УДК 336.011

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ В КОММЕРЧЕСКИХ БАНКАХ

Гусев Е.Г.,
Дальневосточный федеральный университет, Владивосток,
email: gusev.eg@dvfu.ru

Поршкевич Н.Ю.,
Морской государственный университет имени адмирала Г.И. Невельского, Владивосток,
email: porshkevich@inbox.ru, vvswork19@gmail.com

Шумихин В.В.,
Морской государственный университет имени адмирала Г.И. Невельского, Владивосток,
email: porshkevich@inbox.ru, vvswork19@gmail.com

Аннотация. *На сегодняшний день информация играет особую роль в процессе развития личности, общества, государства и всей цивилизации в целом. Особая значимость информации проявляется именно для банковской сферы, которая напрямую связана с ее спецификой, без которой невозможно представить осуществление банковской деятельности. Цель исследования – разработка модели эффективного управления информационной безопасностью в коммерческих банках. Предмет исследования – процесс управления информационной безопасностью в коммерческих банках. Гипотеза исследования заключается в предположении о том, что: 1) информационная безопасность кредитных организаций приобретает все больший научный и практический интерес в связи с активизацией кибермошенничества и цифровизацией экономических систем; 2) вариативность информационных систем обеспечивает возможность эффективного управления информационной безопасностью кредитных организаций с учетом особенностей организационного устройства, финансовых возможностей, специфики операций. При написании работы были использованы общенаучные методы исследования (анализ, синтез, сравнение, логическая интерпретация, аналогия), метод сбора информации (контент – анализ).*

Ключевые слова: экономическая безопасность, управление, риски, оценка, управление, кредитная организация, банк, цифровизация, информационная безопасность.

INFORMATION SECURITY MANAGEMENT IN COMMERCIAL BANKS

Gusev E.G.,
Far Eastern Federal University, Vladivostok,
email: gusev.eg@dvfu.ru

Porshkevich N.Yu.,
Admiral G.I. Nevelskiy Maritime State University, Vladivostok,
email: porshkevich@inbox.ru, vvswork19@gmail.com

Shumikhin V.V.,
Admiral G.I. Nevelskiy Maritime State University, Vladivostok,
email: porshkevich@inbox.ru, vvswork19@gmail.com

Abstract. *Today, information plays a special role in the development of the individual, society, the state and the entire civilization as a whole. The special importance of information is manifested precisely for the banking sector, which is directly related to its specifics, without which it is impossible to imagine banking activities. The purpose of the study: to develop a model for effective information security management in commercial banks. The subject of the study is the information security management process in commercial banks. The hypothesis of the study is the assumption that: 1) information security of credit institutions is gaining increasing scientific and practical interest in connection with the intensification of cyberbullying and digitalization of economic systems; 2) the variability of information systems makes it possible to effectively manage the information security of credit institutions, taking into account the peculiarities of the organizational structure, financial capabilities, and specifics of operations. When writing the work, general scientific research methods (analysis, synthesis, comparison, logical interpretation, analogy), the method of collecting information (content analysis) were used.*

Keywords: economic security, management, risks, assessment, management, credit institution, bank, digitalization, information security.

Банковский бизнес развивается в условиях, которые носят неопределенный характер. Финансовые организации должны выстраивать целостную систему управления всеми выявляемыми банковскими рисками. В современных социально-экономических условиях следует уделить особое внимание развитию финансовой сферы России и важной ее составляющей – банковской системы. Каждый коммерческий банк функционирует не обособленно, а в общем пространстве, и его действия должны быть согласованы с интересами клиентов, инвесторов, конкурентов. Вопрос банковской безопасности является актуальным для его владельцев, акционеров, поскольку от того, насколько будет защищенным банк, будет зависеть степень развития бизнеса, уровень полученной прибыли.

