УДК 004.056:004.738.5

Евсеев С.П.

Харьковский национальный экономический университет им. С. Кузнеца, Харьков

МОДЕЛЬ НАРУШИТЕЛЯ ПРАВ ДОСТУПА В АВТОМАТИЗИРОВАННОЙ БАНКОВСКОЙ СИСТЕМЕ НА ОСНОВЕ СИНЕРГЕТИЧЕСКОГО ПОДХОДА

В статье предложена модель нарушителя прав доступа в автоматизированную банковскую систему (АБС) на основе синергетического подхода оценки рисков, предложен классификатор угроз АБС.

Ключевые слова: модель нарушителя прав доступа, взвешенные метрики оценки угроз, автоматизированная банковская система, банковская информация, синергетический подход.

Постановка проблемы в общем виде и ее связь с важными практическими заданиями.

Основной задачей исследований в области безопасности автоматизированных банковских систем является разработка новых и усовершенствование имеющихся методов оценки уязвимости (рисков), нанесения ущерба АБС в целом или отдельным ее составляющим компонентам. Вопросы защиты банковской информации (БИн) регламентируются международными и национальными стандартами, Указами президента Украины, постановлениями кабинета министров Украины, нормативными документами национального банка Украины (НБУ). При проведении работ по защите ресурсов БИн требования нормативно-методических ресурсов являются обязательными, в остальных случаях носят рекомендательный характер. Одной из задач мероприятий по защите БИн является построение системы защиты, направленной на противодействие угрозам безопасности. Как правило система защиты строится с учетом моделей нарушителя и модели угроз.

Анализ последних исследований [1 – 17] показал, что 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 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. При первом подходе используется модель на основе системы управления информационной безопасностью (СУИБ) [4, 8, 13, 16], второй основывается на использовании системы менеджмента информационной безопасности (СМИБ) [10 – 12, 15]. В обоих подходах для оценки рисков используются теоретические модели безопасности, основанные на различных моделях разграничения доступа [1 – 3, 18 – 20].

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.

Одной из основных частей моделей угроз является модель нарушителя, обеспечивающая смысловые отношения между полным описанием угроз и предположением о возможностях нарушителя, являющегося источником угроз, которые он может использовать для разработки и проведении атак, а также об ограничениях на эти возможности.

Для построения модели нарушителя используются подходы, имеющие общие классификационные признаки, однако не всегда коррелированные в различных источниках.

При построении моделей нарушителя выделяют внутренних и внешних нарушителей, а также учитывают [5]:

наличие у нарушителей доступа к штатным средствам (совокупность программного, программно-аппаратного и технического обеспечения);

– уровень знаний нарушителей об объектах атак;

– уровень профессиональной подготовки нарушителей;

– возможность использования нарушителями различных средств для проведения атак;

– преследуемые нарушителями цели;

– возможный сговор нарушителей разных категорий.

Помимо этих аспектов, при построении модели нарушителя в АБС следует рассматривать перечень соответствия объектов доступа субъектам атак, описание каналов атак, обоснование исключения субъектов атак из числа потенциальных нарушителей, а также стадии жизненного цикла и уровни АБС, на которые может воздействовать нарушитель.

Для гарантированного решения задач защиты информации в АБС [21, 22] необходимо учитывать следующие уровни воздействия нарушителей: уровни технических каналов, несанкционированного доступа, вредоносного воздействия, закладных устройств, системы защиты информации. Штатные средства, с использованием которых возможен несанкционированный доступ, могут быть самыми разными: программное, программно-аппаратное и техническое обеспечение средств вычислительной техники (СВТ) или АБС. Следовательно, необходимо классифицировать уровень несанкционированного доступа к защищаемой БИн, а также к объектам и линиям связи (ЛС) АБС.

Целью статьи является создание модели нарушителя прав доступа в автоматизированной банковской системе на основе предложенного в [1] синергетического подхода.

Изложение основного материала.

