МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра Информационных технологий и систем безопасности

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

(дипломная работа)

На тему « Разработка модели аудита безопасности информации в финансово–экономической организации в условиях деструктивных воздействий»

Исполнитель _____ Демакова Анастасия Ивановна

(подпись) (фамилия, имя, отчество)

Руководитель _____ Юрин Игорь Валентинович

(подпись) (фамилия, имя, отчество)

«К защите допускаю»

Заведующий кафедрой _____ Лепешкин Олег Михайлович

(подпись) (фамилия, имя, отчество)

«____»_____2026г.

Санкт–Петербург 2026

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра Информационных технологий и систем безопасности

«УТВЕРЖДАЮ»

Заведующий кафедрой

_____ Лепешкин Олег Михайлович

(подпись) (фамилия, имя, отчество)

«_____»_____ 20__ года

Задание

на выпускную квалификационную работу

студенту: Демаковой Анастасии Ивановне

(фамилия, имя, отчество)

1. Тема Разработка модели аудита безопасности информации в финансово–экономической организации в условиях деструктивных воздействий

закреплена приказом ректора Университета от «___» _____20___ года,

№ _____

2. Срок сдачи законченной работы «___» _____20___ года

3. Исходные данные к выпускной квалификационной работе:

_____

4. Перечень вопросов, подлежащих разработке (краткое содержание работы:

Введение. Актуальность темы, цели и задачи ВКР

Глава 1 Анализ предметной области и теоретические основы аудита системы обеспечения информационной безопасности финансово-экономической организации

(наименование главы)

Глава 2 Деструктивные условия окружающей среды и требования к аудиту системы обеспечения информационной безопасности

(наименование главы)

Глава 3 Разработка теоретической модели аудита системы обеспечения информационной безопасности финансово-экономической организации в деструктивных условиях окружающей среды

(наименование главы)

Заключение. Выводы по работе в целом. Оценка степени решения поставленных задач. Практические рекомендации.

5. Перечень материалов, представляемых к защите:

- Пояснительная записка;
- Блок-схема процесса аудита СОИБ;

6. Дата выдачи задания: «___» _____ 20___ года

Руководитель выпускной квалификационной работы

_____ _____

(должность, ученая степень, ученое звание, фамилия, имя, отчество) (подпись)

Задание принял к исполнению «___» 20___ года

Студент Демакова Анастасия Ивановна, ИБ–С20–1 _____

(фамилия, имя, отчество, учебная группа) (подпись)

РЕФЕРАТ

Дипломная работа: с., рис., табл., приложения, источников литературы.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, СИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, РИСК–ОРИЕНТИРОВАННЫЙ ПОДХОД, ФИНАНСОВО–ЭКОНОМИЧЕСКАЯ ОРГАНИЗАЦИЯ, ДЕСТРУКТИВНЫЕ УСЛОВИЯ.

Объект исследования: система обеспечения информационной безопасности финансово–экономической организации.

Предмет исследования – процессы, методы и критерии аудита системы обеспечения информационной безопасности в условиях деструктивного воздействия окружающей среды.

Цель работы – разработка модели аудита системы обеспечения информационной безопасности финансово–экономической организации, обеспечивающей адаптацию аудиторских процедур к деструктивным условиям окружающей среды и повышение результативности оценки уровня информационной безопасности.

В дипломной работе рассмотрены теоретические основы аудита системы обеспечения информационной безопасности и существующие подходы к его проведению. Выявлены и классифицированы деструктивные условия окружающей среды, влияющие на функционирование системы обеспечения информационной безопасности. Разработана модель аудита системы обеспечения информационной безопасности и предложена методика ее применения на примере типовой финансово–экономической организации.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Финансово-экономические организации опираются на непрерывную обработку транзакций и данных клиентов: учет операций, дистанционное обслуживание, формирование регуляторной и управленческой отчетности, взаимодействие с платежной инфраструктурой и контрагентами реализуются преимущественно через информационные системы. Поэтому устойчивость и корректность работы этих систем напрямую определяют способность организации выполнять обязательства перед клиентами и соблюдать требования внешнего контроля.

Инциденты информационной безопасности в данной сфере, как правило, имеют измеримый ущерб. Компрометация конфиденциальности приводит к утечкам персональных и финансовых данных, нарушению режима коммерческой или банковской тайны; нарушение целостности выражается в искажении учетной информации и параметров операций; нарушение доступности – в простоях сервисов и невозможности проведения операций в установленные сроки. Тем самым обеспечение конфиденциальности, целостности и доступности информации выступает не вспомогательной, а системообразующей задачей управления организацией.

Контроль уровня информационной безопасности требует не только внедрения мер защиты, но и регулярной оценки их достаточности и работоспособности. Таким инструментом выступает аудит системы обеспечения информационной безопасности (СОИБ), позволяющий сопоставлять фактическое состояние с установленными требованиями, выявлять несоответствия и формировать приоритетные рекомендации. Однако при росте внешних воздействий и ограниченности ресурсов организации возрастает риск формального аудита, который фиксирует наличие документов и средств защиты, но не отражает устойчивость процессов и реальный уровень риска. В связи с этим актуальной является разработка теоретической модели аудита СОИБ финансово-экономической организации, адаптированной к

деструктивным условиям окружающей среды.

Актуальность выпускной квалификационной работы определяется необходимостью совершенствования теоретических и методических подходов к аудиту информационной безопасности финансово-экономических организаций в условиях нестабильной и неблагоприятной внешней среды, а также потребностью в формализованных моделях аудита, обеспечивающих объективную и воспроизводимую оценку состояния СОИБ.

Объект исследования – система обеспечения информационной безопасности финансово-экономической организации.

Предмет исследования – процессы, методы и критерии аудита системы обеспечения информационной безопасности в условиях деструктивного воздействия окружающей среды.

Цель выпускной квалификационной работы – разработка модели аудита системы обеспечения информационной безопасности финансово-экономической организации, обеспечивающей адаптацию аудиторских процедур к деструктивным условиям окружающей среды и повышение результативности оценки уровня информационной безопасности.

Задачи исследования:

1. проанализировать особенности финансово-экономических организаций как объекта аудита информационной безопасности;
2. рассмотреть теоретические основы и существующие подходы к аудиту системы обеспечения информационной безопасности;
3. выявить и классифицировать деструктивные условия окружающей среды, влияющие на функционирование СОИБ;
4. определить требования к процессу аудита информационной безопасности в условиях деструктивного воздействия;
5. разработать структуру и содержание модели аудита системы обеспечения информационной безопасности;
6. сформировать критерии и показатели оценки соответствия,

результативности и устойчивости, включая элементы оценки процессов ИБ;

7. разработать методику применения модели аудита на примере типовой финансово-экономической организации.

Методы исследования – методы теоретического анализа, методы системного анализа, методы структурного и функционального моделирования, методы анализа рисков информационной безопасности, методы экспертной оценки.

Нормативно-правовую и нормативно-техническую основу исследования составляют Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [1], Федеральный закон № 152-ФЗ «О персональных данных» [2], Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [3], Приказ ФСТЭК России № 21 (в части организационных и технических мер по обеспечению безопасности персональных данных) [4], Положение Банка России № 851-П (требования к обеспечению защиты информации при осуществлении банковской деятельности) [5], а также ГОСТ Р 57580.1–2017 и ГОСТ Р 57580.2–2018, регламентирующие требования и методику оценки соответствия защиты информации финансовых организаций [6], [7]. Теоретическая и методическая база исследования опирается на работы по аудиту информационной безопасности и ИТ-аудиту [8], [9], по управлению информационной безопасностью [10], а также на риск-ориентированные подходы к внутреннему аудиту ИБ [11], международные руководства по построению СУИБ и организации аудита [12], [13], и рекомендации по контролям и оценке рисков (NIST) [14], [15].

Выпускная квалификационная работа состоит из следующих разделов: введения, трех глав, заключения, списка использованных источников и приложений.

В первой главе рассмотрены особенности финансово-экономических организаций как объекта защиты, раскрыта структура и функции системы обеспечения информационной безопасности, проанализированы подходы к аудиту СОИБ, нормативно-методическая база и критерии оценки, а также сформулирована постановка задачи выпускной квалификационной работы.

Во второй главе введено понятие деструктивных условий окружающей

среды применительно к аудиту информационной безопасности, выполнена классификация факторов и анализ их влияния на риски и функционирование СОИБ, определены показатели устойчивости и метрики контроля, а также сформулированы требования к модели аудита, адаптированной к деструктивному внешнему контексту.

В третьей главе разрабатывается теоретическая модель аудита системы обеспечения информационной безопасности финансово-экономической организации: описываются структура модели, этапы проведения аудита, входные данные и артефакты, правила классификации несоответствий и формирования рекомендаций.

В заключении представлены итоги исследования и основные выводы, отражающие степень достижения цели и решения поставленных задач.

ГЛАВА 1. АНАЛИЗ ПРЕДМЕТНОЙ ОБЛАСТИ И ТЕОРЕТИЧЕСКИЕ ОСНОВЫ АУДИТА СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ФИНАНСОВО-ЭКОНОМИЧЕСКОЙ ОРГАНИЗАЦИИ

1.1. Особенности финансово-экономических организаций как объекта обеспечения информационной безопасности

Финансово-экономические организации (банки, микрофинансовые организации, брокерские и управляющие компании, платежные сервисы, страховые организации, казначейские и расчетные подразделения крупных корпораций) характеризуются высокой зависимостью от информационных технологий и непрерывной обработкой данных. Для таких организаций информационные активы выступают не вспомогательным ресурсом, а ядром бизнес-деятельности: через информационные системы осуществляется учет операций, управление счетами и договорами, формирование отчетности, взаимодействие с клиентами и контрагентами, а также выполнение обязательных требований внешнего контроля.

Особенность предметной области состоит в том, что последствия инцидентов информационной безопасности приобретают системный характер. Нарушение конфиденциальности приводит к утечкам персональных и финансовых данных клиентов, нарушению банковской или коммерческой тайны. Нарушение целостности может выражаться в подмене реквизитов платежей, искажении данных учета, манипуляциях с лимитами и параметрами финансовых операций. Нарушение доступности отражается на невозможности осуществлять операции, обслуживать клиентов и выполнять обязательства в установленные сроки. Следовательно, для финансово-экономической организации критичны все базовые свойства безопасности информации: конфиденциальность, целостность и доступность.

