УДК 621.391

С.П. Евсеев

Харьковский национальный экономический университет имени Семена Кузнеца, Харьков

СИНЕРГЕТИЧЕСКИЙ ПОДХОД К ОЦЕНКЕ БЕЗОПАСНОСТИ БАНКОВСКИХ СИСТЕМ

Рассматриваются законодательные акты в области защиты банковских транзакций, структура банковской информации. Проводится анализ основных источников угроз в модели CIA: конфиденциальность, целостность и доступность данных в автоматизированных банковских системах. В статье предложена синергетическая модель угроз безопасности банковской информации, которая впервые с системных позиций позволила раскрыть современное состояние исследуемой проблемы. Показано и доказано, что на современном этапе развития науки и техники, обеспечение безопасности банковской информации должно основываться на принципиально новом подходе, который предложено называть синергетическим. Его внедрение позволит получить синергетический эффект при взаимодействии выбранных профилей безопасности и, как следствие, проявить качественно новые и неизвестные до этого эмерджентные свойства системы безопасности.

Ключевые слова: *информационная безопасность, безопасность информации, кибернетическая безопасность, угрозы банковских данных.*

Введение

Важное значение в обеспечении безопасности Украины, и особенно экономической ее составляющей, имеет защита ее рыночных основ, определяющих экономическую составляющую конкуренции. Развитие государства тесно связано с развитием рыночных отношений и рентабельной конкурентоспособной экономики, в которой банковский сектор играет главную роль. Революционные изменения последнего десятилетия в электронной индустрии, объединение инфокоммуникационных и компьютерных сетей в единое пространство существенно расширили спектр услуг автоматизированных банковских систем (АБС), при этом одной из наибольшей небезопасной угрозой для экономики Украины является нарушение ее финансово-банковской системы. Таким образом, решение вопросов обеспечения безопасности транзакций в АБС остается актуальной и на сегодняшний день.

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

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

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

Цели и задачи исследования. Целью работы является постановка проблемы обеспечения безопасности банковской информации, а также формирование необходимых и достаточных условий для создания принципиально нового методологического базиса, направленного на достижение синергетического эффекта в сфере безопасности государственных и частных коммерческих систем банковской защиты.

Для достижения поставленной цели были сформулированы следующие частные задачи:

всеобъемлющий критический анализ сущности и содержания категории “банковская информация” на современном этапе развития науки и техники, актуальности и содержательности законодательной и нормативно-правовой базы в сфере защиты банковских транзакций в государственных и частных АБС;

уточнение и дополнение множества актуальных угроз безопасности банковской информации с триединой позиции обеспечения информационной безопасности, безопасности информации и кибербезопасности в банковском секторе, как основы для создания нового синергетического подхода в области обеспечения информационной безопасности АБС;

формализация сущности и содержания проблемы обеспечения безопасности банковской информации на основе предложенного синергетического подхода.

Результаты исследований

1. Анализ основных законодательных актов в сфере защиты банковских транзакций в АБС, структура банковской информации. Деятельность АБС обеспечивается и регулируется на основе законодательных актов и рекомендаций Национального банка Украины, основные нормативные акты представлены на рис. 1. Проведенный анализ законодательной базы Украины показал, что для обеспечения защиты информации в АСБ используются системы управления информационной безопасностью (СУИБ), обеспечивающие контроль функционирования комплексных систем защиты информации.

Таким образом, АБС является комплексной информационной банковской системой, интегрирующей различные сферы деятельности банка, способной автоматизировать и объединить в единые целые бизнес-процессы финансового учреждения. Комплексная система, поддерживающая централизованную обработку, мультивалютность и автоматизацию основных финансовых операций, должна обеспечивать эффективное управление, контроль, получение отчетов о текущей деятельности всех филиалов банка.

Среди функций, присущих современным комплексным АБС, можно выделить следующие: операционный день; операции на фондовом рынке, работа банка с ценными бумагами; внутрихозяйственная деятельность; розничные банковские услуги; дистанционное банковское обслуживание; электронные банковские услуги; расчетный центр и платежная система (карточные продукты); интеграция бэк-офиса банка с его внешними операциями; управление деятельностью банка, реализация бизнес-логики, контроль, учет, в том числе налоговый, и отчетность; управление рисками и стратегическое планирование; программы лояльности клиентов, маркетинговая, рекламная и PR-службы.

Приведенные основные функции АБС реализуются посредством следующих технологий: системы управления базами данных (распределенных);

хранилища данных, OLAP- и OLTP-технологии обработки данных (системы оперативной аналитической обработки и системы оперативной обработки транзакций);

системы поиска, извлечения и подготовки достоверных данных;

распределенная вычислительная система, организация коллективной работы пользователей, создание реального информационного пространства банка, включая филиалы, клиентов и партнеров;

безопасное подключение информационной системы банка к внешним вычислительным сетям (Интернет);

организация безопасной, достоверной передачи данных по общедоступным каналам связи (криптография: шифрование и электронная цифровая подпись (ЭЦП), организационные меры), электронный документооборот;

техническое, программное, математическое и другое обеспечение;

информационная аналитика и системы поддержки принятия решений (decision support systems, DSS);

защита хранимой и обрабатываемой информации, всей АБС в целом;

системы удаленной работы с фондовыми рынками и программы предсказания поведения курсов;

CRM-системы управления отношениями с клиентами;

программы реализации фронт-офиса взаимодействия с клиентами;

системы поддержки внутренней организации, менеджмента и исполнительной деятельности персонала;

разграничение доступа к информации разного уровня секретности;

антивирусная защита;

интернет-магазины и интернет-карточки;

центры обработки вызовов (call-центры) и IP-телефония;

поддержка различных каналов доступа: Интернет, телефон, мобильная сеть, SMS, WAP и др.;

поддержка множественных стандартов учета, включая управленческий учет;

поддержка и исследования в области планомерного информационного развития АБС.

Основой комплексной АБС является *банковская информация* – совокупность сведений, связанных с Уставными документами и Руководством банковского учреждения, организационно-правовой формой банковской учреждения, нынешним видом банковского учреждения и его служащих, видами и формами банковского обслуживания, количеством и составом клиентов, операциями по счетам клиентов, наличием корреспондентских отношений и техническим обеспечением банка [8].

На рис. 2 приведена признаковая классификация банковской информации.

Преимуществом предложенной признаковой классификации банковской информации (см. рис. 2) является то, что она в отличие от известных классификаций позволяет раскрыть глубину содержания сущности данной категории. Например, по видам банковская информация бывает организационной, технологической и параметрической. При этом под *организационной банковской информацией* следует понимать информацию, отображающую характер деловых связей банка с клиентами, информацию про особенности организации и построения системы управления банка. *Технологическая банковская информация* – это информация о принципах управления банком при осуществлении им всех видов банковской деятельности, а также информация о применяемых в системах банковской защиты новейших высокотехнологических разработках. *Параметрическая банковская информация* – это информация, отражающая количественные показатели, отображающие банковский капитал и величину его кредитного портфеля при осуществлении банком всех видов деятельности. Еще одним преимуществом предложенной классификации является то, что в случае появления новых признаков, характеризующих те или иные аспекты категории банковская информация в предложенной классификации, предусмотрена возможность расширения множества признаков.

