УДК 004.056:004.738.5

Евсеев С.П.

Харьковский национальный экономический университет им. С. Кузнеца, Харьков

СИНЕРГЕТИЧЕСКАЯ МОДЕЛЬ ОЦЕНКИ БЕЗОПАСНОСТИ БАНКОВСКОЙ ИНФОРМАЦИИ

В статье 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.

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

Переход от постиндустриального общества к обществу высоких технологий на ряду с позитивными переменами в информационном пространстве и увеличении новых форм использования компьютерных технологий трансформировал и негативные последствия применения открытых коммуникационных систем, обеспечив не только появление новых функций и услуг, но и эволюцию алгоритмов и сценариев их взлома. Особо остро это отмечается с развитием и практической реализацией киберугроз на инфраструктуры критического применения (ИКП) к которым относятся энергетика, транспорт, связь, экологически опасные производства, объекты оборонного комплекса, финансово-кредитная сфера и т.п. Особое место среди ИКП занимают АБС банковского сектора, обеспечивающего в последние годы не только экономическую, но и политическую стабильность государства.

Современные компьютерные технологии, предоставив новые инструментарии в жизнедеятельность и коммуникации банковского сектора качественно изменили и обострили проблему безопасности банковской информации. Возможности несанкционированного доступа к информации, возможности несанкционированного получения и, как правило, без существенных организационных и материальных затрат огромных массивов данных, составляющих в ряде случаев ценнейшие корпоративные ресурсы, возможности мгновенного разрушения информационных ресурсов, хранящихся или использующихся в компьютерной форме, предопределили перевод задач обеспечения безопасности информации из разряда вспомогательных, в число основных приоритетов и условий функционирования банковских систем [1 – 8, 16, 18, 19, 20]. В практическом плане задачи обеспечения безопасности требуют теоретической базы, программно-технических решений и механизмов обеспечения безопасности при коллективной обработке общих информационных ресурсов. Работы в этом направлении ведутся на протяжении более 30 лет, в том числе и по разработке принципов построения и теории защиты, а также соответствующих стандартов оценки ее прочности. Однако различного рода потери от несанкционированного доступа (НСД) к банковской информации продолжают расти, и могут привести к быстрому развитию системного кризиса

платежной системы Национального банка Украины (НБУ), нанести непоправимый ущерб собственникам и клиентам банковской системы НБУ и государству в целом.

Анализ последних исследований [1 – 13] и публикаций [14 – 20] 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. [2, 6 –8, 13,16, 19, 20]. Считается, что перечисленные модели являются инструментарием при разработке политик безопасности, определяющих множество требований, которые должны быть выполнены в конкретной реализации системы. Непрерывное развитие технических средств защиты информации (ТСЗИ), которые длительное время являлись базисом реализации политики информационной безопасности (ПИБ), ведет к эволюции алгоритмов реализации кибернападений, а возникновение новых систем защиты информации (СЗИ) сопровождается новыми сценариями реализации кибератак [3, 4]. Это обуславливает сложность теоретических моделей и алгоритмов киберзащиты.

В настоящее время наблюдается рост объема рынка СЗИ, что предопределило возможность реализации концепции восходящего проектирования с использованием типовых решений по средствам защиты, основой концепции является принятая ПИБ на основе модели политики безопасности (МПБ), обуславливающей определенные уязвимости в информационных процедурах (ИП) и обеспечивающая выполнение основных процедур как глобальной, так и локальной политик безопасности (ПБ). Любая МПБ обязана поддерживать глобальную ПБ, которая определяет требуемые параметры ИП, и может содействовать локальной ПБ, регламентирующей правила перехода ИП между смежными состояниями АБС ИКП. При этом к динамичным МПБ относятся модели с возможностью поддержки локальной ПБ, и обусловленных ограниченностью состояний ИП в АБС ИКП. Отсутствие такой поддержки свидетельствует о статичности МПБ. Базисом таких моделей является основная теорема безопасности (ОТБ), в соответствии с которой [2, 4,14 – 16, 19, 20] в начальный момент времени ТСЗИ обеспечивают защиту и выполняются все постулаты глобальной и локальной ПБ, при этом глобальная ПБ будет выполняться и в будущем, и, следовательно, уязвимости в ИП не заложены в модель ПБ, и могут быть выявлены только при осуществлении кибератаки или попытки НСД.

