Известия Высших Технических Учебных
Заведений Азербайджана
Том 19, № 2 (2017), 77-86
УДК 621.391

Анализ методик оценки рисков нарушения безопасности банковской информации

Информатика и автоматика

Евсеев С.П., Сочнева А.С., Король О.Г., Абдуллаев В.Г.
Харьковский национальный экономический университет им. С. Кузнеца
Азербайджанский государственный университет нефти и промышленности
E-mail: evseev_serg@inbox.ru

Рассматриваются основные функции системы управления информационной безопасности (СУИБ), структура банковской информации. Проводится анализ основных источников угроз в модели CIA: конфиденциальность, целостность и доступность данных, безопасность информации, кибербезопасность. Анализируются методы выявления аномалий и методики оценки рисков нарушения безопасности банковской информации для формирования модели комплексного подхода оценки безопасности банковских систем.

Ключевые слова: безопасность информации, кибернетическая безопасность, угрозы банковских данных, автоматизированные банковские системы, модель CIA.

Введение

Важное значение в обеспечении безопасности государства, и особенно экономической ее составляющей, является 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 государства является нарушение ее финансово-банковской системы. Таким образом, решение вопросов обеспечения безопасности транзакций в АБС остается актуальной и на сегодняшний день.

Постановка задачи

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]. 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 аутенти-

фикации и контроля действий как внутренних пользователей, так и клиентов. 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 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 [7]. 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.

Целью работы является анализ основных функций СУИБ банковских транзакций, структуры банковской информации, проведение оценки основных источников угроз в модели CIA: конфиденциальность, целостность и доступность данных, разработка модели синергетического подхода оценки безопасности банковских систем.

Решение задачи

В соответствии со стандартом СОУ Н НБУ 65.1 СУИБ 1.0: 2010 руководству коммерческих банков предлагается процессный подход к управлению информационной безопасностью, поощряет его пользователей делать упор на важности [8]:

– понимания требований информационной безопасности организации и необходимости разработки политики и целей информационной безопасности;

– осуществления безопасности и обеспечения их функционирования для управле-

ния угрозами информационной безопасности организации в контексте общих бизнес-угроз банка;

– мониторинга и просмотра производительности и эффективности СУИБ (система управления информационной безопасности);

– постоянном совершенствовании, основанном на объективном измерении. Стандарт принимает модель “Планируй-Выполняй-Проверяй-Действуй” (“Plan-Do-Check-Act”), в дальнейшем ПВПД (PDCA), которую применяют для структуризации всех процессов СУИБ. СУИБ обеспечивает выбор адекватных и взаимосвязанных мер безопасности, которые защищают информационные ресурсы СУИБ и гарантируют конфиденциальность заинтересованным сторонам [8]. Деятельность АБС обеспечивается и регулируется на основе законодательных актов и рекомендаций Национального банка государства. Проведенный анализ законодательной базы показал, что для обеспечения защиты информации в АСБ используются системы управления информационной безопасностью (СУИБ), обеспечивающие контроль функционирования комплексных систем защиты информации. Принятие модели ПВПД (PDCA) отображает принципы, установленные Руководством ОЕСР, регулирующие безопасность информационных систем и сетей. Этот стандарт предоставляет надежную модель для внедрения принципов этой установки, влияющих на оценку рисков, проектирование и внедрение безопасности, управление безопасностью и повторную ее оценку.

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.

Проведенный анализ классификации банковской информации показал, что в подсистемах АБС Банка циркулирует информация различных уровней конфиденциальности (секретности), содержащая сведения ограниченного распространения (служебная коммерческая, банковская информация, персональные данные) и открытые сведения. В документообороте АБС Банка 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.

Таким образом, в самом общем виде *банковскую информацию* можно определить, как информацию, возникающую в результате банковской деятельности. Это, прежде всего сведения, характеризующие сам банк, его финансовое положение, надёжность, выполнение требований законодательства и т.п. Такую информацию можно почерпнуть из устава банка, его лицензий, бухгалтерских балансов, отчетов о прибыли и убытках и других источников.

Кроме того, банковская информация – это сведения о конкретных операциях банка. Такая информация характеризует не только банк, но и тех лиц, с которыми банк вступает в правоотношения. Анализируя эту информацию, можно многое узнать о клиентах банка и их деятельности. В этом смысле наиболее ценными являются сведения о наличии счетов или вкладов и об операциях по ним, об имуществе, находящемся на хранении в банке, и т.п.

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 *конфиденциальность*ю 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.1).

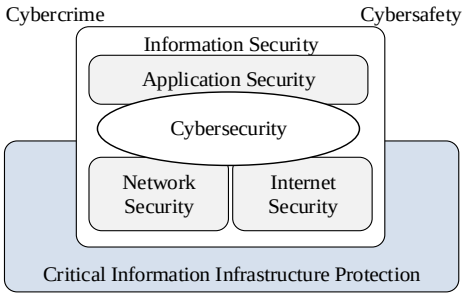

Рис.1. Взаимосвязь между кибербезопасностью и другими доменами безопасности

Таким образом, известная модель триады CIA для комплексных АБС может быть представлена в виде, указанном на рис.2.

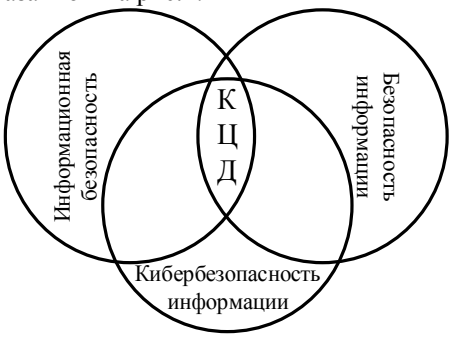

Рис. 2. Модель триады CIA для комплексных АБС

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

Угрозы банка – потенциально возможные или реальные действия злоумышленников или конкурентов, способные нанести банку материального или морального вреда [8].