Из предложенной классификации также следует вывод о том то, что в подсистемах АБС Банка циркулирует информация различных уровней конфиденциальности (секретности) от открытой информации, до сведений, содержащих информацию с ограниченным доступом (коммерческая, банковская и служебная тайна). В документообороте АБС Банка также присутствуют: платежные поручения и другие расчетно-денежные документы, отчеты (финансовые, аналитические и др.), сведения о лицевых счетах, обобщенная информация и другие конфиденциальные (ограниченного распространения) документы и т.д., которые также могут быть отнесены к понятию банковской информации.

Таким образом, в самом общем виде под *банковской информацией* можно понимать информацию, которая возникает в результате банковской деятельности. Это, прежде всего сведения, характеризующие сам банк, его финансовое положение, надёжность и выполнение требований законодательства.

Такую информацию можно почерпнуть из устава банка, его лицензий, бухгалтерских балансов, отчетов о прибыли и убытках и других источников. Кроме того, в более узком понимании банковская информация – это сведения о конкретных операциях банка. Такая информация характеризует не только банк, но и тех лиц, с которыми банк вступает в правоотношения. В качестве примера банковской информации можно привести сведения о наличии счетов или вкладов и об операциях по ним, об имуществе, находящемся на хранении в банке.

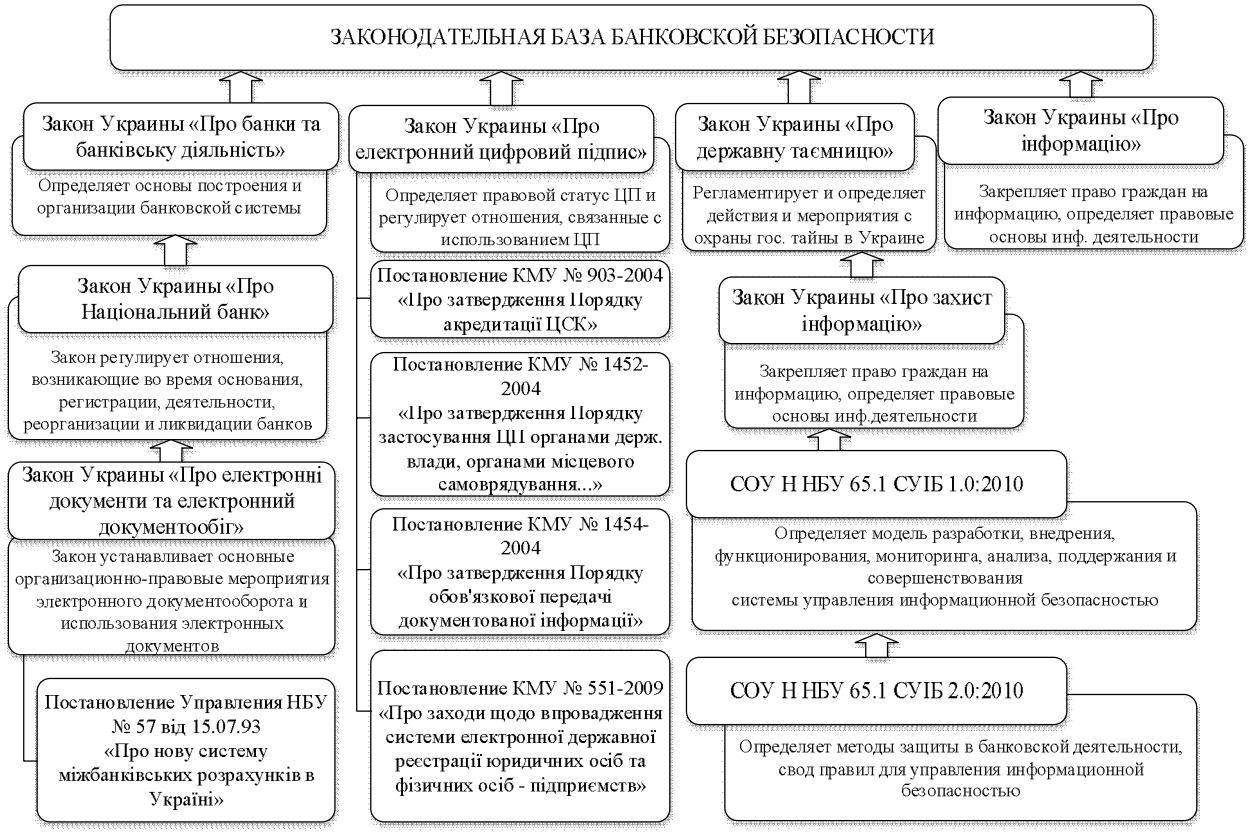

Рис. 1. Нормативная база деятельности АБС

Рис. 2. Признаковая классификация банковской информации

2. Уточнение и дополнение множества актуальных угроз безопасности банковской информации с триединой позиции обеспечения информационной безопасности, безопасности информации и кибербезопасности в банковском секторе, как основы для создания нового синергетического подхода в области обеспечения информационной безопасности АБС. Для анализа основных видов угроз безопасности банковской информации используем известную модель безопасности – триады CIA (confidentiality, integrity, availability) в трех сферах (профилях) безопасности: информационной безопасности, безопасности информации и кибернетической безопасности.

В данной модели под *информационной безопасностью* понимается процесс обеспечения конфиденциальности, целостности и доступности информации клиентами/клиентом банка на основе совокупности коллективного и индивидуального сознания. В рассматриваемой модели под *конфиденциальностью* понимается обеспечение доступа к информации только авторизованным пользователям,

под *целостностью* – обеспечение достоверности и полноты информации, и методов ее обработки для авторизованных пользователей, под *доступностью* – обеспечение доступа к информации и связанным с ней активам авторизованных пользователей по мере необходимости.

Безопасность информации – состояние защищенности данных, при котором обеспечиваются их конфиденциальность, доступность и целостность. *Безопасность информации* определяется отсутствием недопустимого риска, связанного с утечкой информации по техническим каналам, несанкционированными и непреднамеренными воздействиями на данные и (или) на другие ресурсы автоматизированной информационной системы, используемые в автоматизированной системе.

Кибербезопасность – набор средств, стратегий, принципов обеспечения безопасности, гарантий безопасности, подходов к управлению рисками, действий, профессиональной подготовки, страхования и технологий, которые используются для защиты киберсреды, ресурсов организаций и пользователей. Кибербезопасность подразумевает достижение и сохранение свойств безопасности у ресурсов организации или пользователей, направленных против соответствующих киберугроз. Кибербезопасность охватывает такие понятия, как защита персональной информации, а именно обнаружение, избежание или реакция на атаки. Стандарт ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity – дает четкое понимание связи термина cybersecurity (кибербезопасность) с сетевой безопасностью, прикладной безопасностью, Интернет-безопасностью и безопасностью критичных информационных инфраструктур (рис. 3).

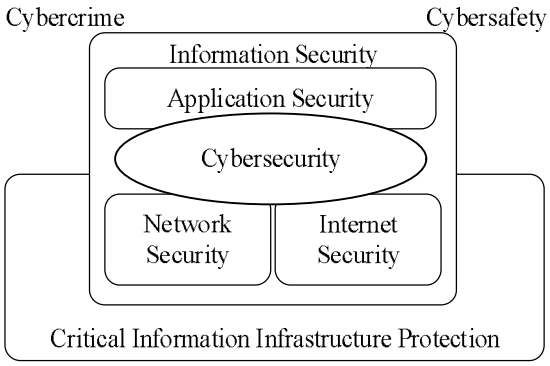

Рис. 3. Взаимосвязь между кибербезопасностью и другими доменами безопасности

Таким образом, известная модель триады CIA для комплексных АБС может быть представлена в виде, представленном на рис. 4.