Для построения модели нарушителя АБС воспользуемся подходом, предложенным в работах [1, 5] и на основании [21, 22]. Проведенный анализ литературы [8, 14, 20, 23, 24] позволяет сделать вывод, что архитектура системы безопасности (СБ) АБС организаций банковского сектора (ОБС), покрывающая основные классы угроз должна содержать компоненты, приведенные на рис. 1. Инфраструктурную модель АБС представим, как 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 $A^{ABS} = \left\| a_{ij}^{ABS} \right\|$. $\{I_A\}$ – множество элементов информационных активов. Каждый элемент $I_{A_i} \in \{I_A\}$ описывается вектором $I_{A_i} = \left(Type, A^C, A^D, A^A, A^K, C_Y\right)$. *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.

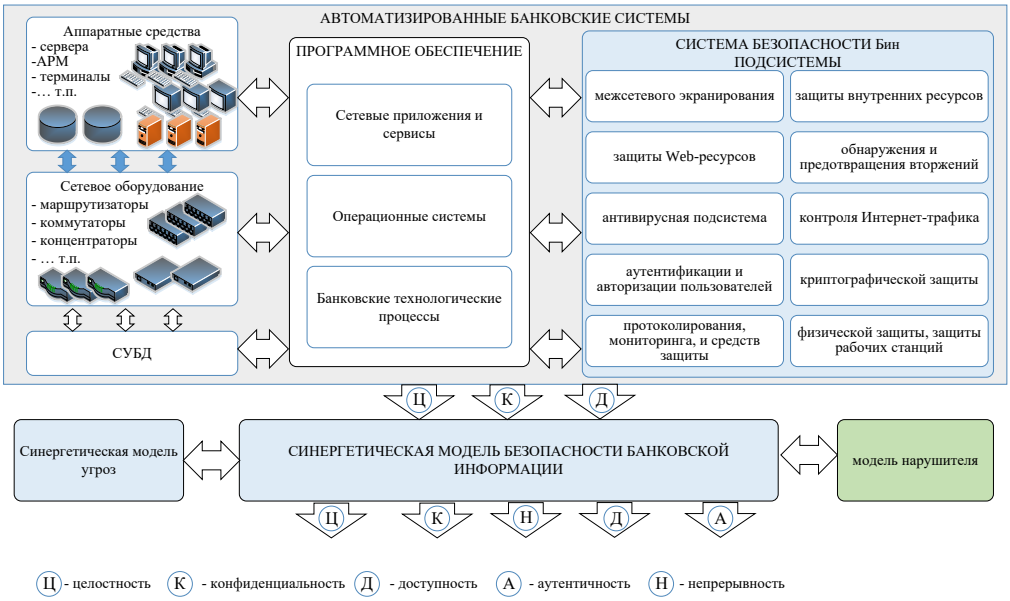


Рис. 1. Архитектура СБ АБС

Каждый элемент $O_l \in \{O^{ABS}\}$, описывается вектором $O_l = \{Y^{ABS}, TO\}$, где Y^{ABS} – уровень иерархии информационной структуры, определяемый множеством $Y^{ABS} = \{FL, NL, OSL, DBL, BL\}$, где 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). 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 $\forall l \in \{O^{ABS}\}$:

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

На основании предложенных квалификационных признаков в [5, 21] модель нарушителя определим за пятью категориями:

1. Пользователи АБС и приложений – работники организации БС, обладающие возможностями по доступу к информации конфиденциального характера в рамках реализации своих служебных обязанностей. Могут воздействовать уровень систем управления базами данных (04), и уровень банковских технологических приложений и сервисов (05), с целью хищения информации, самоутверждения или случайно.

При этом используют технические средства перехвата (ТСП) без модификации компонентов АБС, а также штатные средства и недостатки систем защиты для ее преодоления.

Категорию пользователей АБС целесообразно разделять на следующие группы по уровню доверия: 1.1 – доверенный пользователь (например, высшее руководство организации БС); 1.2. – пользователь (большинство работников ОБС); 1.3 – пользователь “в зоне риска” (например, работники ОБС на испытательном сроке, подавшие заявление на увольнение или ранее участвовавшие в инцидентах ИБ).