Дополнительной характеристикой является высокая доля регламентированных процессов и требований доказуемости. Организация должна поддерживать управляемость процессов, включая процессы

обеспечения информационной безопасности: наличие политик, регламентов, процедур, журналов учета, планов реагирования и восстановления. Поэтому оценка информационной безопасности должна учитывать не только наличие технических средств защиты, но и полноту организационно-распорядительной документации, качество процессов управления рисками и инцидентами, дисциплину исполнения регламентов персоналом.

Практически объект аудита ИБ в финансово-экономической организации целесообразно описывать через взаимосвязанные компоненты: (1) активы и данные; (2) процессы, в которых данные используются; (3) инфраструктура, обеспечивающая выполнение процессов. К активам относятся базы данных клиентов и операций, учетные и отчетные данные, платежные документы, ключевая информация, учетные записи и права доступа, а также программные и аппаратные компоненты. Процессы включают проведение операций, обработку платежей, дистанционное обслуживание, управление договорной базой, интеграцию с внешними системами. Инфраструктура включает рабочие места, серверы, средства виртуализации, сетевое оборудование, каналы связи, системы резервного копирования, средства мониторинга и защиты.

В контексте настоящей работы под деструктивными условиями окружающей среды понимается совокупность факторов внешней среды, повышающих вероятность реализации угроз и/или ухудшающих способность организации поддерживать устойчивое функционирование системы обеспечения информационной безопасности. Для финансово-экономических организаций такими факторами могут выступать рост активности организованных киберпреступных групп, увеличение числа атак на дистанционные каналы обслуживания, усложнение цепочек поставок ИТ-услуг, изменения требований внешнего контроля, а также кадровые ограничения. Эти обстоятельства требуют от аудита перехода от формального контроля к риск-ориентированной оценке результативности и устойчивости СОИБ.

Примеры наиболее критичных информационных активов финансово-

экономической организации приведены в таблице 1.1.

Таблица 1.1 – Примеры критичных информационных активов финансово-экономической организации

Группа активов	Пример	Возможные последствия компрометации
Данные клиентов	Персональные данные, реквизиты, идентификаторы	Утечки, санкции, репутационный ущерб
Финансовые операции	Платежные поручения, транзакционные журналы	Мошеннические операции, искажение учета
Учетные записи	Администраторские и сервисные учетные записи	Эскалация привилегий, захват систем
Ключевая информация	Криптографические ключи, сертификаты	Компрометация защищенных каналов, подмена
Отчетные данные	Регуляторная и управленческая отчетность	Недостоверные отчеты, санкции

1.2. Система обеспечения информационной безопасности: состав, функции и документы

Система обеспечения информационной безопасности в организации целесообразно рассматривать как управляемый контур: кто и на основании каких правил принимает решения по защите, какие процедуры выполняются регулярно, какие данные и журналы подтверждают выполнение требований, и какие технические средства поддерживают эти процедуры. Такое понимание СОИБ важно для аудита, поскольку позволяет оценивать не отдельные «средства защиты», а согласованность ролей, документов, процессов и технологических механизмов, обеспечивающих снижение рисков.

Для корректного построения и последующего аудита СОИБ целесообразно рассматривать ее как систему управления, в которой выделяются: цели и принципы обеспечения ИБ; организационная структура и роли; процессы управления рисками и инцидентами; техническая архитектура защиты; контроль и улучшение. В таком представлении аудит оценивает не только наличие отдельных мер, но и их взаимосвязанность, достаточность и управляемость.

Организационная компонента СОИБ включает распределение ролей и полномочий (руководитель по ИБ, подразделение ИБ, администраторы, владельцы бизнес-процессов, пользователи), а также механизмы контроля исполнения (внутренние проверки, обучение, контроль соблюдения регламентов). Правовая и регламентная компонента включает локальные нормативные акты: политику ИБ, положения о доступе, порядок управления учетными записями, требования к аутентификации, порядок обработки инцидентов, порядок резервного копирования и восстановления, правила работы с носителями и каналами связи, договорные требования к подрядчикам.

Техническая компонента СОИБ включает средства идентификации и аутентификации, управления доступом, сетевой защиты (межсетевые экраны, сегментация, VPN), антивирусной защиты, предотвращения вторжений, контроля целостности, резервного копирования, журналирования, мониторинга и управления событиями безопасности. Для финансово-экономических организаций характерно усиленное внимание к защите дистанционных каналов обслуживания и контролю транзакций, что обусловлено высоким риском мошенничества.

Процессная компонента СОИБ выражается в наличии управляемых циклов: управление рисками, управление изменениями, управление уязвимостями, управление инцидентами, обеспечение непрерывности и восстановление после сбоев, контроль соответствия требованиям. При отсутствии формализованных процессов организация действует реактивно, что

снижает эффективность защиты и затрудняет аудит из-за нехватки критериев оценки и доказательств выполнения процедур.

Документирование в СОИБ выполняет две функции. Во-первых, документы устанавливают требования и правила, обязательные для исполнения. Во-вторых, документы и записи (журналы, отчеты, протоколы) формируют доказательную базу аудита. Поэтому аудит должен оценивать как актуальность нормативных документов, так и фактическое выполнение требований, подтвержденное артефактами.

1.3. Аудит информационной безопасности: сущность, виды и результаты

Аудит информационной безопасности представляет собой систематизированную оценку состояния СОИБ, направленную на получение обоснованных выводов о соответствии требованиям и о фактической результативности мер защиты. Отличительной особенностью аудита является ориентация на доказательства: документы, записи, журналы, результаты проверок и интервью, позволяющие подтвердить выполнение процедур и выявить причины несоответствий. Результаты аудита используются для управленческих решений — выбора приоритетов улучшения и распределения ресурсов с учетом рисков.

По признаку субъекта проведения различают внутренний и внешний аудит. Внутренний аудит выполняется силами организации и применяется для регулярного улучшения СОИБ при обеспечении независимости оценки. Внешний аудит выполняется независимыми специалистами и используется для подтверждения соответствия требованиям и повышения доверия со стороны партнеров и иных заинтересованных сторон.

По содержанию выделяют аудит соответствия и аудит эффективности. Аудит соответствия отвечает на вопрос, выполнены ли установленные требования: внедрены ли предписанные меры, имеются ли необходимые регламенты и соблюдаются ли процедуры. Аудит эффективности отвечает на вопрос, достигаются ли цели безопасности: снижаются ли риски,

обеспечивается ли своевременное выявление и реагирование на инциденты, устойчивы ли процессы. Для финансово-экономических организаций важно сочетание обоих видов, поскольку формальное соответствие не гарантирует устойчивости к актуальным угрозам.

По объекту проверки аудит может быть комплексным (охватывающим СОИБ в целом) либо тематическим (например, аудит управления доступом, аудит резервного копирования, аудит безопасности дистанционных каналов, аудит управления инцидентами). Тематические аудиты позволяют фокусировать ресурсы на наиболее критичных направлениях и получать практический эффект в короткие сроки.

Результаты аудита оформляются отчетом, включающим область аудита и примененную методику, перечень выявленных несоответствий и наблюдений, оценку рисков и их критичности, рекомендации и план корректирующих действий. Для воспроизводимости результатов целесообразно применять единые классификаторы несоответствий и стандартизированные формы отчетности.

1.4. Подходы к аудиту СОИБ и критерии оценки

Методология аудита определяет, какие вопросы проверяются в первую очередь и как интерпретируются результаты. При контрольном подходе основной акцент делается на закрытие перечня требований, что удобно для первичной оценки соответствия. Однако для финансово-экономической организации в условиях повышенного давления внешней среды более ценен риск-ориентированный и процессный анализ, который связывает несоответствия с потенциальным ущербом и проверяет устойчивость ключевых процедур (мониторинг, управление доступом, восстановление, реагирование).

Риск-ориентированный подход предполагает, что приоритет и глубина аудиторских процедур определяются оценкой рисков. Аудит концентрируется на наиболее значимых активах, уязвимостях и сценариях угроз, способных привести к неприемлемым последствиям. Такой подход позволяет эффективнее

использовать ресурсы и повышает управленческую ценность результатов, что особенно важно при росте неопределенности и угроз.

Процессный подход рассматривает СОИБ как совокупность управляемых процессов и оценивает их наличие, полноту регламентации, распределение ответственности, наличие входов и выходов, показателей результативности и механизмов контроля. В рамках такого подхода аудит анализирует управляемость и повторяемость действий организации, а не ограничивается наличием отдельных средств защиты.

Зрелостный подход дополняет процессный и позволяет оценивать уровень развития процессов по шкале зрелости (от неформализованного и реактивного управления до измеряемого и постоянно улучшаемого). Применение шкалы зрелости удобно тем, что дает ориентир для поэтапного развития и позволяет сопоставлять результаты аудита между периодами.

Критерии оценки в аудите СОИБ целесообразно разделять на три группы: (1) критерии соответствия — наличие и выполнение требований (политики, регламенты, процедуры, записи); (2) критерии результативности — способность мер защиты снижать риск и предотвращать инциденты; (3) критерии устойчивости — способность системы сохранять приемлемый уровень безопасности при ухудшении внешних условий. Включение критериев устойчивости является необходимым для аудита СОИБ в деструктивных условиях окружающей среды.

1.5. Анализ существующих подходов к аудиту СОИБ и типовые ограничения

В практике аудита СОИБ применяются различные методологические подходы, которые условно можно разделить на нормативно-ориентированные (аудит соответствия), риск-ориентированные, процессно-ориентированные и комбинированные. Нормативно-ориентированный подход строится на проверке выполнения требований стандартов и внутренних регламентов организации. Риск-ориентированный подход фокусируется на оценке актуальных рисков и

проверке ключевых зон, определяющих уровень остаточного риска. Процессный подход концентрируется на управляемости и воспроизводимости процедур ИБ, а зрелый — на оценке уровня развития процессов и их способности к улучшению.

Нормативно-ориентированный аудит наиболее распространен в силу относительной простоты: наличие перечня требований позволяет быстро формировать программу проверки и фиксировать несоответствия. Однако в финансово-экономической организации данный подход имеет ограничения. Во-первых, выполнение формальных требований не гарантирует эффективности мер защиты в реальных сценариях атак. Во-вторых, нормативные требования нередко задают минимально допустимый уровень, тогда как в условиях повышенной активности угроз и высокой ценности активов требуется углубленная оценка критичных контуров. В-третьих, акцент на документах может приводить к недооценке фактического исполнения процедур и качества контроля.