Несмотря на широкое применение различных криптографических алгоритмов на различных уровнях защиты АБС подвержена различным угрозам, общая классификация угроз приведена в трех сферах безопасности на рис. 5.

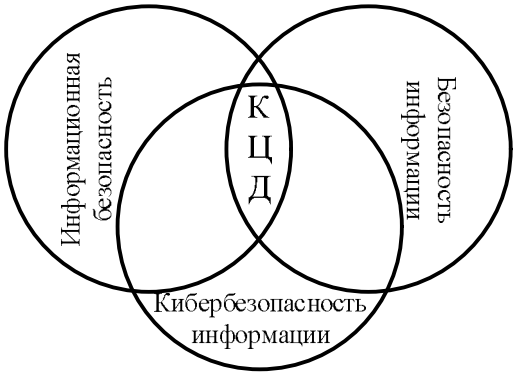

Рис. 4. Модель триады CIA для комплексных АБС

Угрозы банка – потенциально возможные или реальные действия злоумышленников или конкурентов, способные нанести банку материальный или моральный вред [9].

По происхождению источников угрозы: внутренние и внешние. Как первые, так и вторые по направленности и характеру воздействия на деятельность банков могут быть экономическими, физическими и интеллектуальными.

Экономические угрозы: коррупция, мошенничество, недобросовестная конкуренция, использование банками неэффективных технологий банковского производства. Реализация таких угроз ведет к причинению убытков банкам или упущения ними выгоды.

Физические угрозы: кражи, грабежи имущества и средств банков, поломки, вывод из строя оборудования банков, неэффективна его эксплуатация. В результате реализации таких угроз наносятся убытки банкам, связанные с потерей своей собственности и необходимостью нести дополнительные расходы на восстановление средств производства и других материальных средств.

Интеллектуальные угрозы: разглашение или неправомерное использование банковской информации, дискредитация банка на рынке банковских услуг, разного рода социальные конфликты вокруг банковских учреждений или в них самих. Последствия реализации таких угроз: убытки банков, ухудшение их имиджа, социальная или психологическая напряженность вокруг учреждения банков или в их коллективах.

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

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

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

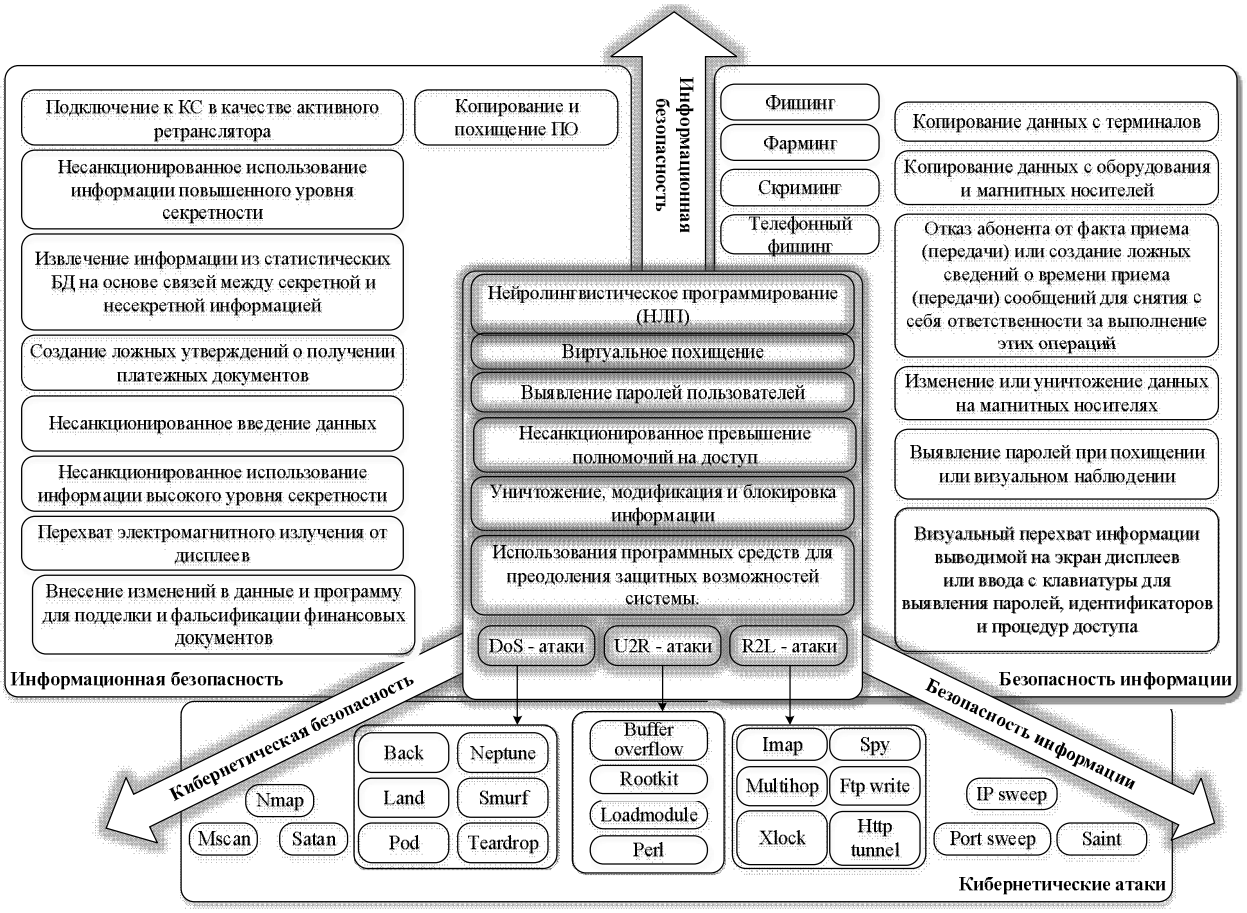

Рис. 5. Общая классификация угроз АБС

Эти особенности порождают такие проблемы:

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

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

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

– обеспечение исполнения документа (проблема взаимного недоверия между отправителем и получателем из-за их принадлежности к разным организациям и взаимной независимости) [3].

Результаты исследований компании “Arbor Networks” (июнь 2015 г.) атак на компьютерные сети приведены на рис. 6.

Проведенный анализ рис. 5, 6 показал, что с ростом киберпреступности и вычислительных возможностей злоумышленников наблюдается дальнейшее совершенствование известных кибератак и появление новых.

Основная классификация кибератак представлена на рис. 7.

Проведенный анализ рис. 5 – 7 подтверждает пропорциональный рост кибератак с эволюционным ростом вычислительной техники в последние десятилетия и компьютерной грамотностью злоумышленников.

Основой управления информационной безопасностью АБС является анализ рисков. Фактически риск представляет собой интегральную оценку того, насколько эффективно существующие средства защиты способны противостоять информационным атакам.

Обычно выделяют две основные группы методик расчёта рисков безопасности. Первая группа позволяет установить уровень риска путём оценки степени соответствия определённому набору требований по обеспечению информационной безопасности. Вторая группа методик оценки рисков информационной безопасности базируется на определении вероятности реализации атак, а также уровней их ущерба. В данном случае значение риска вычисляется отдельно для каждой атаки и в общем случае представляется как произведение вероятности проведения атаки на величину возможного ущерба от этой атаки. Значение ущерба определяется собственником информационного ресурса, а вероятность атаки вычисляется группой экспертов, проводящих процедуру аудита.