2. Эксплуатационный персонал – лица, в том числе не являющиеся работниками организации БС, обладающие возможностями по доступу к информации конфиденциального характера при осуществлении задач, связанных с эксплуатацией и (или) администрированием информационной инфраструктуры ОБС, АБС и приложений организации БС. Могут воздействовать на все уровни – физический уровень (01), сетевой уровень (02), уровень операционных систем (ОС) (03), уровень систем управления базами данных (04), уровень банковских технологических приложений и сервисов (05), с целью хищения информации, а также с целью вывода из строя АБС. При этом используют все средства атак. Возможен сговор с нарушителями третьей и пятой категорий. Не имеют прав доступа к конфигурированию технических средств сети, за исключением контрольных (инспекционных).

3. Технический и вспомогательный персонал – лица, в том числе не являющиеся работниками ОБС, не обладающие полномочиями по доступу к информации конфиденциального характера, но осуществляющие непосредственный физический доступ в помещения, в которых осуществляется обработка такой информации. Могут воздействовать на все уровни – физический уровень (01), сетевой уровень (02), уровень операционных систем (ОС) (03), уровень систем управления базами данных (04), уровень банковских технологических приложений и сервисов (05), с целью хищения информации, а также с целью вывода из строя АБС. При этом используют все средства атак. Возможен сговор с нарушителями второй и пятой категорий.

4. Лица, не являющиеся работниками организации БС, обладающие доступом к информации конфиденциального характера на основании договорных отношений (например, аудиторы, партнеры и подрядчики), требований законодательства (например, органы государственной власти) и (или) судебного решения. Могут воздействовать на все уровни, с целью вывода из строя АБС. При этом используют все средства атак. Возможен сговор с нарушителями второй и пятой категорий. Не имеют доступа к средствам защиты информации и протоколирования и к части ключевых элементов АБС.

5. Внешние нарушители, которыми являются лица, осуществляющие воздействие за пределами контролируемой зоны ОБС. Могут воздействовать на все уровни с целью хищения информации, самоутверждения, а также вывода из строя АБС. При этом используют методы и средства активного воздействия (модификация и подключение дополнительных технических средств, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ).

Данная классификация наиболее полно охватывает аспекты, отраженные в нормативно-методической документации, а также позволяет однозначно классифицировать нарушителя.

Формальную модель нарушителя определим с учетом предложений авторов [5, 15, 16]:

$$G_{IA}^{ABS} = \left\{ aid_i, pur_i, T_{IA}, S_{\max_i}, pr_j, MS_i^{ABS} \right\} \forall i \in n, \forall j \in m, \quad (3)$$

где $aid_i \in \{aid\}$ – идентификатор нарушителя (категория 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.

В ходе анализа нормативных документов [21, 22], предложений изложенных в работе [16] 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), $CL^{[I]}$.

Под *источником угроз* понимается субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации [16].

Множество источников угроз включает источники четырёх видов:

$$DF^{ABS} = \left\{V^{NS}, V^{AS}, TS, PI, NI\right\}, \quad (4)$$

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 [16].

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 [25, 26]: 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:

$$d_i = \prod \left(M_{ih}^{DF^{ABS}} \right)^{w_{ih}^{DF^{ABS}}} \quad (5)$$

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:

$$\psi j = \prod_g \left(\sum_l w_{gl}^{SZ^{ABS}} \times M_{gl}^{SZ^{ABS}} \right)^{w_{jg}^K}, \quad (6)$$

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:

$$w_i = \overline{b_i} \Big/ \sum_{i=1}^{m} \overline{b_i}, \forall i \in [1; m], \quad \overline{b_i} = \sqrt[K_E]{\prod_k b_{ik}}, \quad (7)$$

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 формулою, предложенной в работе [17]:

$$K_E \geq 0{,}5\left(0{,}33/\beta + 5\right), \quad (8)$$

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

Согласованность полученных оценок определяется дважды [16]. Сначала оценивается индекс согласованности оценок эксперта:

$$C_E = \frac{\lambda_{k_{\max}} - m}{m - 1}, \quad (9)$$

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. 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 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:

$$\delta_i = t_{cm} \times \sigma_{gi} / \sqrt{K_E} \ , \qquad (10)$$

где t_{cm} =0,95 – критерий Стьюдента;

σ_{gi} – геометрическое стандартное отклонение.