Риск-ориентированный аудит обеспечивает более высокий управленческий эффект, поскольку связывает выявленные несоответствия с потенциальным ущербом и вероятностью реализации угроз. Его ключевым преимуществом является возможность приоритизации проверок при ограниченных ресурсах. Вместе с тем риск-ориентированный подход предъявляет требования к качеству исходных данных: необходимо иметь хотя бы минимально формализованный реестр активов, описание угроз и уязвимостей, а также понятные правила оценки вероятности и ущерба. При отсутствии этих предпосылок риск-оценка становится экспертной и нуждается в стандартизации, чтобы результаты были сопоставимы между периодами.

Процессный и зрелостный подходы позволяют оценить устойчивость СОИБ в динамике. Для финансово-экономической организации это критично, поскольку устойчивость определяется не только набором технических средств, но и способностью поддерживать регулярные циклы: управление изменениями,

управление уязвимостями, мониторинг и реагирование, контроль доступа, резервное копирование и восстановление. Если процессы не закреплены ответственностью и метриками, система функционирует реактивно: ошибки обнаруживаются поздно, решения принимаются ситуативно, а результаты аудита сложно преобразовать в план улучшений.

Типовой проблемой практики аудита является разрыв между «проверкой наличия» и «проверкой работоспособности». Например, наличие регламента резервного копирования не подтверждает достижение целевых показателей восстановления без проведения тестов; наличие журналирования не подтверждает своевременное обнаружение атак без процедур анализа и реагирования; наличие политики доступа не подтверждает корректность выдачи привилегий без выборочных проверок заявок, согласований и фактических прав. Поэтому в современных условиях аудит должен сочетать документальную проверку, интервью, выборочные технические проверки и анализ артефактов выполнения процедур.

Отдельное ограничение связано с контекстом деструктивных условий окружающей среды. При росте интенсивности атак, ограничениях обновлений, зависимости от подрядчиков и дефиците кадров повышается вероятность того, что внедренные меры защиты будут работать неполноценно. Следовательно, аудит должен оценивать не только «проектное состояние» (что внедрено), но и «эксплуатационное состояние» (как поддерживается, как контролируется, как реагируют на отклонения). Это требует дополнительных критериев устойчивости и правил адаптации программы аудита под внешний контекст.

1.6. Нормативно-методическая база аудита и управления информационной безопасностью

Нормативно-методическая база является опорой для формулирования критериев аудита СОИБ и определения ожидаемых результатов проверки. Для финансово-экономических организаций, как правило, применима многоуровневая система требований: международные стандарты и лучшие

практики, национальные стандарты и методические документы, а также внутренние регламенты организации и требования договоров с контрагентами. В рамках ВКР нормативно-методическая база рассматривается как источник критериев аудита, но не как перечень для механической «галочки».

К числу наиболее применимых международных документов относятся стандарты семейства ISO/IEC 27000. ISO/IEC 27001 задает требования к системе менеджмента информационной безопасности и структуре управления, ISO/IEC 27002 содержит набор практик (контролей), ISO/IEC 27005 описывает подходы к управлению рисками, а ISO/IEC 27007 и ISO/IEC 27008 отражают вопросы проведения аудита и оценки контролей. Использование этих документов позволяет формировать понятные области проверки: управление доступом, управление активами, криптографическая защита, безопасность операций, управление инцидентами, непрерывность и др.

Национальные стандарты и документы в области ИБ дополняют международные подходы с учетом особенностей регулирования и практики применения в Российской Федерации. Они обеспечивают более точную привязку к терминологии и организационным требованиям, включая требования к документации, классификации информации и порядку контроля. Для целей аудита важно, что внутренние документы организации (политики, положения, регламенты) должны быть согласованы с внешними требованиями и непротиворечиво описывать обязанности подразделений и пользователей.

В контексте аудита СОИБ существенную роль играют методы внутреннего контроля и управления соответствием (compliance). Финансово-экономическая организация обычно имеет развитую систему внутреннего контроля, в которую включаются процедуры идентификации рисков, контроля изменений, управления доступом, разделения полномочий, фиксации операций и расследования инцидентов. Поэтому модель аудита СОИБ целесообразно согласовывать с внутренними контрольными процедурами, чтобы результаты аудита были встроены в контур управления и не оставались «отчетом ради

отчета».

Кроме стандартов и требований существенным источником критериев выступают договорные обязательства и требования к подрядчикам. Для финансово-экономических организаций характерны интеграции с внешними сервисами и поставщиками, а также использование облачных и инфраструктурных услуг. Следовательно, аудит должен учитывать короткий перечень ключевых требований к третьим сторонам: разграничение доступа, журналирование действий, уведомление об инцидентах, порядок изменения конфигураций, требования к резервному копированию и обеспечению непрерывности.

Таким образом, нормативно-методическая база определяет «рамку» аудита: какие области должны быть охвачены, какие документы и записи считаются обязательными, и какие критерии могут использоваться для оценки соответствия и результативности. Однако в деструктивных условиях окружающей среды одного соответствия недостаточно: необходима адаптация программы аудита на основе риска и оценка устойчивости процессов, что будет учтено в последующих главах.

1.7. Аудиторская доказательная база и методы получения свидетельств

Для финансово-экономической организации качество аудита определяется не только перечнем проверенных областей, но и качеством доказательной базы. Под аудиторскими свидетельствами (доказательствами) в настоящей работе понимаются сведения, позволяющие обоснованно подтвердить выполнение требований и работоспособность процедур СОИБ. В деструктивных условиях, когда внешняя среда нестабильна, возрастает риск формальной отчетности; поэтому аудит должен опираться на проверяемые артефакты и выборочные проверки, отражающие фактическое выполнение процедур.

Доказательная база формируется из нескольких источников. Документальные свидетельства включают политики, положения, регламенты,

инструкции, планы реагирования и восстановления, модели угроз, результаты оценок рисков, протоколы согласований изменений. Технические свидетельства включают конфигурации средств защиты, настройки политик доступа, выгрузки журналов, отчеты сканирования уязвимостей, результаты тестовых восстановлений, статистику инцидентов и событий безопасности. Интервью и наблюдение используются для подтверждения того, что сотрудники понимают и исполняют процедуры, а также для выявления практик, не отраженных в документах.

С позиции надежности свидетельства могут иметь различную степень доверия. Наиболее надежными являются машинно-генерируемые записи из независимых источников (например, журналы событий, центральный сбор логов, отчеты средств мониторинга), а также результаты контролируемых тестов (например, тестовое восстановление из резервной копии). Менее надежными являются устные объяснения без подтверждающих артефактов и документы, не подтвержденные фактами исполнения. Поэтому в программе аудита целесообразно заранее определять минимально достаточный набор свидетельств для каждой области проверки.

В условиях ограниченных ресурсов важным становится принцип выборочного тестирования. Аудит редко проверяет все объекты полностью; вместо этого применяется выборка: набор пользователей, учетных записей, изменений, инцидентов, систем и журналов за период. Выборка должна быть репрезентативной по критичности: включать ключевые сервисы, привилегированные роли и наиболее рискованные зоны. Правила выборки и ограничения фиксируются в отчете аудита, чтобы результаты были воспроизводимыми и сопоставимыми во времени.

Сопоставление основных видов свидетельств и их надежности приведено в таблице 1.6.

Таблица 1.6 – Виды аудиторских свидетельств и оценка надежности

Вид свидетельства	Примеры	Преимущества	Ограничения/риск

			и
Документальные	Политика ИБ, регламенты, планы DR/IR	Задают требования и ответственность	Могут быть формальными без исполнения
Технические конфигурации	Настройки МЭ, VPN, политики доступа	Показывают фактическую реализацию мер	Требуют экспертизы; возможны исключения
Журналы и отчеты	SIEM/лог-менеджмент, отчеты AV/EDR	Высокая доказательность, отражают факты	Нужны корректные настройки и хранение
Результаты тестов	Тестовое восстановление, учения реагирования	Проверяют работоспособность	Требуют времени и планирования
Интервью/наблюдение	Опрос сотрудников, walkthrough процесса	Выявляют практику и слабые места	Субъективность, нужны подтверждения

1.8. Подходы к оценке рисков информационной безопасности в финансово-экономической организации

Риск-ориентированная модель аудита требует понятного представления о том, как в организации оцениваются и сравниваются риски. В общем виде риск информационной безопасности может быть представлен как сочетание вероятности реализации угрозы, уязвимости объекта и величины потенциального ущерба. Для финансово-экономической организации ущерб часто имеет как прямую финансовую составляющую (потери, мошеннические операции, штрафы), так и косвенную (срыв обязательств, репутационный ущерб, рост оттока клиентов). Поэтому при аудите важно, чтобы оценка рисков учитывала критичность сервисов и данных и была увязана с бизнес-процессами.

На практике применяются качественные, полуколичественные и количественные подходы. Качественная оценка использует словесные шкалы

вероятности и ущерба («низкий», «средний», «высокий») и удобна при ограниченности статистики. Полуколичественный подход задает балльные шкалы (например, 1–4 или 1–5), что позволяет сравнивать риски между областями и выстраивать приоритеты корректирующих действий. Количественная оценка опирается на денежные показатели и вероятностные модели, но требует зрелых данных о частоте событий и ущербе, что доступно не во всех организациях.

Для целей аудита особенно важна воспроизводимость: одинаковые исходные предпосылки должны приводить к сопоставимым оценкам риска. Поэтому целесообразно применять утвержденные шкалы вероятности и ущерба, фиксировать источники данных и экспертные допущения, а также поддерживать реестр активов и рисков. Пример шкал вероятности и ущерба приведен в таблице 1.4.

Использование матрицы рисков позволяет визуально представить приоритеты: риски с высокой вероятностью и высоким ущербом подлежат первоочередной обработке. Пример матрицы рисков для полуколичественной оценки приведен в таблице 1.5. В контексте аудита такая матрица полезна как инструмент планирования: области с наиболее высокими рисками получают большую глубину проверки и более строгие требования к доказательной базе.