Синтез сложных систем СЗИ требует от разработчиков соблюдения баланса между ТСЗИ, организационными и законодательными мерами. Преимущество получил комплексный, системный подход к защите информации, основанный на рассмотрении широкого спектра разноплановых задач по защите информации, информационной безопасности и кибербезопасности, путем использования совокупности средств и методов и мероприятий, направленных на получение эмерджентных свойств СЗИ и формировании синергетического подхода к оценке полученных результатов. Целями такого моделирования является поиск оптимальных решений задач синтеза СЗИ, управления механизмами защиты, оценки эффективности использования средств и методов защиты и т.п. Модель с позиции математического моделирования представляет собой математическое и логическое описание компонентов и функций, отображающих наиболее существенные свойства моделируемого объекта или процесса [13, 16, 19, 20]. Моделирование системы заключается в построении некоторого математического аналога, адекватного с точностью до целей моделирования исследуемой системы, и выявления с помощью построенной модели необходимых свойств реальной системы. Объем и виды мероприятий, принимаемых организациями банковского сектора (БС) для защиты БИн зависит не только от желания и возможностей собственника, но

и определяется рядом обязательных требований регуляторов, в их числе – постановления и инструкции НБУ; различные международные и национальные стандарты.

Целью статьи является раскрытие сущности построения синергетической модели безопасности банковской информации (БИн) на основе методологии и синергетическом подходе к обеспечению безопасности БИн и оцениванию безопасности информационных технологий АБС 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.

Изложение основного материала.

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 информационных угроз с наилучшим качеством и минимально возможными затратами ресурсов. Наиболее эффективно задачи защиты информации решаются в рамках *упреждающей стратегии защиты*, когда на этапе проектирования оцениваются потенциально возможные угрозы и реализуются механизмы защиты от них. При этом в процессе проектирования систем ЗИ разработчик, не имея статистических данных о результатах функционирования создаваемой системы, вынужден принимать решение о составе комплекса средств ЗИ, находясь в условиях значительной неопределенности [2, 6, 8, 16, 19, 20].

Модели безопасности играют важную роль в процессах разработки и исследования защищенных компьютерных систем к которым относятся и АБС, так как обеспечивают системотехнический подход, включающий решение важнейших задач: выбора и обоснования базовых принципов архитектуры АБС, определяющих механизмы реализации средств и методов защиты информации, подтверждение свойств (защищенности) разрабатываемых систем путем формального доказательства соблюдения политики безопасности (требований, условий, критериев), составление формальной спецификации политики безопасности как важнейшей составной части организационного и документационного обеспечения разрабатываемых защищенных компьютерных систем. Построение моделей при проектировании или модернизации системы защиты информации в банках представляется естественным путем решения задач анализа и проектирования с минимальными затратами и высокой эффективностью. Так, на этапе анализа модель системы защиты информации используется для исследования каждой выполняемой функции (операции), чтобы выявить, например, к какой информации и к каким ресурсам должен иметь доступ каждый сотрудник при выполнении служебных обязанностей [2, 14 – 16, 19, 20].

Основным результатом формирования методологических основ обеспечения безопасности ИП, в соответствии с системным подходом [4, 6, 8, 10 – 14, 16, 19, 20] 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.

В работах [1 – 4, 6 – 11, 14 – 20] отмечается, что безопасность информации, в том числе и банковской, 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. Игнорирование методологии

системного анализа в отношении создания системы обеспечения банковской информации исходя из сложности, а иногда и из невозможности объективного подтверждения эффективности созданной системы из-за несовершенства нормативно-методического обеспечения информационной безопасности, прежде всего в области показателей и критериев [17, 16, 19, 20], так же создает препятствия на пути нахождения решения обозначенной проблемы.