Для построения метрик угроз на основе синергетического подхода, предложенного в работе [1] воспользуемся подходом построения классификатора угроз на основе информационно-аналитической модели метода двойных троек, предложенного авторами в работах [9–12]. 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). При этом введем следующие определения:

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 АБС.

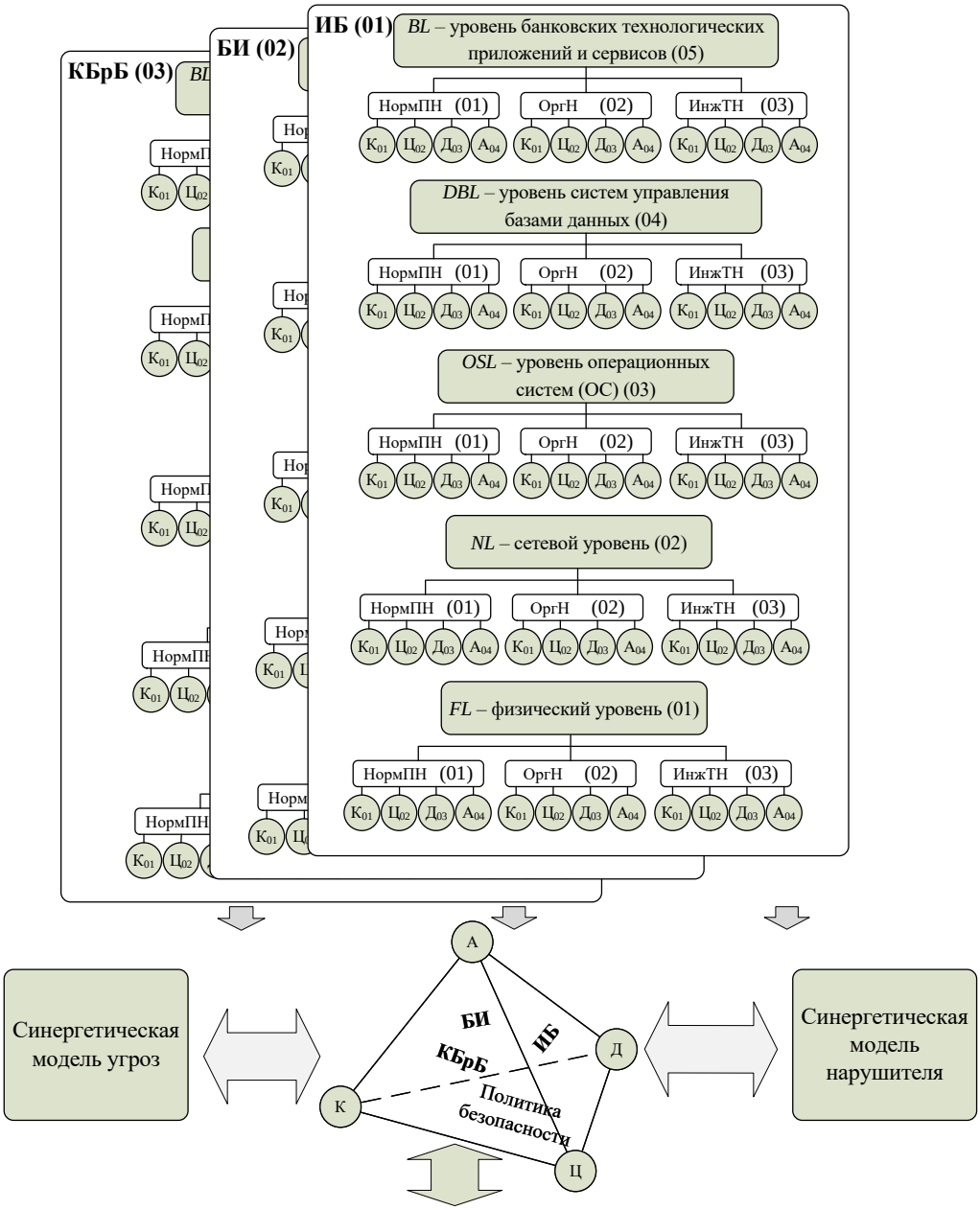
Информационная безопасность банковской информации (ИБ БИн) – состояние защищенности информационной среды ОБС, обеспечивающее ее формирование, использование и развитие в интересах граждан и ОБС.