Рассматриваемая тема достаточно широко раскрыта в научной литературе с теоретической и методологической стороны, а также с точки зрения изучения опыта коммерческих банков в данной сфере. Экономическая безопасность кредитных организаций комплексная и многогранная категория, включающая различные составляющие: финансовую, кадровую, информационную, цифровую и др. Каждая составляющая характеризуется определенным набором критериев и показателей. В научном пространстве активно исследуются каждая составляющая, изучается их взаимовлияние и корреляция. Например, финансовая составляющая активно изучается и представлена в работах Левкиной Е.В., Лялиной Ж.И., Локша А.В. [1,2], а кадровая составляющая рассматривается в научных исследованиях Т.М. Ярковой[3]. Информационная безопасность раскрывается в работах: С.Ю. Балычева, Н.О. Бебишевой, Н.В. Гриневой, В.В. Еремеева, С.Ч. Кадимовой, А.А. Коваленко, С.С. Морозкиной, Т.А. Селищевой, Н.Э. Соколинской, Э.А. Умерова и пр.

В условиях санкционных ограничений, закрытия зарубежных проектов и программ безопасности, учащения кибермошенничества изучение информационной безопасности и разработка алгоритмов и моделей управления ей приобретает все большую актуальность в современном мире цифровизации экономических систем.

Методика исследования

При написании работы были использованы общенаучные методы исследования (анализ, синтез, сравнение, логическая интерпретация, аналогия), метод сбора информации (контент-анализ).

Информационной базой для проведения исследования служат отчёты по формам статистической налоговой отчётности, база данных единой межведомственной информационной-статистической системы (ЕМИСС), налоговый паспорт субъекта РФ.

Результаты исследования

Для совершенствования управления, прежде всего, необходимо определиться с методическим обеспечением процесса: задать теоретическую рамку, выбрать методику, определить алгоритм действий. Под информационной системой коммерческого банка в исследовании понимается набор взаимосвязанных компонентов, которые собирают, обрабатывают, хранят и распространяют информацию и обеспечивают механизм обратной связи для достижения цели.

Можно отметить, что информационная система представляет собой и совокупность множества наборов данных, которые обеспечивают успешное выполнение бизнес-задачи. Информационные системы не являются самостоятельной моделью ИТ-индустрии. Вместо этого важнейшим аспектом их успешного внедрения является их интеграция с данными и бизнес-процессами.

Информационные системы можно рассматривать как состоящие из пяти основных компонентов: аппаратного обеспечения, программного обеспечения, данных, людей и процессов. Соответственно, предметом защиты информации является информация, хранящаяся, обрабатываемая и передаваемая в компьютерных системах. К объектам защиты информации относятся информация, носитель информации или информационный процесс, которые нуждаются в защите от несанкционированного доступа, изменения и копирования третьими лицами. В свою очередь носителями защищаемой информации могут быть физические лица, материальные объекты, физические поля.

На данный момент существует множество российских и зарубежных организаций, которые создают различные автоматизированные банковские системы, и если говорить об использовании автоматизированных банковских системах в России, то пятью самыми популярными разработчиками АБС являются: ЦФТ, Диасофт (клиентами которого являются ПАО «Сбербанк России», АО «Газпромбанк», АО «АльфаБанк»), R-Style, ПрограмБанк, Инверсия. На их долю приходится почти 95% всего рынка АБС. Системы, произведенные за рубежом, не очень популярны из-за сложной адаптации к российскому законодательству.

В целом, информационные системы банка используются как в управленческой деятельности банка (учет, контроль, анализ), так и при осуществлении традиционных банковских операций (расчетно-кассовое обслуживание, кредитование и т.д.). Информационная система банка также включает в себя и телекоммуникационные средства, позволяющие осуществлять электронные банковские услуги (дистанционное обслуживание), а также поддерживать расчеты с банками-корреспондентами, собственными филиалами, и структурными подразделениями. Приведенный перечень составляющих информационных систем в определенной степени условный, поскольку на практике информационная система может решать комплекс задач, обладать рядом свойств и характеристик, поэтому при работе следует учитывать специфику конкретной информационной системы. Информационные системы являются предметом процесса обеспечения информационной безопасности. В свою очередь, информацион-

ная безопасность – это набор методов, направленных на защиту персональных данных от несанкционированного доступа и изменения во время хранения или передачи из одного места в другое. Информационная безопасность разработана и внедрена для защиты печатных, электронных и других частных, конфиденциальных и персональных данных от посторонних лиц, используется для защиты данных от неправильного использования, раскрытия, уничтожения, изменения и нарушения.