Для выявления аномалий (отклонений) от нормальной работы АБС используются методы выявления аномалий, общая классификация и основные характеристики представлены в табл. 1.

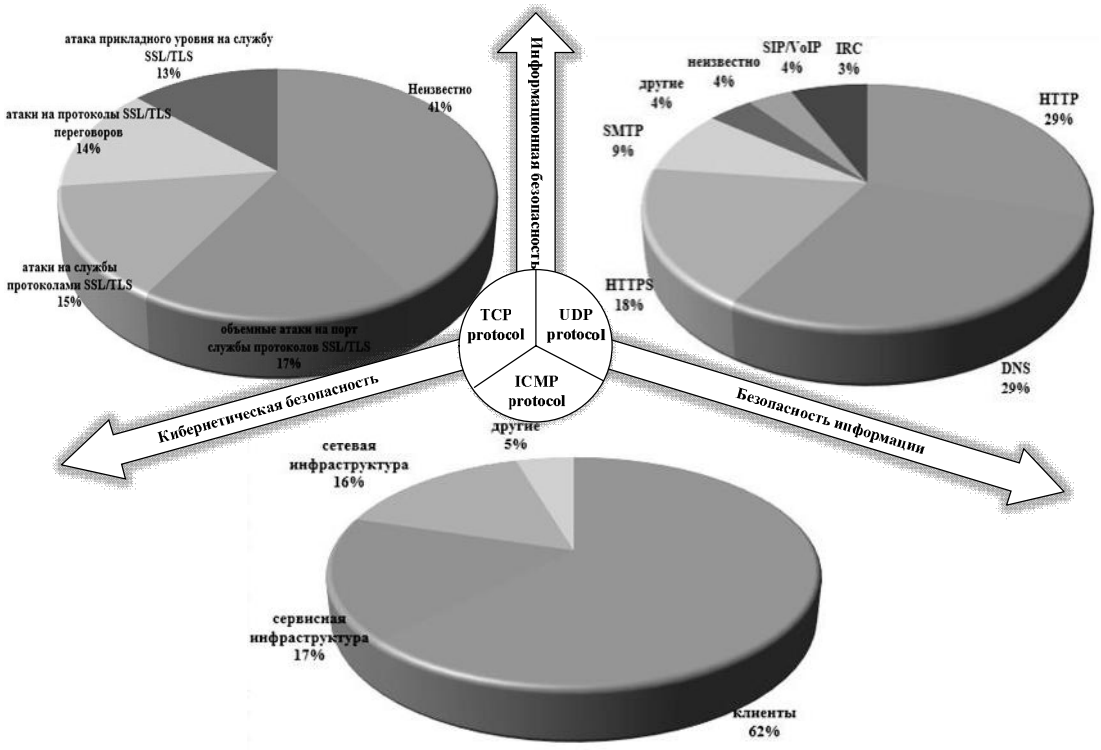

Рис. 6. Исследование угроз на протоколы IP-сетей

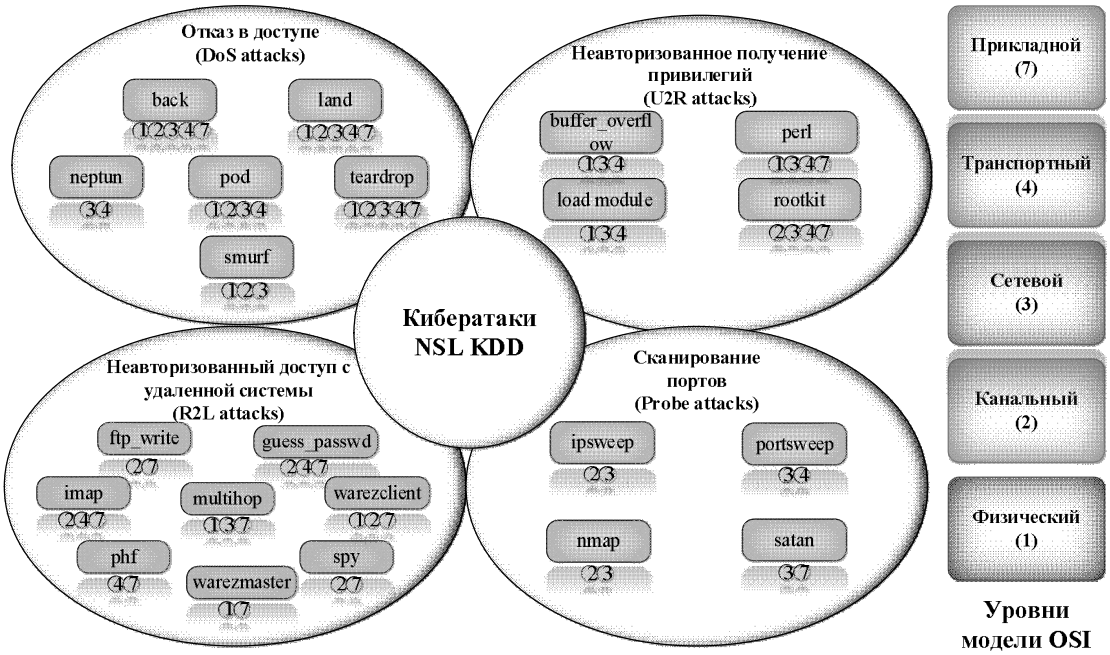

Рис. 7. Классификация кибератак

Таблица 1

Методы обнаружения аномалий и злоупотреблений

Метод	Входящие данные	Математический аппарат	Выходные данные	Эконом. эффективность	Вычислит. сложность
1	2	3	4	5	6
Анализ систем состояний (переходов)	Шаблоны нормального поведения системы, шаблоны атаки	Теория графов	Вероятностная оценка реализации атаки	качественная оценка	P
Графы сценариев атак	Модель защищаемой системы, свойство корректности	Теория графов	Вероятностная оценка реализации атаки	качественная оценка	NP
Нейронные сети	Траектории в некотором числовом пространстве признаков	Алгоритмы обучения нейронных сетей	Вероятностная оценка реализации атаки	качественная оценка	P

Окончание табл. 1

1	2	3	4	5	6
Иммунные сети	Шаблоны нормального поведения	Специфические иммунологические теории	Вероятностная оценка реализации атаки	качественная оценка	P
Support vector machines (SVM)	Векторы признаков нормального поведения системы, шаблоны атаки	Алгоритмы обучения и переобучения	Вероятностная оценка реализации атаки	качественная оценка	NP
Экспертные системы	Факты о событиях в системе и правила вывода	Сопоставление фактов и правил	Вероятностная оценка реализации атаки	качественная оценка	NP
Основанный на спецификациях	Спецификации атак	Анализ данных	Вероятностная оценка реализации атаки	качественная оценка	NP
Сигнатурный	События в системе, сигнатуры атак	Анализ данных	Вероятностная оценка реализации атаки, количественные показатели	количественная оценка	NP
Multivariate Adaptive Regression Splines (MARS)	Пространство признаков	Аппроксимация функций	Вероятностная оценка реализации атаки, количественные показатели	количественная оценка	P
Статистический анализ	Статистические данные о системе на некотором временном промежутке	Математическая статистика	Вероятностная оценка реализации атаки, количественные показатели	качественная и количественная оценка	P
Кластерный	Векторы свойств системы	Кластерный анализ	Вероятностная оценка реализации атаки, количественные показатели	качественная и количественная оценка	P
Поведенческая биометрия	Профиль нормального поведения системы	Сравнительный анализ	Вероятностная оценка реализации атаки	качественная и количественная оценка	P