Развитие теорий ИБ, БИ, КБз в настоящее время связаны с учетом новых обстоятельств, характерных для современного периода развития информатизации общества на основе высоких технологий. Во-первых, так как все большую актуальность приобретает не только защита информации, но и защита сообщества, личности и коммуникационных систем, в первую очередь, критического применения (КП) от разрушающего воздействия информации в киберпространстве, то формируется задача обеспечения безопасности, как органической совокупности задач защиты информации и защиты от информации.

Во-вторых, с самого начала регулярного использования автоматизированных технологий обработки информации актуальность задачи обеспечения требуемого качества информации возрастает, а сама задача усложняется. Следовательно, эволюция вычислительных технологий ведет к появлению эмерджентных свойств автоматизированных систем управления, а обеспечение безопасности невозможно без учета задач обеспечения качества информации.

В-третьих, решение задач защиты информации, задач защиты от информации и обеспечения качества информации обусловливает эффективность деятельности объектов. Возникает обобщенное понятие управления информацией, которое объединяет выше обозначенные понятия. В свою очередь, учет задач управления информацией необходим при формировании, поддержке и использовании концепции информационного обеспечения деятельности объектов.

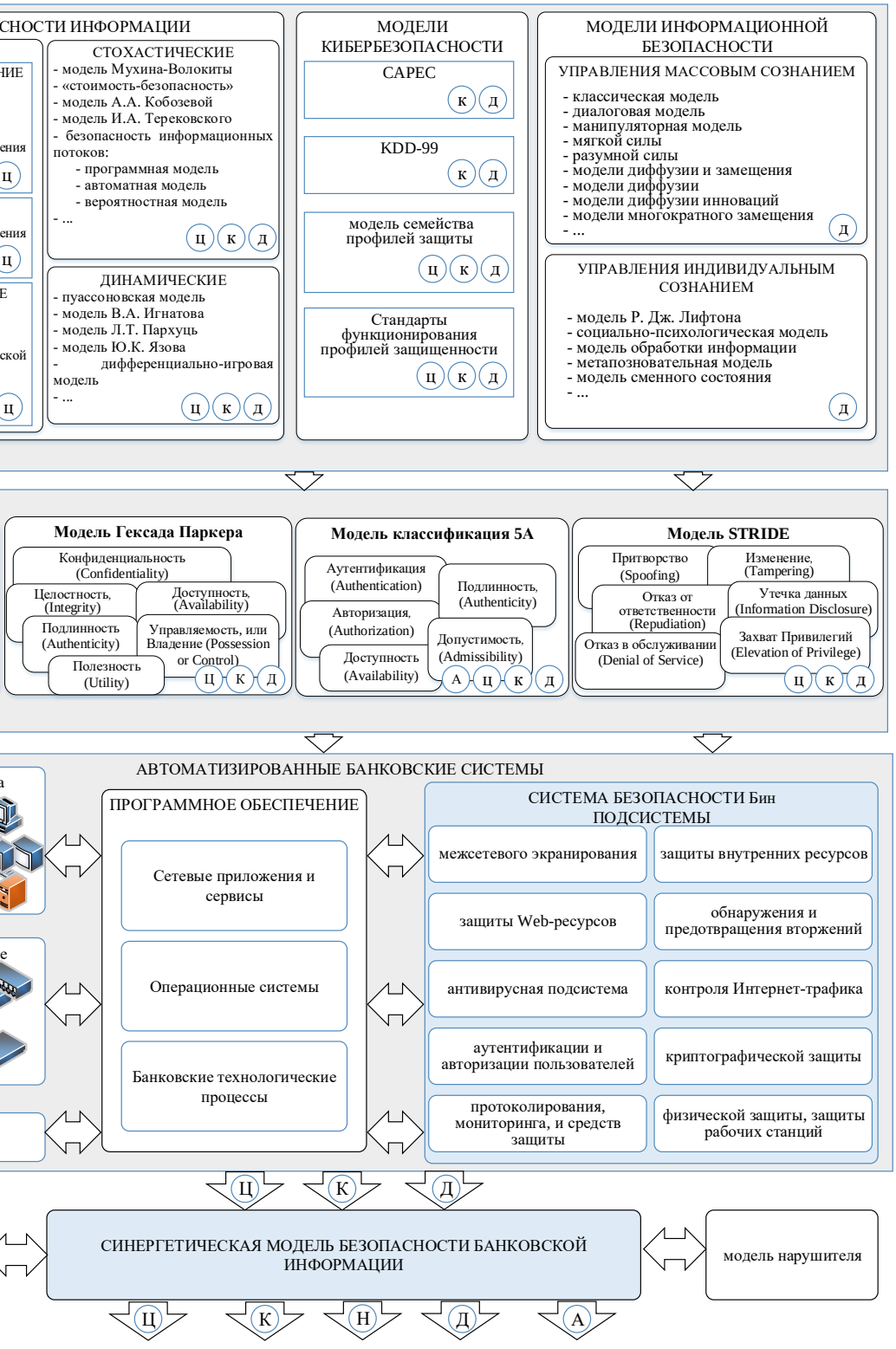
В-четвертых, серьезное внимание на новом этапе развития теории защиты информации должно быть уделено совершенствованию научно-методологического базиса и инструментальных средств, обеспечивающих решение любых возникающих задач на регулярной основе в органической связи с решением проблем информационной безопасности, информационных технологий, информатизации общества. Таким, образом, выше изложенное позволяет выделить следующие наиболее острые проблемы развития теории и практики информационной безопасности [22, 23, 25]:

• создание теоретических основ и формирование научно-методологического базиса, позволяющих адекватно описывать процессы в условиях значительной неопределенности и непредсказуемости проявления дестабилизирующих факторов (информационных угроз) при комплексированном синергетическом подходе к их оценке во всех составляющих понятия безопасности: БИ, ИБ, КБз;

• разработка научно-обоснованных нормативно-методических документов по обеспечению безопасности информации на базе исследования и классификации угроз информации и выработки стандартов требований к защите;

• стандартизация подходов к созданию систем защиты информации и рационализация схем и структур управления защитой на объектовом, региональном и государственном уровнях.

Решение спектра перечисленных задач имеет большое значение для реализации положений Стратегии национальной безопасности Украины и Доктрины безопасности банковской информации. 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 с целью уменьшения трудозатрат и повышения степени соответствия нормативных документов при проектировании систем (подсистем) ЗИ и планировании мер защиты на протяжении всего цикла использования ТСЗИ в АБС. На рис. 1 приведен обобщенный подход к построению синергетической модели безопасности БИн в АБС.



общенный подход формирования синергетической модели безопасности БИн

Анализ рис. 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.

На практике наибольшее распространение получили два подхода к обоснованию проекта подсистемы обеспечения безопасности [1 – 4, 25].

Первый из них основан на проверке соответствия уровня защищенности ИС требованиям одного из стандартов в области информационной безопасности. Это может быть класс защищенности в соответствии с требованиями профиля защиты разработанных в соответствии со стандартом ISO-15408, или какой-либо другой набор требований. Тогда критерий достижения цели в области безопасности – это выполнение заданного набора требований. Критерий эффективности – минимальные суммарные затраты на выполнение поставленных функциональных требований: $\Sigma c_i \rightarrow min$, где c_i – затраты на i-е средство защиты. Основной недостаток данного подхода заключается в том, что в случае, когда требуемый уровень защищенности жестко не задан (например, через законодательные требования) определить “наиболее эффективный” уровень защищенности АБС достаточно сложно.

Второй подход к построению системы обеспечения безопасности связан с оценкой и управлением рисками на основе принципа “разумной достаточности”. Однако, проведенный анализ показал, что соблюдение баланса между затратами на защиту и получаемым эффектом, в т.ч. и экономическим, заключающимся в снижении потерь от нарушений безопасности носит субъективный характер, и напрямую зависит от оценки риска угроз на элементы АБС.