Существует несколько основных компонентов информационной безопасности.

1. Конфиденциальность. Данные являются конфиденциальными, когда к ним имеют доступ только авторизованные лица. Чтобы обеспечить конфиденциальность, необходимо использовать все методы, разработанные для обеспечения безопасности, такие как надежный пароль, шифрование, аутентификация и защита от атак проникновения.

2. Целостность – означает сохранение данных и предотвращение их случайных или злонамеренных изменений. Методы, используемые для обеспечения конфиденциальности, могут защитить целостность данных, поскольку киберпреступник не может изменить данные, если он не может получить к ним доступ. Чтобы обеспечить всестороннюю целостность, несколько инструментов помогают улучшить ее.

3. Доступность – это еще один базовый элемент информационной безопасности. Очень важно убедиться, что к данным не имеют доступа посторонние лица, но только те, у кого есть разрешение, могут получить к ним доступ. Доступность в информационной безопасности означает соответствие сетевых и вычислительных ресурсов для вычисления доступа к данным и реализации более эффективной политики для целей аварийного восстановления. Именно системное поддержание равновесия между различными элементами системы информационной безопасности может обеспечить ее бесперебойное и длительное функционирование. Поддержание такого равновесия и есть основная задача банка.

В современных реалиях основная угроза информационной безопасности – человеческий фактор. Основополагающая часть утечки информации объясняется халатностью банковского персонала [4]. Также серьезные опасения вызывает, например, новый источник информации, особенно в рамках автоматизированного сбора данных. Угроза кибератак сегодня очень реальна и может повлиять на широкий сегмент пользователей. Большинство актов киберпреступности выпадают на долю банков. Банки, в свою очередь, не заинтересованы в раскрытии общественности такой информации, поскольку даже слухи об этом могут дискредитировать их в глазах клиентов, что повлечет за собой значительный отток капитала, поэтому кибератаки остаются вне статистики. В то же время из– за этого банки несут убытки, оцениваемые в миллиарды долларов. Стоит отметить, что ключевым мотивом кибератак на банковский сектор является не столько финансовая выгода, сколько желание получить данные: 66% против 31%, и объектами атак в большинстве случаев являются компьютеры, серверы и сетевое оборудование – 89% [5].

Несанкционированный доступ (НСД) – вид компьютерных нарушений, при котором злоумышленник получает доступ к объекту, на который у него нет разрешения в соответствии с принятой в организации политикой информационной безопасности. Самая главная проблема этой угрозы заключается в четком разграничении круга лиц, которые должны иметь доступ к определенным наборам данных.

Фишинговые атаки также являются одной из наиболее распространенных проблем кибербезопасности в банках. Они могут оказать разрушительное воздействие на финансовые учреждения, поскольку их можно использовать для закрепления в сети учреждения для запуска более масштабной атаки, такой как APT (Advanced Persistent Threat). В случае APT неавторизованный пользователь может получить доступ к системе и оставаться незамеченным в течение длительного периода. Это может привести к значительным потерям в денежном выражении, потере данных, а также к репутационному ущербу.

Анализ потенциальных угроз безопасности информационной системы коммерческого банка показал, что в качестве потенциальных угроз безопасности информационной системы коммерческого банка специалистами выделяются такие, как копирование и взлом базы данных 1С; несанкционированный доступ к серверному оборудованию; низкая отказоустойчивости системы, низкий уровень защиты сервера от сбоев; низкий уровень сетевой безопасности и организация защиты информационных систем банка.