Проведенный анализ систем выявления аномалий (СВА) показал, что основным недостатком подавляющего числа современных коммерческих СВА является относительно низкая эффективность обнаружения неизвестных классов кибератак [10 – 12]. При этом большинство современных СВА используют на базовом уровне ту или иную реализацию технологии сигнатурного метода обнаружения кибератак, что само по себе предусматривает организацию процесса защиты с запаздыванием. В [11] автор выделяет два класса методов обнаружения кибератак: методы выявления аномалий и методы выявления злоупотреблений. В обоих случаях входными данными для работы системы выступают сформированные на основе множества входных параметров шаблоны поведения – паттерны событий. Задача обнаружения кибератаки при такой постановке сводится к распознаванию шаблона поведения системы и фиксации факта ее начала. Но, как и в первом, так и во втором случаях множество входных параметров подлежит оцениванию на предмет его информативности.

В табл. 2 приведены результаты исследований некоторых методик оценки рисков. Учитывая разную природу угроз для выбранных профилей обеспечения банковской безопасности и в интересах получения в дальнейшем оценок величины риска эквивалентного денежному капиталу, непосредственно отображающего ее защищенность, предлагается использовать методики, основанные на *комплексном подходе* к оценке рисков, сочетающем количественные и качественные методы анализа, к таким относятся методики CRAMM и ФАИР, структурные схемы представлены на рис. 8, 9 (соответственно) [19 – 21].

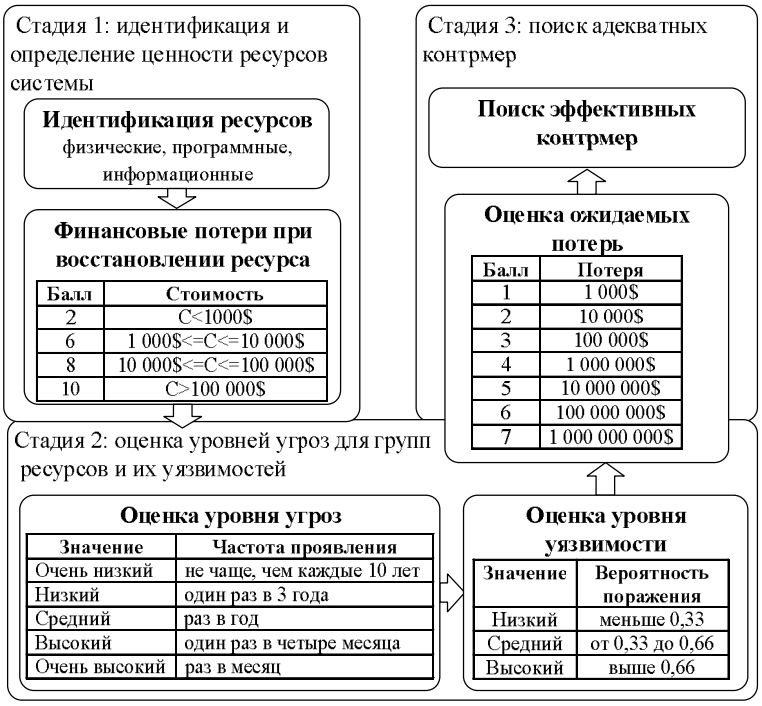

Рис. 8. Методика CRAMM – *комплексный подход* к оценке рисков

Таблица 2

Результаты исследований методик оценки рисков

Методика	Атрибуты							
	1	2	3	4	5	6	7	8
NIST	+			США	+	+	-	-
FAIR			+	США			+	+
EBIOS	+			Франция	+	+	+	-
MEHARI			+	Франция				
OCTAVE	+			США	+			
IT-GRUNDSHULTZ	+			Германия			+	
IRAM	+			Европа				+/-
RISK WATCH		+		США	+	+	+	+
FRAP	+			США				
CRAMM			+	Великобритания	+	+	+/-	+/-
MAGERIT	+	+		Испания	+	+		
Методика НБУ	+			Украина	+		-	+

Номера атрибутов: 1, 2, 3 – качественная, количественная и Комплексная оценки; 4 – страна происхождения; 5 – применение в банковских системах; 6 – программная реализация; 7 – эффективность контрмер; 8 – Простота понимания

