPZ_2 = 0$, в случае, если в ОБС при составлении модели выявлены “незакрытые” угрозы – $OPZ_2 = 1$;

OPZ_3 – уровень соответствия безопасности БИн требованиям регуляторов признан рекомендуемым – $OPZ_3 = 1$, в случае, если признан нерекомендуемым – $OPZ_3 = 0$.

На основании полученных данных системе присваивается один из трех уровней защищенности $UZ^{ABS} = \{\text{низкий, средний, высокиий}\}$ в соответствии с правилом:

$$UZ^{ABS} = \begin{cases} \text{высокий, если } OPZ^{ABS} = 3; \\ \text{срредний если } 1 \le OPZ^{ABS} \le 3; \\ \text{низкий, если } OPZ^{ABS} = 0. \end{cases} \quad (22)$$

Полученная в результате аудита оценка защищенности БИн позволяет определить наиболее ценные информационные активы, эффективность используемых средств для их защиты, а также степень соответствия системы ТСЗИ ОБС требованиям к защите и уровню защищенности регуляторов, выявить наиболее уязвимые места и выработать рекомендации по повышению, в случае необходимости, защищенности АБС ОБС.

Для оценки экономической целесообразности внедрения того или иного механизма ТСЗИ в АБС ОБС в зависимости от ценности БИн, циркулируемой в АБС введем следующие обозначения:

V_{BIn}^{ABS} – ценность БИн для ОБС (стороны, обладающей информацией, и пытающейся ее защитить), V_{BIn}^{IA} – ценность БИн для атакующей стороны (пытающейся добыть информацию);

SZ^{ABS} – средства возможных ТСЗИ; $SV^{AS} = \{SV^{ASIB}, SV^{ASBI}, SV^{ASKBr}\}$ – средства, выделяемые на добывание БИн, SV^{ASIB} – средства взлома механизмов и ТСЗИ информационной безопасности, SV^{ASBI} – средства взлома механизмов и ТСЗИ безопасности информации; SV^{ASKBr} – средства взлома механизмов и ТСЗИ кибербезопасности:

$$SV^{AS} = \{SV^{ASIB}\} \text{I} \{SV^{ASBI}\} \text{I} \{SV^{ASKBr}\}; \quad (23)$$

P_{Vj} – вероятность реализации хотя бы одной i-й угрозы j-му активу (вероятность успеха нападающей стороной); p_{Zj} – вероятность защиты от i-й угрозы j-му актива (вероятность успеха защищаемой стороной). Очевидным признается факт, что бессмысленно вкладывать средства в защиту или добывание информации больше, чем ценность БИн:

$$SZ^{ABS} \le V_{BIn}^{ABS},\ SV^{AS} \le V_{BIn}^{ABS}. \quad (24)$$

Предположим, вероятности определяются по формулам:

$$p_{Z_j} = \frac{q_Z \times SZ^{ABS}}{q_Z \times SZ^{ABS} + q_V \times SV^{AS}}, \quad (25)$$

$$p_{V_j} = \frac{q_V \times SV^{AS}}{q_V \times SV^{AS} + q_Z \times SZ^{ABS}}, \quad (26)$$

где $q_Z, q_V -$ весовые коэффициенты, определяющие насколько каждая из сторон близка к цели.

Предположим, что сумма средств, выделенных атакующей стороной равна ценности БИн, и ценность БИн одинакова для обеих сторон, и противоборствующие стороны находятся в равных условиях, тогда экономическая стоимость затрат на защиту БИн не должна превышать:

$$SZ^{ABS} = V_{BIn}^{ABS} \times \frac{\sqrt{5}-1}{2}. \quad (27)$$

Эффективность предлагаемой модели оценки экономических затрат зависит от точности формулировки вероятности успеха защиты и определения ценности БИн.

Выводы. Предложенная в работе синергетическая модель оценки безопасности банковской информации (БИн) разработана на основе методологии и синергетическом подходе к обеспечению безопасности БИн и оцениванию безопасности ИТ АБС ОБС позволяет переосмыслить подход построения политик безопасности БИн на основе выявления эмерджентных свойств с использованием синергетической модели угроз, что позволяет комплексированно подходить к оценке рисков, с учетом главенствования киберугроз. Модель нарушителя позволяет строить типовые модели нарушителя в соответствии с требованиями регуляторов, при этом используется однозначная классификация нарушителей прав доступа, что позволяет избежать привлечения экспертов на этапе предпроектного обследования. Предложенный модифицированный классификатор угроз в АБС ОБС обеспечивает связь модели нарушителя с моделью угроз, позволяет сформировать соответствующие метрики угроз и превентивных защитных мер, семантику и систему кодирования различных классов угроз в АБС ОБС.