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;

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. 2 приведена взаимосвязь структурной схемы классификатора угроз с АБС ОБС.



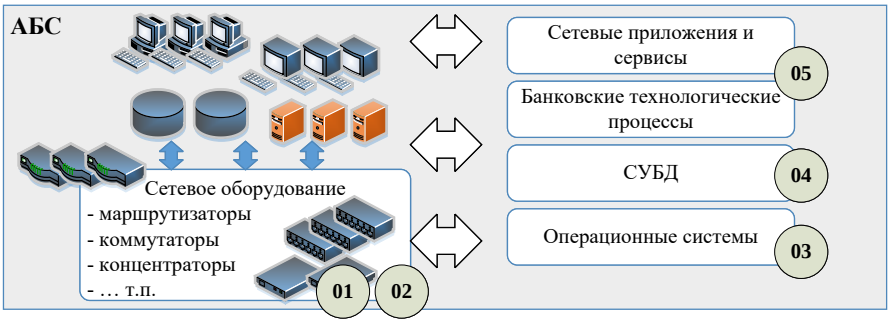


Рис. 2. Взаимосвязь структурной схемы классификатора угроз с АБС ОБС

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 [9 – 12, 17]. В данной работе предлагается модифицированный классификатор, основанный на синергетическом подходе к формированию моделей нарушителя и оценки угроз, с учетом специфики угроз и инфраструктуры в АБС ОБС.

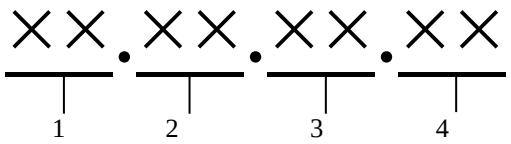
Описание модифицированного классификатора угроз состоит из четырех числовых величин:

– 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. 3.



(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.

Выводы и перспективы дальнейших исследований.

Впервые предложенная в работе модель нарушителя прав доступа в АБС разработана на основе методологии и синергетическом подходе к обеспечению безопасности БИн. Она позволяет систематизировать классификацию нарушителей и обеспечить построение перечня актуальных угроз для каждой категории нарушителей. При исключении субъектов атак из числа потенциальных нарушителей можно уменьшить максимальную категорию нарушителя, а, следовательно, и количество актуальных угроз. Данная модель отличается оригинальной однозначной классификацией нарушителей прав доступа в АБС в соответствии с уровнями их воздействия на АБС, обеспечить возбуждение в системе обеспечения банковской информации управляемых эмерджентных свойств, направленных на получение синергетического эффекта, который достигается благодаря качественно новому подходу к обеспечению безопасности.

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. Применение предложенной модели нарушителя и классификатора угроз позволяет избежать привлечения специалистов по защите информации на этапе предпроектного обследования.

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. Теоретичні основи моделювання процесів нападу на інформацію методами теорій диференціальних ігор та диференціальних перетворень Монографія / Р. В. Грищук. – Житомир : Рута, 2010. – 280 с.

3. Грищук Р.В. Основи кібернетичної безпеки: Монографія / Р.В. Грищук, Ю.Г. Даник; за заг. ред. Ю.Г. Данника. – Житомир: ЖНАЕУ, 2016. – 636 с.

4. Петров О. Повышение информационной безопасности автоматизированных ситсем обработки данных на транспорте / Петров О., Лахно В. // Information Technology in Selected Areas of Management. – Widawnictwa AGH, Krakow 2016. – PP. 65 – 78.

5. Жуков В. Г. Модель нарушителя прав доступа в автоматизированной системе / В. Г. Жуков, М. Н. Жукова, А. П. Стефаров // Программные продукты и системы. – 2012. – № 2. – С. 75 – 78.

8. Аткина В.С. Модель защищенности организаций банковской системы Российской Федерации / В.С. Аткина // Известия ЮФУ. Технические науки, 2013. – Вып. 12 (149). – С.187 – 193.