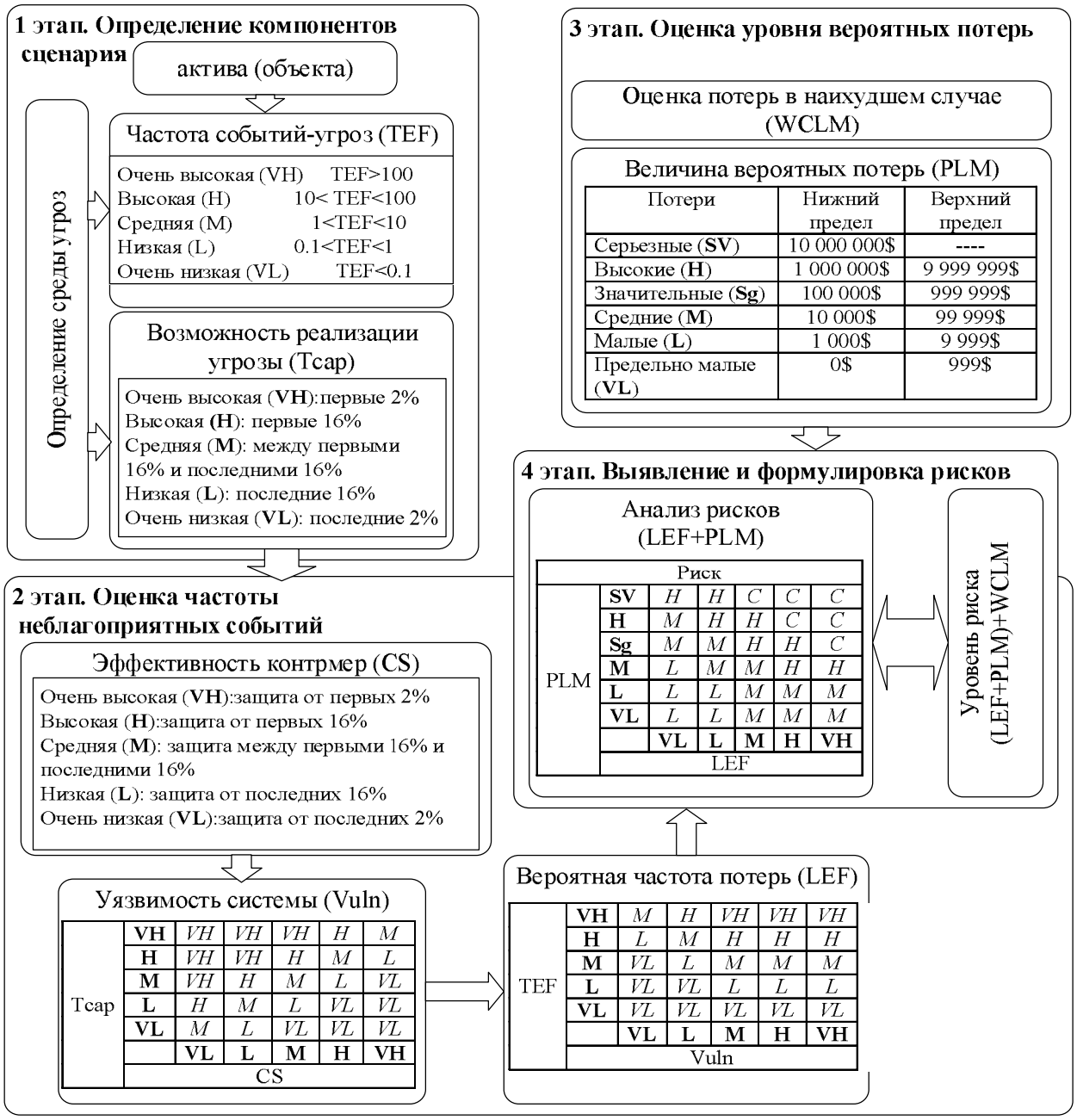

Рис. 9. Методика FAIR

Методики комплексного подхода оценки рисков, как правило, используют следующие стадии (этапы) [20, 21]: – на первой стадии анализируется все, что касается идентификации и определения ценности ресурсов системы: определение границ исследуемой системы: сведения о конфигурации системы, сведения об ответственных лицах за физические и программные ресурсы, определение количества пользователей системы, их привилегии.

Проводится *идентификация* ресурсов: физических, программных и информационных, содержащихся внутри границ системы. Строится модель информационной системы с позиции ИБ;

– на второй стадии идентифицируются угрозы и оцениваются уровни угроз для групп ресурсов и их уязвимостей, оцениваются зависимость пользовательских сервисов от определенных групп ресурсов и существующий уровень угроз и уязвимостей, вычисляются уровни рисков и анализируются результаты. В конце стадии заказчик получает идентифицированные и оцененные уровни рисков для своей системы;

– третья стадия исследования заключается в поиске адекватных контрмер – поиск варианта системы безопасности, наилучшим образом удовлетворяющей требованиям заказчика. На этой стадии генерирует несколько вариантов мер противодействия, адекватных выявленным рискам и их уровням.

Взаимосвязь между методами выявления атак и методиками оценки рисков представлена на рис. 10.

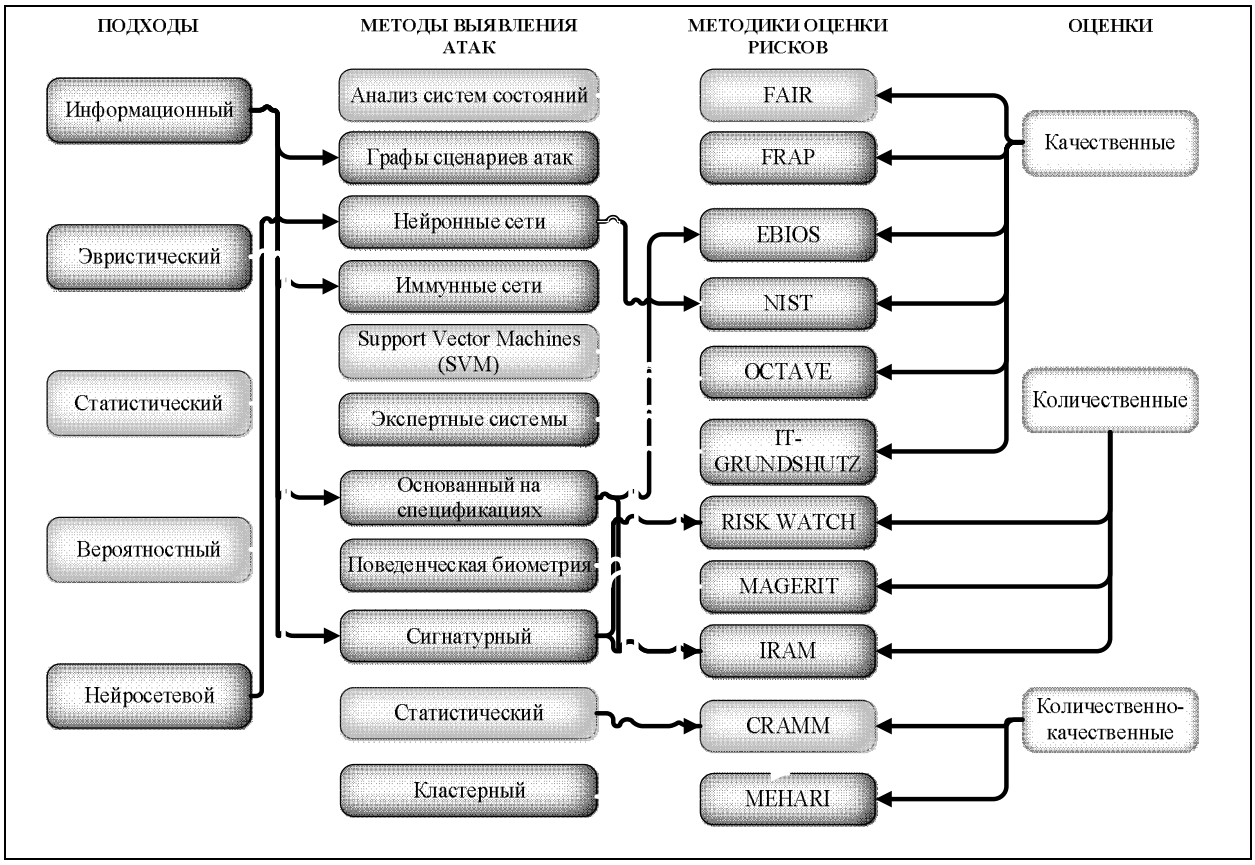

Рис. 10. Взаимосвязь между методами выявления атак и методиками оценки рисков

В контексте повышения эффективности функционирования СВА, несмотря на преимущества и недостатки каждого из направлений, они оба остаются актуальными, а потому и интенсивно развиваются. Альтернативой является дальнейшее развитие классификаторов кибератак, в основу которых положены деревья принятия решений. Последние, при условии правильности их построения, дают возможность получить достаточно достоверные результаты классификации и, что характерно, имеют относительно низкую вычислительную сложность. Важную роль в процессе классификации кибератак играют входные данные, которые выступают основой для построения классификаторов СВА коммуникационных систем. В качестве учебных и тестовых данных в представляемой работе, как и в [13], и других схожих работах, целесообразным видится применение общедоступной и широко известной базы данных KDD99. Такой подход позволят получать количественную характеристику кибератак.

Для получения качественной оценки кибератак и их дальнейшей классификации, предлагается применить известную признаковую классификацию. Такой подход позволит расширить признаковое пространство для описания неизвестных классов кибератак.

Таким образом, комплексирование двух известных подходов позволит объединить преимущества каждого из них, предоставляемые ними по отдельности, и при этом откроет возможности получения как количественных, так и качественных их характеристик для эффективной организации систем защиты.

3. Модель синергетического подхода оценки безопасности банковских систем. В процессе *анализа рисков* информационной безопасности могут использоваться специализированные программные комплексы, позволяющие автоматизировать процесс анализа исходных данных и расчёта значений рисков. Примерами таких комплексов являются “Гриф” и ’Кондор” (компании "Digital Security"), британский CRAMM (компания Insight Consulting, подразделение Siemens), американский RiskWatch (компания RiskWatch), а также “АванГард” (Института Системного Анализа РАН). Основой безопасной ИТ-инфраструктуры АБС является триада сервисов – конфиденциальность, целостность, доступность – Confidentiality, Integrity, Availability (CIA). Целью информационной безопасности является обеспечение трех наиболее важных сервисов безопасности, соответственно модели безопасности информации включают: конфиденциальность, целостность и доступность. На рис. 11 приведены известные модели анализа рисков информационной безопасности.