На основе анализа [1, 3, 4, 10, 16, 18 – 24, 25] введем определения безопасности информации, 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.

Конфиденциальность (confidentiality) – состояние БИн, при котором информация не может быть получена неавторизованным пользователем и/или процессом.

Конфиденциальность системы (system confidentiality) – свойство системы обеспечить защиту БИн при передаче от пассивных атак;

Целостность (integrity) – состояние БИн, при котором информация не может быть модифицирована неавторизованным пользователем и/или процессом.

Целостность системы (system integrity) – свойство системы обеспечить защиту БИн при хранении, а также возможность модификации БИн только авторизованным пользователем и/или процессом.

Доступность (availability) – состояние БИн, при котором отсутствуют препятствия доступа к информации и закономерному ее использованию авторизованным пользователем и/или процессом.

Доступность системы (system availability) – свойство системы, которое заключается в том, что авторизованный пользователь и/или процесс, обладающий соответствующими полномочиями, может использовать ресурс в соответствии с правилами, установленными ПБ, не дожидаясь дольше заданного (малого) промежутка времени, в виде, необходимом

пользователю, в месте, необходимом пользователю, и в то время, когда она ему необходима.

Аутентичность (authenticity) – состояние БИн, при котором информация обеспечивает подтверждение подлинности источника (авторизованного пользователя и/или процесса) информации.

Аутентичность системы (system authenticity) – свойство системы, которое заключается в том, что авторизованный пользователь и/или процесс, обладающий соответствующими полномочиями, может подтвердить подлинность источника информации.

Непрерывность бизнес-процессов (business continuity) – свойство системы, которое заключается в обеспечении бесперебойной работы внутренних и внешних приложений, рабочим нагрузкам и службам работать без перерыва во время запланированного простоя и незапланированных сбоев, а также обеспечить резервное копирование и хранение критических бизнес-данных и возможность их восстановления в течение приемлемого периода времени в случае неожиданного инцидента или аварии.

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.

Объектами угроз ИБ 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 безопасности банковской информации 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*.

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.2.

Рис. 2. Структурная схема концептуальной синергетической модели безопасности БИн

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 [1, 23], 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 $A^{ABS} = \left\| a_{ij}^{ABS} \right\|$. $\{I_A\}$ – 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:

$$IO^R = \left\| IO_{il}^R \right\| \quad (2)$$

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:

$$GR^{ABS} = \left\{\left\{DF^{ABS}\right\}, \{T_{risk}\}, \{T_P\}, \{T_U\}, \{VH\}\right\}. \quad (3)$$

Множество источников угроз безопасности АБС представлено кортежем $DF^{ABS} = \left\{V^{NS}, V^{AS}\right\}$, 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. 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 [28].

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

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

Каждый элемент из множества угроз $DF_i \in \left\{DF^{ABS}\right\}$, 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$\}=\{\alpha_{r1},\alpha_{r2}\}$.

Оценка вероятности реализации i-й угрозы к j-му активу определим на основе предложений авторов в работах [5, 26]: для учета связей между источниками угроз и элементами АБС задается матрица $A^{DF} = \left\| a_{ij}^{DF} \right\|$, 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:

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

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 $V^{AS} = \left\{V^{ASIB}, V^{ASBI}, V^{ASKBr}\right\}$, 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 [26], 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 в соответствии с [27] 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 [27].

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

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

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, 7] в которых определены категории [7] и действия злоумышленников [8]:

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

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.

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 $O_l \in \left\{ O^{ABS} \right\}$, а иначе $a_{ij}^{DF} = 0$.