9. Юдін О.К. Методологія побудови класифікатора загроз державним інформаційним ресурсам / О.К. Юдін, С.С. Бучик, А.В. Чунарьова, О.І. Варченко // Наукоємні технології. – 2014. – № 2 (22). – С. 200-210.

10. Юдін О.К. Класифікація загроз державним інформаційним ресурсам нормативно-правового спрямування. Методологія побудови класифікатора / О.К. Юдін, С.С. Бучик // Захист інформації. – 2015. – Том 17 (2). – С. 108-116.

11. Бучик С.С. Теоретичні основи аналізу ризиків дерева ідентифікаторів державних інформаційних ресурсів / С.С. Бучик // Наукоємні технології. – 2016. – № 1 (29). – С. 70-77.

12. Бучик С.С. Методологія аналізу ризиків дерева ідентифікаторів державних інформаційних ресурсів / С. С. Бучик // Захист інформації. – 2016 – №1 (18). – С. 81-89.

13. Замула А.А. Анализ моделей оценки рисков информационной безопасности для построения системы защиты / А.А. Замула, А.В. Северинов, М.А. Корниенко // Наука і техніка Повітряних Сил Збройних Сил України – 2014. – № 2(15). – С. 133 – 138.

14. Евсеев С.П. Методология оценивания безопасности информационных технологий автоматизированных банковских систем Украины/ С.П. Евсеев// Ukrainian Scientific Journal of Information Security, 2016, vol. 22, issue 3, p. 297 – 309.

15. Нурдинов Р.А., Батова Т.Н. Подходы и методы обоснования целесообразности выбора средств защиты информации // Современные проблемы науки и образования. – 2013. – № 2. [Электронный ресурс]. – Режим доступа к ресурсу: http://elibrary.ru/item.asp?id=21285749.

16. Каторин Ю.Ф. Модель количественной оценки рисков безопасности информационной системы/ Ю.Ф. Каторин, Р.А. Нурдинов, Н.М. Зайцева// [Электронный ресурс]. – Режим доступа к ресурсу: http://www.vestnikmnk/index.php/VMK/article/download/57/56.

17. Бучик С.С. Методика експертного оцінювання функціональних профілів загроз державних інформаційних ресурсів / С.С. Бучик // Открытые информационные и компьютерные интегрированные технологи : науч. тр. – Х.: Нац. аэрокосм. ун-т “ХАИ”, 2015. – Вып. 70. – С. 271-280.

18. Девянин П. Н. Модели безопасности компьютерных систем: Учеб. пособие. – М. : Изд.центр «Академия», 2005. – 144 с.

19. Гайдамакин Н. А. Теоретические основы компьютерной безопасности. - Екатеринбург: изд-во Урал. Ун-та, 2008. – 212 с.

20. Ярочкин В. И. Безопасность банковских систем. – М. : Издательство: Ось-89, 2012. – 416 с.

21. РС БР ИББС-2.9-2016. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Предотвращение утечек информации. [Электронный ресурс]. – Режим доступа к ресурсу: https://www.cbr.ru/credit/Gubzi_docs/rs-29-16.pdf.

22. РС БР ИББС-2.7-2015. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Ресурсное обеспечение информационной безопасности. [Электронный ресурс]. – Режим доступа к ресурсу: http://www.cbr.ru/credit/gubzi_docs/rs-27-15.pdf.

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

24. Евсеев С.П. Анализ законодательной базы к системе управления информационной безопасностью НСМЭП / С.П. Евсеев, О.Г. Король, Г.П. Коц // Восточно-европейский журнал передовых технологий. – Харьков. – 2015. – Вып. 5/3(77). – С. 48-59.

25. ISO/IEC 18045:2014 Information technology – Security techniques – Guidelines for cybersecurity [Электронный ресурс]. – Режим доступа к ресурсу: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=46412

26. ГОСТ Р 181045-2013 Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности ИТ [Электронный ресурс]. – Режим доступа к ресурсу: https://npo-echelon.ru/common_files/gost/GOST-18045-xxxx.pdf.

Рецензент: д.т.н., с.н.с. Грищук Р. В.

Надійшла до редколегії