В деструктивных условиях окружающей среды риск-оценка должна учитывать изменения контекста: рост атак, ограничения обновлений, кадровые дефициты и зависимость от третьих сторон. Это означает, что риск-профиль организации становится динамичным, а аудит должен использовать актуальные данные за период (инциденты, события, изменения, уязвимости) и корректировать приоритеты проверки.

Шкалы вероятности и ущерба для целей полуколичественной оценки рисков приведены в таблице 1.4.

Таблица 1.4 – Пример шкал вероятности и ущерба для оценки рисков ИБ

Уровень	Вероятность (пример)	Ущерб (пример для

		финорганизации)
Низкий	Редко: единичные случаи за год	Незначительные потери, локальная ошибка без клиентов
Средний	Возможны: несколько случаев за год	Ограниченный ущерб, затрагивает часть операций/клиентов
Высокий	Вероятно: ежемесячно/еженедельно	Существенные потери, простой сервиса, регуляторные последствия
Критический	Почти неизбежно: часто/постоянно	Крупные потери, массовые сбои, серьезные санкции и репутационный ущерб

Пример матрицы рисков на основе указанных шкал приведен в таблице 1.5.

Таблица 1.5 – Пример матрицы рисков (полуколичественная оценка)

	Ущерб: низкий	Ущерб: средний	Ущерб: высокий	Ущерб: критический
Вероятность: низкая	Низкий	Низкий	Средний	Средний
Вероятность: средняя	Низкий	Средний	Высокий	Высокий
Вероятность: высокая	Средний	Высокий	Высокий	Критический
Вероятность: критическая	Средний	Высокий	Критический	Критический

1.9. Модель нарушителя и типовые сценарии угроз для финансово-экономической организации

Построение модели аудита невозможно без определения предполагаемого нарушителя и характерных сценариев угроз. Под нарушителем в данной работе понимается субъект, который способен реализовать угрозы безопасности информации, используя внешние или внутренние возможности. Для финансово-экономических организаций характерна высокая привлекательность

активов для киберпреступных групп, а также наличие внутренних рисков, связанных с ошибками персонала и злоупотреблениями.

Типовые категории нарушителей можно представить следующим образом: внешний нарушитель (киберпреступность, целевые атаки), внутренний нарушитель (сотрудник с легитимным доступом, действующий умышленно), внутренний неумышленный нарушитель (ошибки, невнимательность, социальная инженерия), подрядчик или партнер (доступ через договорные отношения), а также технический фактор (сбой, ошибочная конфигурация), который выступает источником уязвимости и запускает цепочку инцидента.

Для каждой категории нарушителя важны три аспекта: мотивация, уровень доступа и технические возможности. Например, внешний нарушитель может иметь высокую мотивацию и широкий набор технических инструментов, но не имеет легитимного доступа; внутренний нарушитель имеет доступ и знания о процессах; подрядчик может иметь привилегии на обслуживание систем и становится критичной точкой риска, если доступ не ограничен и не контролируется. В деструктивных условиях вероятность эксплуатации социальных и организационных слабостей возрастает, поэтому аудит должен оценивать и человеческий фактор (обучение, дисциплину, контроль доступа).

Примеры категорий нарушителей и типовых сценариев угроз приведены в таблице 1.3.

Таблица 1.3 – Категории нарушителей и типовые сценарии угроз

Категория нарушителя	Уровень доступа	Типовые сценарии	Аудиторский фокус
Внешний киберпреступник	Нет легитимного доступа	Фишинг, атаки на веб/API, подбор учетных данных	MFA, мониторинг, защита веб-контуров, реагирование
Целевая атака (APT)	Стремится к длительному присутствию	Латеральное перемещение, компрометация	Сегментация, контроль привилегий,

		привилегий	обнаружение аномалий
Внутренний умышленный	Легитимный доступ	Выгрузка данных, подмена реквизитов	Разделение полномочий, контроль действий админов
Внутренний неумышленный	Легитимный доступ	Ошибки, открытие вредоносных вложений	Обучение, почтовая защита, минимальные привилегии
Подрядчик/партнер	Часто повышенные права	Компрометация учетных данных подрядчика	Договорные требования, журналы работ, временный доступ

1.10. Информационная инфраструктура и критичные сервисы финансово-экономической организации

Специфика финансово-экономической организации как объекта аудита связана с многоуровневой информационной архитектурой и большим числом интеграций. В типовой инфраструктуре присутствуют фронт-офисные каналы (веб-кабинет, мобильное приложение, терминалы самообслуживания), интеграционные компоненты (шлюзы, процессинг, API-шины), ядро учетных систем (например, автоматизированная банковская система или иные учетные платформы), хранилища и витрины данных, а также подсистемы поддержки (CRM, документооборот, сервис-деск, HR/ERP). Отдельное место занимают системы безопасности: централизованная аутентификация, управление доступом, средства мониторинга и корреляции событий, средства резервного копирования, средства защиты рабочих мест и серверов.

Между указанными компонентами формируются потоки данных, включающие персональные данные клиентов, сведения о счетах и договорах, реквизиты платежей, журналы операций, а также служебные данные аутентификации и авторизации. В условиях деструктивной внешней среды именно интеграционные контуры и дистанционные каналы часто становятся

первичной точкой атаки, поскольку они доступны извне и обрабатывают критичную информацию. Поэтому аудит должен учитывать не только отдельные системы, но и взаимосвязи между ними: где проходят границы доверия, какие каналы защищены, какие журналы собираются и как обеспечивается целостность данных.

Для целей аудита удобно классифицировать сервисы по критичности. Критичными считаются сервисы, нарушение доступности которых приводит к остановке финансовых операций и к невыполнению обязательств; сервисы, компрометация целостности которых может вызвать мошеннические операции или искажение учета; сервисы, компрометация конфиденциальности которых приводит к массовым утечкам данных. В финансово-экономической организации критичность определяется не только объемом данных, но и ролью сервиса в цепочке проведения операций.

Упрощенная схема информационных потоков и зон контроля показана на рисунке 1.1.

Сопоставление ключевых бизнес-процессов, информационных систем и зон аудиторского внимания приведено в таблице 1.2.

Клиентские каналы (веб/моб.)	→	Интеграционный контур (API/шина)	→	Ядро учетных систем (учет)
		↓		↓
Контур безопасности (IAM, MFA, WAF)	→	Мониторинг (SIEM/логи)	→	Хранилища данных (DWH)
		↑		↑
Резервное копирование и восстановление	←	Контроль изменений и уязвимостей	←	Эксплуатация (ИТ/ИБ)

Рисунок 1.1 – Упрощенная схема информационных потоков и зон контроля в финансово-экономической организации

Таблица 1.2 – Связь бизнес-процессов, информационных систем и областей

аудита

Бизнес-процесс	Информационные системы	Ключевые данные/активы	Приоритет аудита
Дистанционное обслуживание	Веб/моб. приложения, API	Учетные данные, сессии, ПДн	Защита каналов, MFA, журналирование
Проведение платежей	Платежный шлюз, процессинг, учетная система	Реквизиты, журналы транзакций	Целостность, контроль реквизитов, мониторинг
Учет и отчетность	Учет, DWH, отчеты	Учетные записи, отчеты	Контроль изменений, целостность, разграничение доступа
Работа с подрядчиками	Сервис-деск, VPN, админ. доступ	Привилегии, конфигурации	Контроль доступа подрядчиков, журналы работ
Восстановление после сбоев	Backup/DR, резервные площадки	Копии данных, планы DR	Тесты восстановления, достижимость RTO/RPO

1.11. Показатели эффективности и индикаторы риска (KPI/KRI) в управлении СОИБ

Для управления СОИБ и для последующего аудита важно иметь набор измеримых показателей. В финансово-экономической организации показатели используются как для внутреннего контроля (оперативный мониторинг), так и для подтверждения результативности мер защиты. В настоящей работе показатели разделяются на KPI (показатели эффективности) и KRI (индикаторы риска). KPI отражают достижение целевых значений процессов (например, доля закрытых уязвимостей в срок), KRI отражают рост риска (например, рост числа успешных фишинговых компрометаций учетных записей).

Применение KPI/KRI в аудите имеет две цели. Во-первых, показатели позволяют оценивать фактическую результативность процессов ИБ и выявлять

деградацию при деструктивных внешних условиях. Во-вторых, показатели формируют основу для сопоставимости между периодами: аудит может фиксировать динамику, а не только состояние на момент проверки. Для обеспечения сопоставимости важно, чтобы показатели имели единое определение, период измерения, источник данных и ответственного владельца.

Типовой набор KPI/KRI для ключевых процессов СОИБ приведен в таблице 1.9. Приведенные показатели могут быть адаптированы под конкретную организацию и ее архитектуру, однако сама логика — измерять устойчивость и управляемость процессов — сохраняется.

Таблица 1.9 – Пример KPI и KRI для ключевых процессов СОИБ финансово-экономической организации

Процесс	KPI (пример)	KRI (пример)	Источник данных
Мониторинг и реагирование	Доля инцидентов, закрытых в SLA; MTTR	Рост повторных инцидентов; рост критичных алертов	SIEM, тикет-система
Управление доступом	Доля пересмотров прав в срок; время отзыва доступа	Рост числа привилегий; рост исключений по MFA	IAM, AD, журналы
Управление уязвимостями	Доля закрытых критичных CVE в срок	Рост просроченных патчей; рост исключений	Сканеры, CMDB
Непрерывность и восстановление	Процент успешных тестов восстановления	Невыполнение RTO/RPO; рост отказов копирования	Backup, DR-отчеты
Третьи стороны	Доля подрядчиков с актуальными требованиями ИБ	Рост инцидентов у подрядчиков; отсутствие отчетов	Договоры, отчеты

1.12. Внутренний контроль, распределение ролей и место аудита ИБ в системе управления организацией

Эффективность аудита СОИБ повышается, если он встроен в систему управления рисками и внутреннего контроля организации. В финансово-экономических организациях обычно используется принцип трех линий защиты: (1) владельцы процессов и подразделения, выполняющие операции (они отвечают за соблюдение правил и первичный контроль); (2) функции управления рисками, комплаенс и информационная безопасность (они устанавливают требования, методики и осуществляют мониторинг); (3) внутренний аудит (он предоставляет независимую оценку соответствия и эффективности контроля). Такая структура снижает риск конфликта интересов и обеспечивает независимость выводов.