Для обеспечения защиты от вышеизложенных угроз необходимо эффективное управление информационной безопасностью в банке. Информационное обеспечение управления банка представляет собой связь информации с основными системами управления, а также с управленческим процессом в целом, которая формируется в процессе сбора и переработки информации, необходимой для обеспечения указанных процессов и принятия обоснованных управленческих решений. Таким образом, эффективность информационного обеспечения управления должна оцениваться с точки зрения таких факторов как:

– сила связи информации с основными системами управления организации, а также с управленческим процессом в целом;

– организация сбора и переработки информации;

– уровень автоматизации сбора и переработки информации;

– абсолютных и относительных величин оценки соотношения затрат на информационное обеспечение управления и полученных доходов.

Управление информационной безопасностью – это совокупность практик, связанных с поддержкой, определением и направлением усилий организации по обеспечению безопасности. Управление безопасностью тесно связано и часто переплетается с корпоративным и ИТ-управлением.

Надежность и эффективность банковской деятельности обеспечивается через реализацию соответствующих требований к системе безопасности (непрерывность, плановость, конкретность, активность, гибкость, комплексность), а важной составляющей банковской безопасности является информационная безопасность.

С помощью современных информационных систем обеспечивается оптимальная экономическая безопасность банка. Рассмотрим подробнее существующие системы.

1. Управление инцидентами и событиями безопасности (SIEM). Решения SIEM позволяют вам получать и сопоставлять информацию из разных ваших систем. Такое объединение данных позволяет группам более эффективно обнаруживать угрозы, более эффективно управлять оповещениями и обеспечивать лучший контекст для расследований. Решения SIEM также полезны для регистрации событий, происходящих в системе, или для составления отчетов о событиях и производительности. Затем вы можете использовать эту информацию для подтверждения соответствия требованиям или для оптимизации конфигураций.

2. Предотвращение потери данных (DLP). Стратегии DLP включают инструменты и методы, которые защищают данные от потери или изменения. Это включает в себя категоризацию данных, резервное копирование данных и мониторинг того, как данные передаются внутри организации и за ее пределами. Например, вы можете использовать решения DLP для сканирования исходящих электронных писем, чтобы определить, не передается ли конфиденциальная информация ненадлежащим образом.

3. Система обнаружения вторжений (IDS). Решения IDS – это инструменты для мониторинга входящего трафика и обнаружения угроз. Эти инструменты оценивают трафик и предупреждают о любых случаях, которые кажутся подозрительными или вредоносными.

4. Система предотвращения вторжений (IPS). Решения для обеспечения безопасности IPS аналогичны решениям IDS, и они часто используются вместе. Эти решения реагируют на трафик, который идентифицируется как подозрительный или вредоносный, блокируя запросы или завершая сеансы пользователей. Вы можете использовать решения IPS для управления сетевым трафиком в соответствии с определенными политиками безопасности [6].

5. Поведенческая аналитика пользователей (UBA). Решения UBA собирают информацию о действиях пользователей и соотносят это поведение с базовым уровнем. Затем решения используют этот базовый уровень для сравнения с новыми моделями поведения для выявления несоответствий. Затем решение помечает эти несоответствия как потенциальные угрозы. Например, вы можете использовать решения UBA для мониторинга действий пользователей и определения того, начинает ли пользователь экспортировать большие объемы данных, что указывает на инсайдерскую угрозу.

6. Кибербезопасность блокчейна – это технология, которая опирается на неизменяемые транзакционные события. В технологиях блокчейна распределенные сети пользователей проверяют подлинность транзакций и обеспечивают сохранение целостности. Хотя эти технологии еще не получили широкого распространения, некоторые банки начинают внедрять блокчейн в большее количество решений.

7. Решения для кибербезопасности EDR позволяют отслеживать активность конечных точек, выявлять подозрительные действия и автоматически реагировать на угрозы. Эти решения предназначены для улучшения видимости конечных устройств и могут использоваться для предотвращения проникновения угроз в ваши сети или утечки информации. Решения EDR основаны на непрерывном сборе данных о конечных точках, механизмах обнаружения и регистрации событий [6].

8. CSPM – это набор методов и технологий, которые можно использовать для оценки безопасности облачных ресурсов. Эти технологии позволяют сканировать конфигурации, сравнивать средства защиты с эталонными показателями и обеспечивать единообразное применение политик безопасности. Часто решения CSPM предоставляют рекомендации или рекомендации по исправлению, которые вы можете использовать для улучшения своей системы безопасности.