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 упущению ими выгоды.

Физические угрозы: кражи, грабежи имущества и средств банков, поломки, вывод из строя оборудования банков, неэффективная 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 непосредственно через канал связи.

Эти особенности порождают следующие проблемы [3]:

– 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).

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 таблице.

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 работе [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 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 целесообразным видится применение общедоступной и широко известной базы данных KDD99 [13].

Таблица. Методы обнаружения аномалий и злоупотреблений

Метод	Входящие данные	Математический аппарат	Выходные данные	Эконом. эффективность	Вычислит. сложность
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
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, количественная оценка	P
Кластерный	Векторы свойств системы	Кластерный анализ	Вероятностная оценка реализации атаки, количественные показатели	качественная, качественная оценка	P
Поведенческая биометрия	Профиль нормального поведения системы	Сравнительный анализ	Вероятностная оценка реализации атаки	качественная, качественная оценка	P

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. Структурная схема СВА, основанная на комплексировании двух известных подходов качественного и количественного, приведена на рис.3.

Рис. 3. Структурная схема СВА на основе комплексированного подхода

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

Заключение

Проведенные исследования показали, что развитие вычислительных ресурсов позволили расширить спектр банковских услуг на основе использования интернет-ресурсов. Одной из существенных проблем при проектировании и эксплуатации систем защиты банковской информации является игнорирование методологии системного анализа в отношении средств и инструментов для их защиты Задача защиты банковской информации, как правило, включает решение частных задач по обеспечению надежной и безопасной работы АБС, безопасного доступа сотрудников и клиентов к банковской системе в территориально распределенной сети, доступа сотрудников к внешним информационным сетям (интернет-ресурсам), защиту банкоматов и терминалов, возможности контроля всех процессов в системе и своевременного обнаружения любых нарушений.

Прогресс в технике преступлений идет не менее быстрыми темпами, чем развитие банковских технологий, рост кибератак пропорционален эволюционному росту вычислительной техники в последние десятилетия и компьютерной грамотности злоумышленников. Проведенный анализ систем выявления аномалий (СВА) показал, что основным недостатком подавляющего числа современных коммерческих СВА является относительно низкая эффективность обнаружения неизвестных классов кибератак. С целью повышения эффективности функционирования СВА и получения как количественных, так и качественных характеристик кибератак, в данной работе предлагается комплексирование двух современных подходов: усовершенствование методов классификации кибератак на базе парадигмы искусственного интеллекта и на их основе алгоритмов классификации.

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. Перспективным направлением дальнейших исследований является разработка методологии комплексирования известных классификаторов, что позволит получить новый метод выявления кибератак на ресурсы коммуникационных систем.

Литература

1. Химка С.С. Разработка моделей и методов для создания системы информационной безопасности корпоративной сети предприятия с учетом различных критериев. − http://masters.donntu.org/ 2009/fvti/khimka/diss/index.html.

2. Украинский ресурс по безопасности. − http://kiev-security.org.ua.

3. Слободенюк Д. Банковские технологии, средства защиты информации в банковских системах. − http://www.arinteg.ru/about/publications/press/sredstva-zashchity-informatsii-vbankovskikh-sistemakh-131107.html. – 2013.

4. Симаков М.Н. V Съезд директоров по информационной безопасност. – М., 2012. 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. − 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. − http://www.thailawforum.com/articles/internet-banking-thailand.html.

7. Ярочкин, В. И. Информационная безопасность. // Учебник 2-е изд. – М.: Гаудеамус, 2004. – 544 с.

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

9. Старинський М. В. Щодо визначення поняття “банківська інформація” та виділення її видів. / uabs.edu.ua/images/.../K.../Starinskii_s_015.pdf.

10. Ленков, С. В. Методы и средства защиты информации. // Монография Информационная безопасность. – К. : Арий, 2008. − Т. 2. – 344 с.

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

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

13. KDD Cup 1999 Data. − http://cseweb.ucsd.edu/~elkan/clresults.html.

Xülasə

Yevseyev S.P., Soçneva A.S., Korol O.Q., Abdullayev V.Q.

Bank məlumatı təhlükəsizliyinin pozulması risklərinin qiymətləndirilməsi üsullarının təhlili

İnformasiya təhlükəsizliyinin idarə olunması sistemi (İTİS), bank məlumatının strukturu nəzərdən keçirilir. CİA modelində əsas təhdid mənbələrinin təhlili aparılır: verilənlərin məxfiliyi, vahidliyi və əlçatanlığı, məlumatın təhlükəsizliyi, kibertəhlükəsizlik. Qeyri-normallıqların müəyyən olunması üsulları və bank sistemlərinin təhlükəsizliyinin qiymətləndirilməsinin kompleks yanaşması modelinin formalaşdırılması üçün bank məlumatı təhlükəsizliyinin pozulması risklərinin qiymətləndirilməsi metodikası təhlil olunur.

Açar sözlər: məlumatın təhlükəsizliyi, kibernetik təhlükəsizlik, bank verilənlərinin təhdidi, avtomatlaşdırılmış bank sistemləri, CİA modeli.

Summary
Evseev S.P., Sochneva A.S., Korol O.G., Abdullayev V.G.
Analysis of risk assessment methodologies for security violation in bank information

The main functions of information security management system (ISMS) and bank information structure are considered. Analysis of the main sources of risks in the CIA model are performed: data confidentiality, integrity and availability, information security, cyber security. Anomaly detection methods and violation risk assessment methodologies to form the model with an integrated approach of risk assessment for bank systems security are analyzed.

Key words: security of information, cyber security, bank data threats, automatized bank systems, CIA model.