Для практической применимости модели аудита важно заранее определить роли и ответственность. В аудите ИБ участвуют: руководство организации (утверждение политики и риск-аппетита), подразделение ИБ (владельцы требований и процедур), ИТ-служба (эксплуатация инфраструктуры), владельцы бизнес-процессов (определение критичности активов), служба внутреннего аудита (планирование и проведение независимых проверок) и внешние подрядчики (если часть функций вынесена). В условиях деструктивной внешней среды особенно важны роли реагирования на инциденты и управления изменениями, поскольку именно здесь проявляются наиболее критичные сбои управляемости.

Для формализации распределения ролей часто применяют матрицу ответственности RACI (Responsible, Accountable, Consulted, Informed). В аудите СОИБ матрица RACI помогает определить, кто отвечает за предоставление доказательств, кто утверждает результаты, кто участвует в корректирующих действиях и кто получает отчеты. Пример укрупненной матрицы RACI для ключевых процессов приведен в таблице 1.8.

Согласование ролей и ответственности уменьшает сопротивление аудиту и снижает вероятность того, что выявленные несоответствия останутся без корректирующих действий. Следовательно, включение элементов управления (governance) в модель аудита является необходимым условием ее эффективности.

Таблица 1.8 – Пример матрицы RACI для ключевых процессов СОИБ

Процесс/функция	ИБ	ИТ	Бизнес-владелец	Внутренний аудит
Управление доступом	A	R	C	C
Мониторинг и реагирование	A/R	C	I	C
Уязвимости и изменения	C	A/R	I	C
Резервное копирование/DR	C	A/R	C	C
Контроль подрядчиков	A/R	C	C	C
Утверждение планов улучшений	C	C	A	I

1.13. Оценка зрелости процессов СОИБ как элемент аудита

Проверка соответствия требованиям показывает наличие или отсутствие отдельных мер, однако не всегда позволяет оценить устойчивость процессов во времени. Для того чтобы результаты аудита были управленчески полезными, в практике применяется оценка зрелости процессов. Под зрелостью в данной работе понимается степень формализованности, управляемости и воспроизводимости процесса ИБ, а также наличие механизмов контроля и улучшения.

Оценка зрелости позволяет: (1) сравнивать подразделения и процессы между собой; (2) отслеживать динамику улучшений от периода к периоду; (3) обосновывать приоритеты инвестиций в ИБ; (4) выявлять процессы, которые

формально существуют, но не дают результата в условиях нагрузки. В деструктивных условиях зрелость приобретает особую ценность, поскольку именно незрелые процессы «ломаются» первыми: мониторинг становится нерегулярным, изменения выполняются без контроля, восстановление не достигает целевых параметров.

В настоящей работе предлагается использовать укрупненную пятиуровневую шкалу зрелости: 0 – отсутствует/хаотично; 1 – начальный (есть отдельные меры, но нет регулярности); 2 – повторяемый (процедуры выполняются по правилам, но контроль ограничен); 3 – управляемый (есть метрики, ответственность, регулярный контроль); 4 – оптимизируемый (процесс улучшается на основе анализа данных, автоматизация). Пример описания уровней приведен в таблице 1.7.

В аудите шкала зрелости применяется совместно с критериями соответствия и результативности. Например, процесс может соответствовать требованиям (есть регламент), но иметь низкую зрелость (нет метрик и контроля), что в деструктивных условиях повышает риск. Соответственно, итоговый вывод по процессу должен учитывать все три измерения: соответствие, результативность и зрелость/устойчивость.

Таблица 1.7 – Укрупненная шкала зрелости процессов СОИБ для целей аудита

Уровень	Характеристика	Признаки в доказательствах
0 – отсутствует	Процесс не определен, действия хаотичны	Нет регламентов, нет записей выполнения
1 – начальный	Есть отдельные меры, нерегулярное выполнение	Разрозненные документы, единичные записи
2 – повторяемый	Процедуры выполняются по правилам	Регламенты, журналы выполнения, но мало метрик
3 – управляемый	Есть ответственность, метрики, контроль	SLA, отчеты, регулярные проверки, улучшения по итогам
4 – оптимизируемый	Процесс улучшается на	Автоматизация, тренды

	основе анализа	KPI/KRI, постоянное улучшение

1.14. Выводы по главе 1 и постановка задачи выпускной квалификационной работы

Дополнительно в главе 1 обоснована роль оценки зрелости процессов СОИБ (таблица 1.7), рассмотрены вопросы управления и распределения ответственности в контуре внутреннего контроля (таблица 1.8), а также предложен набор KPI/KRI для мониторинга устойчивости процессов (таблица 1.9). Эти элементы используются как критерии и показатели в модели аудита, разрабатываемой в главе 3.

Дополнительно в главе 1 уточнены особенности информационной инфраструктуры финансово-экономической организации (рисунок 1.1, таблица 1.2), предложена модель нарушителя и типовые сценарии угроз (таблица 1.3), рассмотрены подходы к оценке рисков и инструменты приоритизации (таблицы 1.4–1.5), а также требования к доказательной базе аудита (таблица 1.6). Это усиливает теоретическую основу для разработки модели аудита в главе 3.

Анализ предметной области показал, что финансово-экономическая организация является объектом с повышенной критичностью информационных активов и высокими требованиями к управляемости процессов. Для таких организаций значимы не только формальная реализация мер защиты, но и их результативность, а также наличие доказательной базы выполнения регламентов.

Установлено, что традиционные контрольные подходы к аудиту, ориентированные преимущественно на проверку соответствия, обладают ограниченной применимостью в условиях динамично изменяющейся внешней среды. В деструктивных условиях возрастает потребность в приоритизации проверок по рискам, в оценке устойчивости процессов ИБ, а также в сопоставимых метриках, позволяющих отслеживать развитие СОИБ во

времени.

К основным недостаткам типовой практики аудита СОИБ, препятствующим получению управленчески значимых результатов в деструктивных условиях, относятся: недостаточная формализация учета внешних факторов и их влияния на риски; отсутствие единых критериев оценки устойчивости мер защиты; ограниченное применение шкал зрелости процессов; разнородность отчетных форм, затрудняющая сравнение аудитов между периодами.

С учетом выявленных недостатков постановка задачи настоящей выпускной квалификационной работы заключается в разработке теоретической модели аудита системы обеспечения информационной безопасности финансово-экономической организации, ориентированной на риск-ориентированное планирование и учитывающей влияние деструктивных условий окружающей среды. Модель должна определять состав входных данных и аудиторских артефактов, этапы аудита и распределение ролей, критерии оценки соответствия, результативности и устойчивости, шкалу зрелости процессов ИБ, а также правила классификации несоответствий и формирования рекомендаций, обеспечивающих воспроизводимость и практическую применимость результатов.

ГЛАВА 2. ДЕСТРУКТИВНЫЕ УСЛОВИЯ ОКРУЖАЮЩЕЙ СРЕДЫ И ТРЕБОВАНИЯ К АУДИТУ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1. Понятие и классификация деструктивных условий окружающей среды

В рамках настоящей выпускной квалификационной работы под деструктивными условиями окружающей среды понимается совокупность факторов внешней среды, которые повышают вероятность реализации угроз информационной безопасности и/или снижают способность организации поддерживать устойчивое функционирование системы обеспечения информационной безопасности (СОИБ). В отличие от обычной неблагоприятной обстановки деструктивные условия характеризуются устойчивым или резким ухудшением нескольких параметров одновременно: ростом активности нарушителей, повышением неопределенности, дефицитом ресурсов и усложнением зависимостей организации от внешних участников (поставщиков, подрядчиков, инфраструктурных операторов).

Для целей аудита важно, что внешняя среда влияет не только на набор угроз, но и на надежность предпосылок, на которых строится СОИБ: доступность обновлений и поддержки, возможность оперативного восстановления, обеспеченность квалифицированными кадрами, предсказуемость требований внешнего контроля. Поэтому в деструктивных условиях в качестве объекта оценки выступают не только отдельные технические меры, но и устойчивость процессов ИБ, способность организации поддерживать приемлемый уровень риска при внешних воздействиях.

Классификацию деструктивных факторов целесообразно выполнять по их природе и каналу влияния. В данной работе предлагается выделять пять укрупненных групп факторов: (1) угрозовые (киберпреступность, целевые атаки, рост фишинга и атак на дистанционные каналы); (2) регуляторно-правовые (изменение требований и ответственности, усиление внешнего

контроля); (3) технологические (сложность архитектуры, зависимость от компонентов и поддержки, дефицит обновлений и патчей, рост технического долга); (4) организационно-кадровые (дефицит специалистов, текучесть персонала, снижение дисциплины исполнения процедур); (5) инфраструктурные и партнерские (подрядчики, облачные сервисы, провайдеры связи, цепочки поставок).

Указанные факторы могут действовать одновременно и взаимно усиливать друг друга. Например, рост кибератак при кадровом дефиците снижает качество мониторинга и реагирования, а технологические ограничения увеличивают окно уязвимости. В таких условиях аудит должен выявлять не только отсутствие отдельных мер, но и слабые места устойчивости, которые проявятся при ухудшении внешней обстановки.

Укрупненная классификация деструктивных факторов окружающей среды приведена на рисунке 2.1.

Группа факторов	Примеры проявлений
Угрозовые, технологические	Рост атак; задержка патчей; усложнение архитектуры
Регуляторные, организационные, партнерские	Изменение требований; дефицит кадров; риски подрядчиков и провайдеров

Рисунок 2.1 – Укрупненная классификация деструктивных факторов окружающей среды

Для формализации учета деструктивных условий в аудите целесообразно описывать их через набор индикаторов (например, интенсивность внешних атак, частота выявления критических уязвимостей, доля критичных сервисов у внешних поставщиков, кадровая обеспеченность функций ИБ). Такая формализация позволяет сформировать профиль контекста аудита и использовать его при выборе области и глубины проверок, а также при интерпретации выявленных несоответствий.

Пример формализации контекста аудита с использованием индикаторов

приведен в таблице 2.2.