9. Виртуальная частная сеть удаленного доступа (VPN) позволяет организациям обеспечивать безопасный удаленный доступ к данным и приложениям, находящимся в корпоративной сети. VPN создает туннель между сетью и удаленным пользователем. Он защищает трафик, проходящий через туннель, путем его шифрования. Удаленный доступ по VPN подключает одного пользователя к локальным ресурсам, но не обеспечивает доступ к облачным ресурсам. Пограничная служба безопасного доступа (SASE) обеспечивает безопасность в гибридной среде, обеспечивая видимость всех ресурсов. SASE – это облачный сервис, который не полагается

на VPN или автономные прокси– серверы. Вместо этого он предоставляет различные инструменты сетевой безопасности в виде облачного сервиса [6].

10. «Принесите свое собственное устройство» (BYOD) – это подход, который позволяет сотрудникам использовать свои личные устройства, такие как ноутбуки, планшеты, смартфоны, USB-накопители и ПК, для рабочих целей. Это означает, что сотрудники могут использовать свои устройства для подключения к корпоративной сети и доступа к конфиденциальным системам и конфиденциальным данным. BYOD может улучшить пользовательский опыт, позволяя сотрудникам работать с использованием привычных устройств из любого места. Это позволяет сотрудникам использовать свои устройства для удаленной работы из дома или во время путешествий. Однако BYOD часто приводит к теневому ИТ, поскольку ИТ-персонал плохо видит эти конечные точки и не может должным образом внедрять и поддерживать меры безопасности. Организации могут защитить себя от угроз BYOD, используя решения для виртуализации приложений и обеспечения безопасности конечных точек, чтобы расширить видимость и получить всесторонний контроль безопасности и управления.

11. Berkshire Bank является примером компании, которая решила реструктурировать свою стратегию DLP. Компания хотела получить доступ к более подробным отчетам о событиях. Их старая система предоставляла только общую информацию, когда угрозы были предотвращены, но компания хотела знать подробности о каждом событии. Шифрование – это процесс скремблирования информации, чтобы сделать ее бессмысленной. Организации часто используют шифрование для защиты информации от несанкционированного использования.

Такие инструменты, как статическое тестирование безопасности приложений (SAST) и динамическое тестирование безопасности приложений (DAST), проверяют наличие уязвимостей в проприетарном коде во время разработки. Организации также могут использовать сканеры с открытым исходным кодом для автоматической инвентаризации компонентов с открытым исходным кодом и поиска известных уязвимостей и потенциальных недостатков. Тестирование на проникновение (пентестинг) включает в себя имитацию кибератаки для поиска уязвимостей и слабых мест в системе безопасности. Это разрешенная форма этического взлома, выполняемая для улучшения состояния безопасности организации. Существуют различные способы проведения пентеста. Например, внешнее пентестирование предполагает попытку взлома сети без предварительного знания архитектуры, в то время как внутреннее тестирование включает проверку исходного кода на предмет обнаружения уязвимостей [6].

Таким образом, с целью предотвращения нарушений информационной безопасности информационных банковских ресурсов нужно постоянно выявлять и анализировать уязвимые места информационной системы банка и ресурсы, которые требуют защиты, а также вероятные атаки, которые могут произойти в конкретном окружении. После этого нужно определить информационные риски для определенного информационного ресурса, выбрать контрмеры, в соответствии с выбранной политикой банковской безопасности, и обеспечить безопасность с помощью механизмов и сервисов безопасности. Политика банковской безопасности должна определять взаимосвязанная совокупность механизмов и сервисов безопасности, адекватную защищаемым ресурсам и окружению, в котором их используют. Механизмы защиты банковской информации подразумевают защиту от утечки, контроль доступа; межсетевые экраны; антивирусные программы; программы шифрования информации и системы распознавания.