Для описания модели оценки защищенности АБС воспользуемся предложениями автора в работе [18] и методологией оценивания безопасности ИТ АБС [23], формально предлагается следующая модель:

$$G_{OZ}^{ABS} = \left\{ \left\{ I_A \right\}, \left\{ O^{ABS} \right\}, \left\{ DF^{ABS} \right\}, \left\{ RR^{ABS} \right\}, \left\{ SZ^{ABS} \right\}, \left\{ ROZ^{ABS} \right\}, \left\{ UZ_r^{ABS} \right\} \right\}, \quad (11)$$

где

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

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

$$\left\| A^{DF} \right\| = \begin{cases} 1, \text{если для } j\text{-го информационного актива существует } i \text{ угроза} \\ 0, \text{если для } j\text{-го информационного актива не существует } i \text{ угроза} \end{cases}. \quad (12)$$

Каждый механизм защиты БИн в АБС $SZ_i \in \left\{ SZ^{ABS} \right\}$ характеризуется вектором $SZ_i = \left(T_{SZ}, T_V, C_{SZ} \right)$, где T_{SZ} – тип средства защиты, T_V – время внедрения, C_{SZ} – стоимость.

Для описания связи между угрозами и ТСЗИ используется матрица $A^{DFSZ} = \left\| a_{ij}^{DFSZ} \right\|$, где a_{ij}^{DFSZ} – отображает наличие связи между *i*-й угрозой нарушения безопасности $DF_i \in \left\{ DF^{ABS} \right\}$ и *j*-м ТСЗИ $SZ_i \in \left\{ SZ^{ABS} \right\}$. В модели предлагается использовать следующие типы связей:

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

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

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

$$\left\| a_{ij}^{DFSZ} \right\| = \begin{cases} MZ, \text{если } i \text{ угроза рззакрываеся } j\text{-м ТСЗИ} \\ NMZ, \text{если } i \text{ угроза рззакрываеся } j\text{-м ТСЗИ} \end{cases}. \quad (13)$$

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 $\left\{ RR^{ABS} \right\}$ включает в себя требования к обеспечению безопасности БИн – $\left\{ R_{BBI} \right\}$, определенных в международных и национальных стандартах, систематизация источников представлена в работе [23], множества оценок степени выполнения требований безопасности – $\left\{ OV_{BBI} \right\}$, итоговый

уровень соответствия безопасности БИн требованиям из множества $\{R_{BBI}\}$ – $\{IU_{BBI}\}$ и определяется:

$$\{RR^{ABS}\} = \{R_{BBI}\} \text{Y} \{OV_{BBI}\} \text{Y} \{IU_{BBI}\}. \quad (14)$$

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:

$$OPZ^{ABS} = \sum_{i=1}^{k} OPZ_i \ , \quad (15)$$

где k – количество частных показателей безопасности, OPZ_i – частный показатель принимающий значения из множества $\{0,1\}$, принимающий значения в соответствии с правилами [18]:

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 $UZ^{ABS} = \{\text{низкий}, \text{средний}, \text{высокиий}\}$ в соответствии с правилом:

$$UZ^{ABS} = \begin{cases} \text{высокий}, \text{если } OPZ^{ABS} = 3; \\ \text{срредний если } 1 \le OPZ^{ABS} \le 3; \\ \text{низкий}, \text{если } OPZ^{ABS} = 0. \end{cases} \quad (16)$$

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:

$$SV^{AS} = \{SV^{ASIB}\} \text{I} \ \{SV^{ASBI}\} \text{I} \ \{SV^{ASKBr}\}; \quad (17)$$

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:

$$SZ^{ABS} \le V_{BIn}^{ABS}, \ SV^{AS} \le V_{BIn}^{ABS}. \quad (18)$$

Предположим, вероятности определяются по формулам:

$$p_{Z_j} = \frac{q_Z \times SZ^{ABS}}{q_Z \times SZ^{ABS} + q_V \times SV^{AS}}, \quad (19)$$

$$p_{V_j} = \frac{q_V \times SV^{AS}}{q_V \times SV^{AS} + q_Z \times SZ^{ABS}}, \quad (20)$$

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:

$$SZ^{ABS} = V_{BIn}^{ABS} \times \frac{\sqrt{5}-1}{2}. \quad (21)$$

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

Выводы и перспективы дальнейших исследований.