Таблица 2.2 – Пример профиля контекста аудита СОИБ (индикаторы деструктивных условий)

Индикатор	Шкала (0–3)	Интерпретация	Как влияет на программу аудита
Интенсивность внешних атак	0 — фоновая; 1 — умеренная; 2 — высокая; 3 — критическая	Оценивается по статистике инцидентов/событий за период	Увеличить долю проверок мониторинга и реагирования; выборки журналов
Окно уязвимости (патчи)	0 — ≤14 дн.; 1 — 15–30 дн.; 2 — 31–60 дн.; 3 — >60 дн.	Отражает доступность обновлений и скорость их внедрения	Сфокусировать аудит на управлении уязвимостями и компенсирующих мерах
Зависимость от подрядчиков	0 — низкая; 1 — средняя; 2 — высокая; 3 — критическая	Доля критичных сервисов у внешних поставщиков	Проверить договорные требования, доступ подрядчиков, контроль изменений
Кадровая обеспеченность ИБ	0 — достаточная; 1 — ограниченная; 2 — дефицит; 3 — критический дефицит	Соотношение задач и доступных специалистов	Упростить доказательную базу, проверять ключевые процессы на устойчивость и передачу ответственности

2.2. Влияние деструктивных условий на риски и функционирование СОИБ

Воздействие деструктивных факторов отражается на рисках информационной безопасности через изменение вероятности реализации угроз и/или изменение величины потенциального ущерба. Для финансово-

экономической организации характерно наличие высокоценных активов (данные клиентов и операций, учетные записи с привилегиями, ключевая информация), что повышает мотивацию нарушителя. Одновременно растет ущерб, поскольку сбой ключевых сервисов или компрометация данных влияет на выполнение обязательств перед клиентами и на устойчивость финансовых операций.

Влияние внешней среды проявляется также через снижение эффективности традиционных контуров защиты. При усложнении инфраструктуры и наличии наследуемых систем возрастает вероятность ошибок конфигурации и скрытых уязвимостей. При ограничениях на обновления увеличивается период эксплуатации известных уязвимостей. При кадровом дефиците снижается качество администрирования и мониторинга, увеличивается время реагирования на инциденты. В результате даже формально внедренные средства защиты могут не обеспечивать требуемого уровня безопасности.

С точки зрения управления ИБ в деструктивных условиях возрастает роль процессной устойчивости. Организация должна иметь возможность: быстро переоценивать риски и приоритеты защиты; обнаруживать события безопасности и инциденты в приемлемые сроки; реагировать с заданными уровнями сервиса; восстанавливать работоспособность критичных систем; обеспечивать доказуемость выполнения требований. При отсутствии этих возможностей СОИБ становится реактивной и утрачивает способность поддерживать приемлемый уровень риска.

Для задач аудита важно, что перечисленные эффекты не всегда выявляются при поверхностной проверке соответствия. Например, наличие регламента резервного копирования не гарантирует достижение целевых показателей восстановления, если не проводятся тестовые восстановления или если резервные копии не защищены от модификации. Аналогично, наличие журналирования не обеспечивает обнаружение атак, если события не

централизованы и отсутствуют процедуры реагирования. Следовательно, аудит должен оценивать не только наличие мер, но и их результативность и устойчивость.

Соответствие деструктивных факторов, их влияния на риск и приоритетов аудита приведено в таблице 2.1.

Таблица 2.1 – Влияние деструктивных факторов на аудит СОИБ и приоритеты проверок

Фактор	Как влияет на риск	Что проверять в аудите	Признак проблемы
Рост кибератак	Повышение вероятности инцидентов	Мониторинг, реагирование, защита каналов, контроль доступа	Нет корреляции событий; длительное время реагирования
Ограничения обновлений	Увеличение окна уязвимости	Управление уязвимостями, компенсирующие меры	Нет реестра уязвимостей; отсутствуют планы закрытия
Кадровый дефицит	Ошибки и нарушения процедур	Распределение ролей, обучение, контроль изменений	Нет владельцев процессов; ручные действия без учета
Риски подрядчиков	Компрометация через цепочку поставок	Договорные требования, контроль доступа подрядчиков	Нет требований в договорах; отсутствуют журналы работ
Рост нагрузки/сбоев	Потеря доступности сервисов	Непрерывность, резервирование, тесты восстановления	Нет тестов DR; невыполнимые RTO/RPO

2.3. Особенности аудита информационной безопасности в деструктивных условиях

Особенности аудита СОИБ в деструктивных условиях обусловлены тем, что традиционный аудит соответствия, опирающийся на фиксированный перечень требований, не учитывает изменчивость угроз и ограниченность ресурсов. При таком подходе организация может получать формально

корректные результаты при наличии существенных рисков, которые не попали в фокус проверки. Следовательно, ключевым принципом аудита становится риск-ориентированная приоритизация процедур.

В деструктивных условиях аудит должен выполнять две функции: подтверждать базовый уровень соответствия установленным требованиям и выявлять уязвимости устойчивости и управляемости, которые проявятся при ухудшении внешней среды. Для реализации второй функции необходимы дополнительные критерии оценки, связанные с устойчивостью процессов: непрерывность мониторинга, управляемость изменений, способность к восстановлению, устойчивость управления доступом при росте числа пользователей и внешних взаимодействий.

Практической особенностью является необходимость проведения аудита в условиях ограничений: нехватка времени, дефицит экспертов, неполные или разрозненные данные, высокая нагрузка на ИТ-службы. Поэтому модель аудита должна предусматривать минимально достаточный набор входных данных и правила формирования доказательной базы: какие документы и журналы обязательны, какие контрольные выборки достаточны, какие интервью и проверки дают максимальную ценность.

В деструктивных условиях повышается значение повторяемости и сопоставимости результатов аудита. Организация должна иметь возможность сравнивать результаты проверок за разные периоды, отслеживать динамику зрелости процессов и эффективности мер, а также фиксировать влияние внешних факторов на риски. Это требует стандартизации отчетных форм, единого классификатора несоответствий и единого подхода к оценке критичности выявленных проблем.

2.4. Требования к модели аудита СОИБ, адаптированной к деструктивным условиям

На основе рассмотренных факторов и их влияния формируются требования к модели аудита СОИБ, применимой в финансово-экономической

организации в деструктивных условиях окружающей среды. Модель должна обеспечивать риск-ориентированное планирование аудита, формализованное описание этапов и артефактов, а также получение воспроизводимых результатов, пригодных для принятия управленческих решений.

Во-первых, модель должна включать механизм учета внешних факторов. Для этого целесообразно вводить входной блок «контекст аудита», включающий описание актуальных деструктивных факторов, их интенсивности и каналов влияния на риски. На основе контекста формируется приоритизация проверок: какие области аудита являются критичными в текущем периоде (например, дистанционные каналы обслуживания, управление привилегиями, мониторинг и реагирование).

Во-вторых, модель должна задавать структуру доказательной базы: перечень обязательных документов и записей, подтверждающих выполнение ключевых процедур. К таким артефактам относятся политика ИБ, регламенты управления доступом, журналы событий и обращений, результаты оценки рисков, планы резервного копирования и восстановления, отчеты о тестовых восстановительных мероприятиях, документы по управлению подрядчиками. Наличие артефактов без их фактического применения должно рассматриваться как фактор риска.

В-третьих, модель должна включать критерии оценки, разделенные на три группы: соответствие, результативность и устойчивость. Для каждой группы критериев должны быть определены показатели и шкалы. Это позволит сопоставлять результаты аудита между периодами и формировать дорожную карту развития СОИБ.

В-четвертых, модель должна предусматривать классификацию несоответствий по критичности, основанную на риске. Для финансово-экономической организации целесообразно применять ранжирование, учитывающее влияние на ключевые сервисы и активы, вероятность эксплуатации и наличие компенсирующих мер. Такое ранжирование

необходимо для формирования приоритезированного плана корректирующих действий.

Модель должна быть реализуема в условиях ограниченных ресурсов. Поэтому в ней следует определить минимально достаточные процедуры (базовый контур аудита), а также расширенные процедуры для углубленной проверки при наличии времени и данных. Это обеспечивает регулярность аудита даже при ухудшении внешней обстановки.

2.5. Сценарный анализ: проявление деструктивных условий и точки контроля аудита

Сценарный анализ используется для того, чтобы связать абстрактные факторы внешней среды с конкретными проверками в аудите. В рамках ВКР под сценарием понимается типовая ситуация, при которой внешние условия приводят к росту риска и требуют усиления определенных процедур контроля. Применение сценариев позволяет уточнять программу аудита, формировать выборки доказательств и задавать критерии оценки устойчивости.

Сценарий 1 «Рост атак на дистанционные каналы обслуживания». При увеличении числа фишинговых рассылок, атак на учетные записи и попыток подмены платежных реквизитов аудит должен уделить приоритетное внимание управлению доступом и аутентификацией, мониторингу событий, защите веб-контуров и API, а также процедурам реагирования на инциденты. В качестве доказательств используются журналы аутентификации и подозрительных событий, регламенты реагирования, результаты расследований, сведения о правилах корреляции и времени реакции. Признаками проблем выступают отсутствие единого контура мониторинга, несогласованность ролей при реагировании, недостаточная защищенность сервисных учетных записей.

Сценарий 2 «Ограничения на обновления и рост окна уязвимости». При отсутствии своевременных патчей или невозможности обновления критичных систем возрастает вероятность эксплуатации известных уязвимостей. Аудит в

этом случае должен проверять наличие реестра активов и версий, процедуры управления уязвимостями, наличие компенсирующих мер (сегментация, ограничение сетевых взаимодействий, усиление мониторинга), а также контроль изменений. Критичным признаком является отсутствие планов закрытия уязвимостей и неформализованный учет исключений, когда устаревшие компоненты используются без управления остаточным риском.

Сценарий 3 «Нестабильность работы подрядчика/провайдера». При высокой зависимости от внешних сервисов риск может реализоваться как компрометация через цепочку поставок или как потеря доступности. В аудите проверяются договорные требования к безопасности, порядок предоставления и отзыва доступа подрядчикам, журналирование работ, процедуры согласования изменений, а также планы обеспечения непрерывности и альтернативные каналы/поставщики. Признаками проблем являются отсутствие регламентов взаимодействия, отсутствие журналов работ и контроля действий, а также непротестированные планы восстановления.

Сценарий 4 «Кадровый дефицит и рост ошибок эксплуатации». Недостаток специалистов приводит к снижению качества администрирования, задержкам в реагировании и ошибкам конфигураций. Аудит должен проверять распределение ответственности (RACI), наличие инструкций и стандартов конфигурации, контроль изменений, обучение и аттестацию персонала, а также механизмы технического контроля (например, централизованные политики, автоматизация проверок конфигураций). В качестве признаков проблем выступают «ручные» операции без регистрации, отсутствие владельцев процессов, рост числа повторяющихся инцидентов и отклонений.