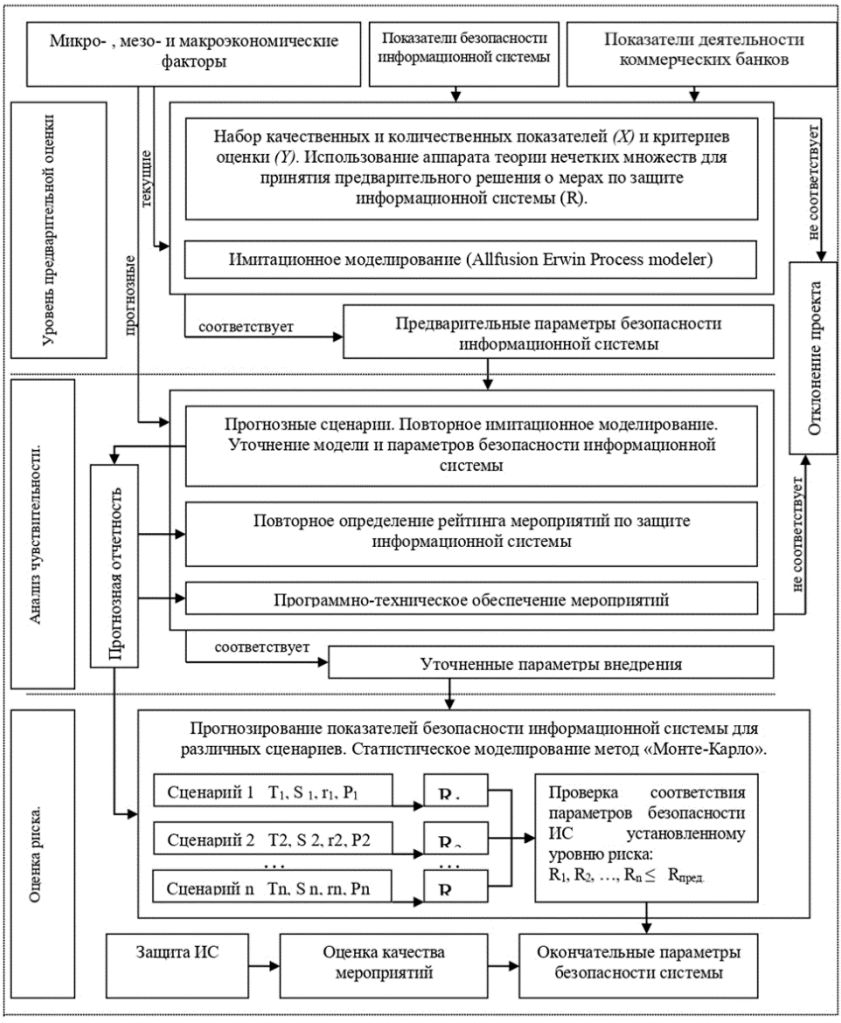


Рис. 1. *Модель системы защиты информационной системы коммерческого банка*

Процесс проектирования концептуальной модели системы защиты информационной системы должен быть разделен на дискретные компоненты информационных технологий, включающие организационные схемы, виды деятельности и потоки процессов функционирования организации. Эти диаграммы могут быть сконфигурированы в виде организационных циклов, включающих периоды и сроки, соответствующие поставщикам технологического оборудования, программного обеспечения и услуг.

Чтобы деконструировать и описать макрофинансовые последствия операционных и киберрисков, модель системного киберриска разделена на четыре отдельных аспекта:

1. Контекст – обстоятельства, при которых возникает киберин– инцидент, в форме кристаллизованного кибер-риска.

2. Шок – описание технических и деловых последствий, испытанных в момент возникновения киберин-инцидента.

3. Усиление – системные усилители и каналы заражения, которые усиливают шок через систему, увеличивая масштаб испытываемого воздействия.

4. Системное событие – точка, в которой система больше не способна поглощать шок.

Общая предлагаемая концептуальная модель системы защиты информационной системы коммерческого банка представлена на рисунке 1.