Проведенный анализ известных моделей анализа рисков информационной безопасности показал, что основу их составляет модель триады CIA, однако рассмотрение услуг безопасности обеспечивает сферу информационной безопасности и не позволяет комплексно оценить сферы безопасности информации и кибербезопасности АБС в режиме реального времени. Таким образом, исходя из потребности соблюдения правила триединой позиции к обеспечению безопасности банковской информации в рамках синергетического подхода при взаимодействии выбранных профилей безопасности и с целью повышения уровня ее защищенности оцениваемого величиной риска эквивалентного денежному капиталу, смысл предлагаемого подхода в самом общем виде может быть представлен в виде некоторой условной фигуры (рис. 12).

Следует отметить ключевую особенность, характерную только предлагаемому синергетическому подходу к обеспечению безопасности банковской информации: предлагаемый подход не является простым комплексированием сил и средств обеспечения безопасности, он так же не является суперпозицией их свойств. **Основная цель предлагаемого подхода – это возбуждение в системе обеспечения банковской информации управляемых эмерджентных свойств, направленных на получение синергетического эффекта, который достигается благодаря качественно новому подходу к обеспечению безопасности.**

Рис. 11. Известные модели анализа рисков информационной безопасности

Разработка такого подхода немыслима без разработки единой методологии построения системы обеспечения безопасности банковской информации, опирающейся на глубокую научную проработку проблемы путем ее всестороннего критического анализа и, на основе полученных выводов, синтеза

новых нетривиальных решений. Сегодня, как показал анализ, и в теории, и практике обеспечения безопасности банковской информации подобная методология отсутствует.

Учитывая разную природу угроз для выбранных профилей обеспечения банковской безопасности и в интересах получения в дальнейшем оценок величины риска эквивалентного денежному капиталу, непосредственно отображающего ее защищенность, так же предлагается введение синергетического показателя безопасности банковской информации в АБС (рис. 13). *Синергетический показатель безопасности банковской информации в АБС* – это синергетическая оценка эффективности комплексного применения сил и средств обеспечения безопасности банковской информации в условиях антагонистического противодействия системы банковской защиты случайным и целенаправленным угрозам безопасности.

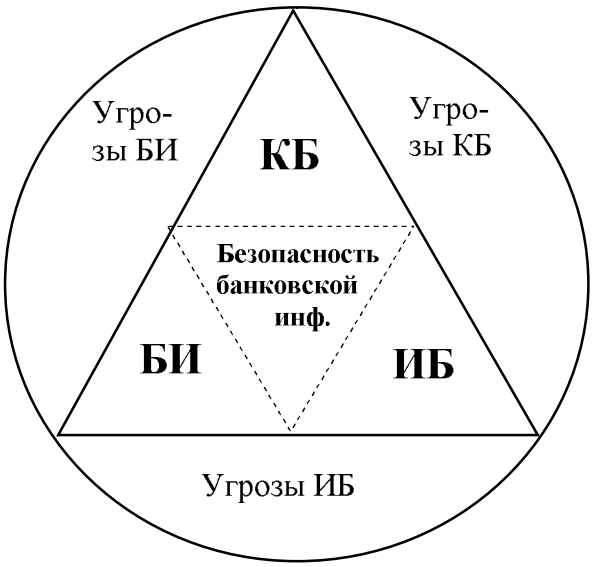

Рис. 12. Сущность синергетического подхода к обеспечению безопасности банковской информации

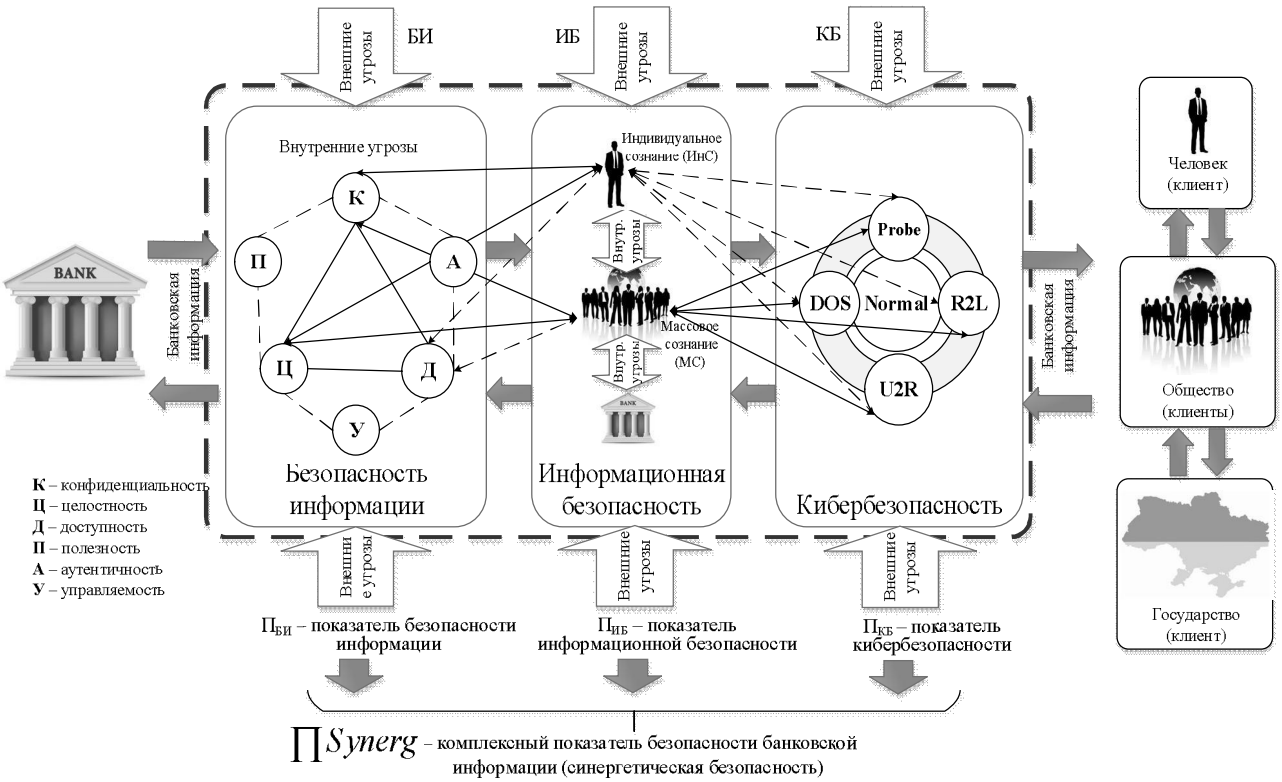

Рис. 13. Роль и место синергетического показателя безопасности банковской информации

Отсутствие на сегодня соответствующей методологии также обусловлено наличием противоречия, которое определяется тем, что с одной стороны, практика требует от теории изыскания новых подходов к обеспечению безопасности банковской информации в условиях роста количества угроз ее кибернетической и информационной безопасности, а также безопасности информации при одновременном росте их технологической сложности. С другой стороны, в теории отсутствует целостная научно обоснованная методология построения на практике системы обеспечения безопасности банковской информации в целом, что обусловлено несовершенством механизмов обеспечения ее информационной безопасности, безопасности информации и кибербезопасности в частности (рис. 14) [13 –18].