Рассмотренные сценарии демонстрируют, что в деструктивных условиях аудит должен «переключаться» на наиболее значимые зоны риска. Следовательно, модель аудита должна содержать правила выбора приоритетов проверки, минимальный набор доказательств и критерии, позволяющие оценить устойчивость процедур при ухудшении внешнего контекста.

2.6. Показатели устойчивости и метрики для оценки аудита в деструктивных условиях

Оценка СОИБ в деструктивных условиях требует использования показателей, которые отражают не только наличие мер защиты, но и их устойчивую работоспособность. Под показателями устойчивости в данной работе понимаются измеримые характеристики, позволяющие судить о способности процессов ИБ сохранять результативность при росте нагрузки, усложнении атак и ограниченности ресурсов. Введение таких показателей повышает сопоставимость результатов аудита между периодами и обеспечивает переход от описательных выводов к управляемым улучшениям.

К группе показателей обнаружения и реагирования относятся: полнота журналирования событий (доля критичных систем, передающих события в единый контур), задержка доставки событий, доля событий с корректной категоризацией, среднее время обнаружения (MTTD) и реагирования (MTTR), доля инцидентов, завершенных в целевые сроки, наличие и актуальность плейбуков реагирования. Для финансово-экономических организаций эти показатели особенно важны в связи с высокой частотой атак на учетные записи и дистанционные сервисы.

К группе показателей управления доступом и привилегиями относятся: доля учетных записей с повышенными правами, покрытых процедурами регулярного пересмотра; доля привилегированных действий, подлежащих журналированию и контролю; выполнение принципа минимальных привилегий; использование многофакторной аутентификации для критичных ролей; время отзыва доступа при увольнении или смене роли. В аудите данные показатели дополняются выборочной проверкой заявок, согласований и фактических прав в системах.

К группе показателей управления уязвимостями и изменениями относятся: среднее окно устранения критичных уязвимостей, доля систем с просроченными обновлениями, доля изменений, оформленных по регламенту,

доля изменений с оценкой влияния на безопасность, наличие списка исключений и компенсирующих мер. В деструктивных условиях важно фиксировать причины невозможности обновления и наличие управляемого остаточного риска.

К группе показателей непрерывности и восстановления относятся: достижимость целевых параметров восстановления (RTO/RPO) для критичных сервисов, частота и результаты тестовых восстановлений, защита резервных копий от модификации, наличие альтернативных площадок/каналов, доля критичных сервисов с актуальными планами восстановления. Для финансово-экономической организации данные показатели позволяют оценивать устойчивость к сбоям и атакам, нацеленным на нарушение доступности.

В практическом применении показатели устойчивости целесообразно использовать в двух режимах: (1) как критерии проверки в аудите (наличие измерений и их целевых значений); (2) как основание для классификации несоответствий (отклонение метрики от цели соответствует более высокой критичности). Такой подход делает результаты аудита управляемыми и обеспечивает основу для формирования корректирующих мероприятий.

2.7. Минимальный контур аудита при ограниченных ресурсах

В деструктивных условиях окружающей среды проведение аудита осложняется нехваткой времени и экспертов, высокой нагрузкой на ИТ-службы и неполнотой данных. Полный аудит всех областей может быть практически невозможен, однако прекращение аудита приводит к накоплению рисков и снижению управляемости. Поэтому модель должна предусматривать минимальный контур аудита — набор обязательных проверок, который обеспечивает базовую оценку защищенности и выявляет критичные несоответствия.

Минимальный контур строится по принципу «критичные активы — критичные процессы — критичные контуры управления». В финансово-экономической организации к таким контурам относятся: управление доступом

и привилегиями, мониторинг и реагирование на инциденты, управление уязвимостями и изменениями, резервное копирование и восстановление, контроль подрядчиков и внешних доступов, защита дистанционных каналов обслуживания. Эти области дают наибольший эффект по снижению риска даже при ограниченной глубине проверки.

Для ускорения аудита применяются пакеты доказательств — заранее согласованные выгрузки и отчеты за период (например, список привилегированных учетных записей, отчеты о закрытии уязвимостей, отчеты SIEM по инцидентам, результаты тестовых восстановлений). Такой подход снижает нагрузку на подразделения и делает аудит регулярным.

Состав минимального контура аудита и рекомендуемые трудозатраты приведены в таблице 2.5.

Таблица 2.5 – Минимальный контур аудита СОИБ в условиях ограниченных ресурсов

Модуль аудита	Ключевые доказательства	Результат проверки	Оценка трудозатрат
Управление доступом	Список привилегий, выборка заявок/согласований, отчеты IAM	Корректность выдачи/отзыва прав	Средние
Мониторинг и реагирование	Отчеты SIEM, плейбуки, выборка инцидентов	Оценка MTTD/MTTR, готовность реагирования	Высокие
Уязвимости и изменения	Отчеты сканирования, реестр исключений, CR-заявки	Окно устранения, контроль изменений	Средние
Резервное копирование	Политика backup, отчеты успешности, тест DR	Достижимость RTO/RPO, защита копий	Средние
Подрядчики и внешние доступы	Договоры, журналы работ, VPN-доступ	Контроль доступа третьих лиц	Низкие–средние
Дистанционные каналы	WAF/защита веб, MFA, отчеты	Устойчивость внешнего	Средние

	атак/блокировок	контура	

2.8. Матрица требований к модели аудита и критерии приемки

Для того чтобы модель аудита могла быть использована в организации и служила основанием для регулярных проверок, необходимо сформулировать требования к ее содержанию и результатам. В рамках данной работы требования делятся на функциональные (что модель должна обеспечивать) и нефункциональные (какими свойствами должна обладать модель).

К функциональным требованиям относятся: наличие входного блока «контекст аудита» (учет деструктивных факторов), формирование программы аудита с приоритизацией областей, определение набора доказательств и артефактов, применение критериев оценки соответствия, результативности и устойчивости, использование шкалы зрелости процессов, классификация несоответствий по критичности и формирование рекомендаций. К нефункциональным требованиям относятся: воспроизводимость результатов, сопоставимость между периодами, реализуемость при ограниченных ресурсах, прозрачность логики ранжирования и возможность интеграции с внутренним контролем организации.

Пример матрицы требований с критериями приемки приведен в таблице 2.4.

Таблица 2.4 – Матрица требований к модели аудита СОИБ в деструктивных условиях

Требование	Обоснование	Критерий приемки
Учет внешнего контекста	Риски меняются при росте угроз и ограничениях	Есть профиль контекста и правила влияния на план аудита
Риск-ориентированная приоритизация	Ресурсы аудита ограничены	Программа аудита ранжирует

		области по риску и критичности
Доказательная база	Нужна подтверждаемость выводов	Определен минимум артефактов по каждой области
Критерии: соответствие/результативность/устойчивость	Соответствие не гарантирует устойчивости	Есть показатели и шкалы по 3 группам
Шкала зрелости	Нужна динамика улучшений	Определены уровни зрелости и правила присвоения
Классификация несоответствий	Нужно управлять устранением	Есть уровни критичности и связь с рисками
Реализуемость	Аудит проводится регулярно	Есть минимальный контур аудита и оценка трудозатрат

2.9. Механизм адаптации программы аудита к контексту деструктивных условий

Ключевым элементом модели аудита в деструктивных условиях является механизм адаптации: правила, по которым меняется программа аудита при изменении внешнего контекста. Такой механизм позволяет отказаться от одинаковой глубины проверок и перейти к управляемой приоритизации: на какие области направить усилия в текущем периоде, какие доказательства собрать и какие выборки расширить.

В качестве входных данных используется профиль контекста аудита (таблица 2.2), где деструктивные факторы описываются через индикаторы и

шкалы. Далее контекст преобразуется в набор приоритетов областей аудита. Например, при высокой интенсивности атак повышается приоритет мониторинга, управления доступом и защиты дистанционных каналов; при увеличении окна уязвимости — приоритет управления уязвимостями и контроля изменений; при высокой зависимости от подрядчиков — приоритет управления доступом третьих сторон и договорного контроля.

Механизм адаптации может быть описан как последовательность шагов: сбор контекстных индикаторов; определение критичных активов и сервисов; расчет приоритетов областей аудита; выбор базового или расширенного набора процедур; формирование плана доказательств и выборок; выполнение аудита и классификация несоответствий; формирование рекомендаций и плана улучшений. Укрупненный алгоритм представлен на рисунке 2.2.

Пример набора правил приоритизации проверок приведен в таблице 2.3.

Сбор контекста (индикаторы)	→	Критичные активы и сервисы	→	Приоритизация областей
		↓		↓
Выбор процедур (база/расшир.)	→	Доказательства и выборки	→	Оценка и выводы
		↓		↓
Рекомендации и план	←	Отчет (метрики, зрелость)	←	Контроль корр. действий

Рисунок 2.2 – Укрупненный алгоритм адаптации программы аудита СОИБ к внешнему контексту

Таблица 2.3 – Пример правил адаптации программы аудита к деструктивным условиям

Контекстный фактор (пример)	Приоритетные области аудита	Как усиливается проверка
Интенсивность атак = высокая	Мониторинг, реагирование, защита веб/API	Расширить выборку событий и инцидентов; проверить плейбуки

Окно уязвимости = критическое	Уязвимости, изменения, сегментация	Проверить исключения и компенсирующие меры; контроль изменений
Зависимость от подрядчиков = высокая	Третьи стороны, доступ, договоры	Проверить журналы работ, временный доступ, условия договора
Кадровая обеспеченность = дефицит	Эксплуатация, контроль процедур	Оценить устойчивость процессов, автоматизацию, RACI
Сбой/нагрузка = высокая	Непрерывность, восстановление	Проверить тесты DR, достижимость RTO/RPO, защиту резервных копий

2.10. Отчет аудита и план корректирующих действий в условиях деструктивной среды

Ценность аудита определяется тем, насколько его результаты могут быть использованы для управления рисками. В деструктивных условиях отчет аудита должен быть максимально прикладным: содержать не только перечень несоответствий, но и оценку критичности, возможные последствия, приоритеты устранения и измеримые корректирующие действия. При высокой нагрузке на организацию важны краткость и однозначность формулировок: что нужно сделать, кто отвечает, к какому сроку и как будет проверяться выполнение.