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. Предложенная модель инфраструктуры АБС позволяет связать элементы иерархической структуры с коммуникационными связями с информационными активами БИн, циркулирующей и обрабатываемой в элементах АБС, и на основании синергетической модели угроз возможные деструктивные последствия. Предложенная 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. Предложенные модели могут быть автоматизованы и оформлены в виде программного пакета или системы поддержки принятия решений по аудиту и оценке безопасности БИн ОБС на основе синергетической модели. Перспективным направлением дальнейших исследований является разработка классификатора метрик БИ, ИБ и КБз для оптимизации программной реализации предложенных решений.

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. Хмелевський Р. М. Дослідження оцінки загроз інформаційній безпеці об’єктів інформаційної діяльності // Сучасний захист інформації. – №4, 2016. – С. 65 – 70.

6. Жуков В. Г. Методика построения модели безопасности автоматизированных систем / В. Г. Жуков, М. Н. Жукова, В. В. Золотарев, И. В. Ковалев // Программные продукты и системы. – 2012. – № 2. – С. 70 – 74.

7. 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. Жукова М.Н. Модель оценки защищенности автоматизированной системы с применением аппарата нечеткой логики // М.Н. Жукова, Н.А. Коромыслов. / Известия ЮФУ. Технические науки. – 2013. – № 12 (149). – С. 63 – 69.

9. Мельник С. В. Концептуальні основи організації криптографічного захисту інформації / С. В. Мельник // Наукові записки Українського науково-дослідного інституту зв'язку. – 2015. – № 6. – С. 19 – 26. – Режим доступу: http://nbuv.gov.ua/UJRN/Nzundiz_2015_6_5

10. Потий А. Эталонная модель системы процессов защиты информации Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні : науково-технічний збірник. – 2006. – Вип. 1(12). – С. 17 – 30.

11. Потій О. Методика оцінки відповідності поточної зрілості цільовим орієнтирам / О. Потій, А. Лєншин // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні : науково-технічний збірник. – 2006. – Вип. 1(12). – С. 31 – 43.

12. Даурцев А. В. Разработка математических моделей оценки показателей эффективности программных систем защиты информации в автоматизированных системах электронного документооборота. – [Электронный ресурс]. – Режим доступа к ресурсу: http://cyberleninka.ru/article/n/razrabotka-matematicheskih-modeley-otsenki-pokazateley-effektivnosti-programmnyh-sistem-zaschity-informatsii-v-avtomatizirovannyh.

13. Карпов В. В. Вероятностная модель оценки защищенности средств вычислительной техники с аппаратно-программным комплексом защиты информации от несанкционированного доступа / В. В. Карпов // Программные продукты и системы. – 2003. – № 1. – С. 31 – 36.

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

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

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

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

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

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

20. Грайворонський М. В. Безпека інформаційно-комунікаційних систем / М. В. Грайворонський, О. М. Новіков. – К. : Видавнича група BHV, 2009. – 608 с.

21. Скрипник Л. В. Методологические аспекты германского стандарта "Руководство по базовому уровню защиты информационных технологий / Л. В. Скрипник, М. Ф. Бондаренко, И. Д. Горбенко, А. А. Ткач, А. В. Потий. – [Электронный ресурс]. – Режим доступа: http://www.bezpeka.com/ru/lib/spec/infsys.html.

22. Азамов О.В. Информационная безопасность /О.В. Азамов, К.Ю. Будылин, Е.Г. Бунев, С.А. Сакун, Д. Н. Шакин/ Вестник Российской Академии естественных наук, 2009. вып. № 3. – С. 35 – 45.

23. 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.

24. ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity [Электронный ресурс]. – Режим доступа к ресурсу: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=44375

25. Нестеров С.А. Анализ и управление рисками в сфере информационной безопасности/ Санкт-Петербург, 2007. – 47 с.

26. 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.

27.РС БС ИББС – 2.2-2009. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности – [Электронный ресурс]. – Режим доступа к ресурсу: www.cbr.ru/credit/gubzi_docs/st22_09.pdf.

28. 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.

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

Надійшла до редколегії