Согласно представленной модели, можно отметить, что на безопасность информационных систем кредитных организаций влияют факторы всех уровней экономической системы: законодательство федерального уровня, политика региона, внешнеэкономические связи, инфляция, цифровизация и т.д. Модель состоит из трех основных этапов (блоков): уровень предварительной оценки, анализ чувствительности и оценка рисков. Предварительная оценка предполагает определение, группировку, аккумуляцию факторов, оказывающих влияние на информационные системы коммерческих банков. С помощью математических методов и имитационного моделирования осуществляется агрегирование факторов и оценка их степени влияния.

Далее за счет имитационного моделирования разрабатываются возможные прогнозные сценарии верификации безопасности информационных систем. По результатам второго этапа «Анализ чувствительности» определяется необходимое программно-техническое обеспечение для безопасности информационных систем. Оценка рисков (третий этап (блок)) заключается в прогнозировании показателей безопасности информационной системы для различных сценариев посредством статистического моделирования методом «Монте-Карло».

Важно помнить, что доля рисков может возрастать с изменением количества и степени влияния фактора каждого уровня, например, с приростом количества пользователей и устройств с доступом. С увеличением числа устройств, принадлежащих сотрудникам банка, возрастает также риск случайной утечки данных через приложения и службы, такие как электронная почта, социальные сети и публичное облако, которые находятся вне контроля кредитной организации. Например, когда сотрудник отправляет последние инженерные фотографии из своей личной учетной записи электронной почты, копирует и вставляет информацию о продукте в социальные сети или сохраняет отчет о продажах в публичном облачном хранилище.

Выводы

Проведенный анализ специфики информационных систем коммерческих банков позволил выявить и структурировать общие требования по защите информации в коммерческом банке, формализовать его структуру и описать процесс автоматизации мониторинга событий информационной безопасности в рамках банковских организаций. Полученные результаты в дальнейшем могут быть использованы при проектировании защищенных информационных систем поддержки операционных задач в финансовой и организационной сферах банковской деятельности. Процесс проектирования концептуальной модели системы защиты информационной системы был разделен на дискретные компоненты информационных технологий, включающие организационные схемы, виды деятельности и потоки процессов функционирования организации. Представленные авторские блоки могут быть сконфигурированы в виде организационных циклов, включающих периоды и сроки, соответствующие поставщикам технологического оборудования, программного обеспечения и услуг.

Литература

1. Левкина Е.В., Лялина Ж.И., Локша А.В. Оценка финансовой составляющей экономической безопасности организации (на примере ПАО АКБ «Приморье», г. Владивосток) // Экономическая безопасность. 2021. Т. 4. № 4. С. 1277-1300. DOI: 10.18334/ecsec.4.4.113195.

2. Левкина Е.В., Лялина Ж.И., Локша А.В. Методические аспекты управления кредитным риском в коммерческих банках (на примере ПАО АКБ «Приморье») // Азимут научных исследований: экономика и управление. 2021. Т. 10. № 3 (36). С. 223-228.

3. Яркова Т.М. Современные подходы обеспечения кадровой безопасности организаций в России // Экономика труда. 2022. Т. 9. № 3. С. 731-742. DOI: 10.18334/et.9.3.114425.

4. Трушко К.О. Необходимость и сущность стратегии информационной безопасности ПАО «Сбербанк» // В сборнике: Пути и методы адаптации экономики региона и предприятий в условиях пандемии и связанных с ней кризисных явлений. Сборник научных статей по материалам международной научно-практической конференции преподавателей, аспирантов, студентов и практиков / Под редакцией В.А. Матчинова, О.Н. Сусляковой. Калуга, 2020. С. 843-849

5. Обухова А.С., Пияльцев А.И. Киберпреступления и кибербезопасность в банковском секторе: понятие и современные угрозы // Известия Юго-Западного государственного университета. Серия: Экономика. Социология. Менеджмент. 2020. Т. 10. № 6. С. 42-51.

6. Касенов А.А., Данильченко П.А., Батов М.А., Седина М.С. Построение эффективной системы защиты информации автоматизированных и информационных систем // Modern Science. 2019. № 12. С. 153-156.