Исходя из сущности научной проблемы (рис. 14) в общем форматизированном виде она может быть поставлена следующим образом.

Рис. 14. Сущность научной проблемы

Пусть создаваемая система обеспечения банковской безопасности состоящая из M базовых профилей безопасности различной сложности и конфигурации, каждый из которых в свою очередь состоит из m элементов обеспечения безопасности в отдельно взятом профиле безопасности, направлена на получения синергетического эффекта – повышение уровня защищенности банковской информации путем максимизации количества ее эмерджентных свойств:

$$\text{Emerdg}=\max\{\Pi_{\text{Synerg}N}^{M}\},$$

где $\Pi_{\text{Synerg}N}^{M}$ – максимальное количество эмерджентных свойств системы обеспечения банковской безопасности в целом, достигаемое при возникновении синергетического эффекта в результате взаимодействия выбранных профилей безопасности, N – количество состояний системы обеспечения безопасности банковской информации или количество ее эмерджентных свойств $M \le N$.

При этом максимальное количество эмерджентных свойств системы обеспечения банковской безопасности в целом достижимо при выполнении условия $\Pi_{\text{Synerg}N}^{M} = \sum_{m=1}^{M} C_N^m$.

Необходимо так решить проблему повышения уровня защищенности банковской информации при заданных условиях, чтобы получить максимальное количество эмерджентных свойств при минимальных ресурсных затратах, направленных на возбуждение в системе синергетического эффекта.

Выводы

Таким образом, в статье в самом общем виде формализована сущность проблемы повышения уровня защищенности банковской информации на основании ее всеобъемлющего критического анализа и синтеза новых решений. В качестве нового прогрессивного решения существующей проблемы предложен принципиально новый синергетический подход, который до сегодняшнего времени не применялся в системах защиты банковской информации. Данное обстоятельство не только определяет актуальность темы исследования, но и определяет его научный приоритет.

Сформулирована гипотеза о том, что неотъемлемыми взаимодействующими профилями обеспечения банковской информации на современном этапе развития науки и техники, приводящими к возникновению синергетического эффекта, и, как следствие, проявлению эмерджентных свойств в системе защиты, должны быть ее информационная безопасность, безопасность информации и кибербезопасность.

На основе предложенного подхода впервые предложена синергетическая модель угроз безопасности банковской информации, раскрыты роль и место синергетического показателя безопасности банковской информации в современных системах банковской защиты автоматизированных банковских систем.

Полученные в статье результаты могут быть использованы для решения частных научных задач в рамках сформулированной проблемы. Перспективным направлением дальнейших исследований является проработка сущности и содержания профилей безопасности, входящих в состав создаваемой системы защиты банковской информации.

Список литературы

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

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

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

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

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

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

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

8. Старинський М.В. Щодо визначення поняття "банківська інформація" та виділення її видів [Електронний ресурс] / М.В. Старинський – Режим доступу: uabs.edu.ua/images/.../K.../Starinskii_s_015.pdf.

9. 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.

10. Ленков С.В. Методы и средства защиты информации: монография [в 2-х т.] Т. 2. Информационная безопасность / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко. – К.: Арий, 2008. – 344 с.

11. Сердюк В.А. Новое в защите от взлома корпоративных систем / В.А. Сердюк. – М.: Техносфера, 2007. – 360 с.

12. Мамарєв В.М. Аналіз сучасних методів виявлення атак на ресурси інформаційно-телекомунікаційних систем [Текст] / В.М. Мамарєв // Захист інформації. – 2011. – № 2. – С. 5-12.

13. Грищук Р.В. Метод скорочення розмірності потоку вхідних даних для мережних систем виявлення атак / Р.В. Грищук, В.М. Мамарєв // Сучасний захист інформації. – К. : ДУІКТ, 2012. – Спецвипуск. – С. 16-19.

14. Грищук Р.В. Атаки на інформацію в інформаційно-комунікаційних системах / Р.В. Грищук // Сучасна спеціальна техніка. – 2011. – №1(24). – С. 61-66.

15. Грищук Р.В. Синергія інформаційних та кібернетичних дій / Р.В. Грищук, Ю.І. Даник // Труди університету. – К. : НУОУ, 2014. – № 6 (127). – С. 132-143.

16. Грищук Р.В. Постановка наукового завдання з розроблення шаблонів потенційно небезпечних кібератак / Р.В. Грищук, В.В. Охрімчук // Безпека інформації – 2015. – Том 21. – № 3. – С. 276-282.

17. Колесников А.А. Синергетическое методы управления сложными системами: теория системного синтеза / А.А. Колесников. – М.: Едиторал УРСС, 2005. – 228 с.

18. Хакен Г. Синергетика. Иерархия неустойчивостей в самоорганизующихся системах и устройствах / Г. Хакен. – М.: Мир, 1985. – 419 с.

19. Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів національного банку України. [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua/laws/show/v0365500-11.

20. FAIR is the Factor Analysis of IT and Information Risk [Електронний ресурс]. – Режим доступу: http://www.risklens.com/what-is-fair.

21. Методика CRAMM [Електронний ресурс]. – Режим доступу: http://www.cramm.com/downloads/techpapers.htm.

Поступила в редколлегию 22.03.2016

Рецензент: д-р техн. наук, с.н.с. Р.В. Грищук, Житомирский военный институт имени С.П. Королева, Житомир.

СИНЕРГЕТИЧНИЙ ПІДХІД ДО ОЦІНКИ БЕЗПЕКИ БАНКІВСЬКИХ СИСТЕМ

С.П. Євсеєв

Розглядаються законодавчі акти в сфері захисту банківських транзакцій, структура банківської інформації. Проводиться аналіз основних джерел загроз в моделі CIA: конфіденційність, цілісність і доступність даних в автоматизованих банківських системах. В статті запропонована синергетична модель загроз безпеки банківської інформації, яка вперше з системних позицій дозволила розкрити сучасний стан досліджуваної проблеми. Показано і доведено, що на сучасному етапі розвитку науки і техніки, забезпечення безпеки банківської інформації повинно ґрунтуватися на принципово новому підході, який запропоновано називати синергетичним. Його впровадження дозволить отримати синергетичний ефект при взаємодії обраних профілів безпеки і, як наслідок, проявити якісно нові і невідомі до цього емерджентні властивості системи безпеки.

Ключові слова: *інформаційна безпека, безпека інформації, кібернетична безпека, загрози банківських даних.*

THE SYNERGETIC APPROACH FOR BANK SYSTEMS' SECURITY ASSESMENT

S.P. Yevseiev

Acts of legislation in the sphere of bank transaction security, bank information structure are considered. The analysis of the main sources of risks in the automated banking systems accordingly to CIA (confidentiality, integrity, availability of data) model is performed. The article proposes the synergetic model of bank information security threats, which allowed to show the current state of researched problem from system position. It is showed and proved that providing bank information security today must be based on conceptually new approach, which is proposed to be called synergetic. Its implementation will enable to get synergetic effect from interaction of selected safety profiles and, consequently, demonstrate a qualitatively new and previously unknown security emergent properties.

Keywords: *information security, security of information, cybersecurity, bank data threats.*