Структура отчета обычно включает: (1) цель и область аудита, контекст (деструктивные факторы), используемые критерии; (2) краткое резюме состояния СОИБ; (3) перечень выявленных несоответствий и наблюдений, сгруппированных по областям; (4) оценку зрелости процессов и ключевые метрики; (5) рекомендации и план корректирующих действий (CAPA). В деструктивных условиях целесообразно добавлять раздел «риски устойчивости», где фиксируются уязвимости, проявляющиеся при росте нагрузки (например, отсутствие тестов восстановления или зависимость от единственного подрядчика).

План корректирующих действий должен быть приоритезирован по критичности и по эффекту на снижение риска. Для этого несоответствия

классифицируются по уровням: критические, высокие, средние, низкие. Для каждого уровня задаются рекомендуемые сроки устранения и необходимость компенсирующих мер. Пример классификации и шаблона плана действий приведен в таблице 2.8.

Укрупненная логика формирования отчета и контроля выполнения корректирующих мероприятий показана на рисунке 2.3. Данный элемент будет использован в главе 3 при описании выходных артефактов модели аудита.

Результаты проверок (доказательства)	→	Формулировка несоответствий	→	Оценка критичности (по риску)
		↓		↓
Рекомендации и меры	→	План CAPA (сроки/ответст.)	→	Контроль выполнения и повторный аудит

Рисунок 2.3 – Формирование отчета аудита и контроль корректирующих действий

Таблица 2.8 – Пример классификации несоответствий и структуры плана корректирующих действий

Уровень	Критерий	Рекомендуемый срок	Пример CAPA
Критический	Высокая вероятность + высокий ущерб	Немедленно/до 30 дней	Ввести компенсирующие меры, устранить первопричину
Высокий	Значимый риск без компенсаторов	До 60 дней	Исправить конфигурации, усилить мониторинг, обновить регламенты
Средний	Риск ограничен или есть частичные компенсаторы	До 90 дней	Оптимизировать процесс, внедрить метрики, обучить персонал
Низкий	Низкий	Планово	Уточнить

	ущерб/вероятность		документацию, улучшить отчетность

2.11. Риски третьих сторон и цепочки поставок: требования к аудиту в деструктивных условиях

Зависимость финансово-экономических организаций от третьих сторон постоянно растет: используются облачные платформы, сервисы связи, внешние платежные провайдеры, разработчики и подрядчики по сопровождению. В деструктивных условиях риски третьих сторон усиливаются: доступность услуг может снижаться, повышается вероятность компрометации учетных данных подрядчика, а также риск внедрения уязвимостей через обновления и поставляемые компоненты.

Аудит СОИБ должен включать проверку управления рисками третьих сторон: наличие реестра подрядчиков и критичности услуг, требования к информационной безопасности в договорах, порядок предоставления и отзыва доступа, ограничения по времени и по привилегиям, контроль действий подрядчиков, уведомление об инцидентах и порядок совместного реагирования. Существенным элементом является контроль изменений: какие изменения подрядчик может выполнять без согласования, как фиксируются изменения, как обеспечивается возможность отката и расследования.

В деструктивных условиях отдельным направлением проверки становится устойчивость к сбоям подрядчика: наличие альтернативных поставщиков, возможность переключения, резервирование каналов, перенос критичных функций внутрь организации. Для финансового сектора важны также требования по хранению данных, по журналированию и по доступу к доказательствам в случае инцидента. Практический чек-лист аудита третьих сторон приведен в таблице 2.7.

Таблица 2.7 – Чек-лист аудита управления рисками третьих сторон

Область	Что проверять	Примеры доказательств

Реестр подрядчиков	Критичность услуг и данных	Реестр, классификация, SLA
Договорные требования	ИБ-требования, инциденты, аудит	Договор, приложения, отчеты
Доступ и привилегии	Временный доступ, MFA, журналирование	Списки доступов, логи, заявки
Контроль изменений	Согласование, тестирование, откат	CR-тикеты, протоколы, планы
Непрерывность	Альтернативы, резервирование, DR подрядчика	Планы DR, тесты, отчеты

2.12. Оценка устойчивости контролей: метрики и стресс-тестирование

Рассмотрение устойчивости СОИБ в деструктивных условиях предполагает проверку того, как контуры защиты работают при повышенной нагрузке, при неполноте данных и при ограниченных ресурсах. В дополнение к стандартной проверке соответствия полезно применять элементы стресс-тестирования контролей: контролируемые проверки или моделирование ситуаций, близких к реальным сценариям атак и сбоев. Цель стресс-тестирования — выявить скрытые ограничения (например, недостаточную производительность мониторинга, невозможность восстановления в целевые сроки, отсутствие готовности к массовым компрометациям учетных записей).

Стресс-тестирование может быть организовано без разработки кода: через анализ реальных инцидентов за период, проведение настольных учений (table-top) по реагированию, выборочные проверки процедур восстановления, проверку доступа подрядчиков и имитацию типовых сценариев (например, «потеря доступности внешнего провайдера»). Важно фиксировать критерии успеха (SLA, RTO/RPO, время реакции) и источники данных, подтверждающие результаты.

Связь типовых стресс-сценариев с объектами аудита и ожидаемыми критериями приведена в таблице 2.6. Использование таких сценариев повышает

доказательность аудита и помогает обосновывать приоритеты корректирующих действий.

Таблица 2.6 – Примеры стресс-сценариев для проверки устойчивости СОИБ

Сценарий	Что проверяется	Критерий/метрика
Массовый фишинг	Готовность реагирования, MFA, обучение	Рост успешных входов; время блокировки учетных записей
Эксплуатация критичной уязвимости	Процесс патч-менеджмента, компенсаторы	Окно устранения; наличие сегментации и мониторинга
Сбой провайдера/подрядчика	Непрерывность, альтернативы	Время переключения; достижимость RTO
Ransomware/шифрование	Резервные копии, восстановление	Успешность восстановления; RPO
Компрометация привилегий	PAM/IAM, контроль администраторов	Наличие журналов; пересмотр прав; аномалии

2.13. Выводы по главе 2

Дополнительно в главе 2 предложены: механизм адаптации программы аудита к внешнему контексту (рисунок 2.2), набор правил приоритизации проверок (таблица 2.3), матрица требований к модели (таблица 2.4) и минимальный контур аудита при ограниченных ресурсах (таблица 2.5). Эти элементы обеспечивают практическую применимость модели и воспроизводимость результатов в деструктивных условиях.

В главе 2 определено содержание понятия «деструктивные условия окружающей среды» применительно к аудиту информационной безопасности финансово-экономической организации и предложена классификация соответствующих факторов. Показано, что такие условия влияют на риски информационной безопасности через рост вероятности реализации угроз, увеличение ущерба и снижение эффективности традиционных контуров защиты.

Установлено, что для получения управленчески значимых результатов

аудит СОИБ в деструктивных условиях должен строиться на риск-ориентированном подходе и оценивать не только соответствие требованиям, но и результативность и устойчивость процессов ИБ. Сформулированы требования к модели аудита: учет внешнего контекста, стандартизация артефактов и доказательной базы, наличие критериев и шкал оценки, риск-ориентированная классификация несоответствий и применимость при ограниченных ресурсах.

Сформулированные требования являются исходными данными для проектирования модели аудита СОИБ в главе 3, где будет представлена структура модели, этапы проведения аудита, набор показателей и методика применения на примере типовой финансово-экономической организации.

Дополнительно следует отметить, что сформулированные требования к модели аудита ориентированы на практическую применимость: они позволяют проводить аудит в регулярном режиме и фиксировать динамику состояния СОИБ даже при ограниченных ресурсах и изменчивости внешней среды. Тем самым обеспечивается основа для последующего проектирования модели аудита и методики ее применения.

ГЛАВА 3. РАЗРАБОТКА ТЕОРЕТИЧЕСКОЙ МОДЕЛИ АУДИТА СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ФИНАНСОВО-ЭКОНОМИЧЕСКОЙ ОРГАНИЗАЦИИ В ДЕСТРУКТИВНЫХ УСЛОВИЯХ ОКРУЖАЮЩЕЙ СРЕДЫ

3.1. Назначение модели аудита СОИБ: цель, задачи, область применения

В главе 3 представлена разработанная теоретическая модель аудита системы обеспечения информационной безопасности (СОИБ) финансово-экономической организации, адаптированная к деструктивным условиям окружающей среды. Под моделью аудита в рамках настоящей ВКР понимается формализованное описание состава входных данных, последовательности этапов аудита, набора критериев и шкал оценки, а также правил формирования результатов (отчета, классификации несоответствий и рекомендаций). Модель ориентирована на воспроизводимость: одинаковые исходные условия должны приводить к сопоставимым выводам.

Цель модели — обеспечить управленчески значимую оценку состояния СОИБ, позволяющую принимать решения о приоритетах улучшения и распределении ресурсов. В отличие от формального аудита, фиксирующего только наличие документов и средств защиты, предложенная модель нацелена на оценку: (1) соответствия требованиям; (2) фактической результативности мер защиты; (3) устойчивости процессов ИБ к внешним воздействиям; (4) зрелости управления и способности к улучшению.

Задачи, решаемые моделью, включают: учет внешнего контекста (профиля деструктивных условий); риск-ориентированное планирование; определение минимально достаточной доказательной базы; проведение оценки по единым критериям; классификацию несоответствий по критичности; формирование плана корректирующих и предупреждающих действий (CAPA) с ответственными и сроками; подготовку отчетности, пригодной для внутреннего контроля и руководства организации.

Область применения модели — внутренний аудит СОИБ финансово-

экономической организации, а также подготовка к внешним проверкам и оценкам соответствия. Модель применима как к комплексным аудитам (все ключевые области), так и к тематическим аудитам, когда ресурсы ограничены либо требуется оперативная проверка при ухудшении угрозовой обстановки.

В качестве исходных предпосылок принимается, что организация располагает хотя бы минимальным набором документов и артефактов (политика ИБ, регламенты ключевых процедур, журналы событий и инцидентов, сведения о резервном копировании, данные по уязвимостям). Если часть артефактов отсутствует, это трактуется как отдельный результат аудита и используется для формирования рекомендаций по повышению доказуемости и управляемости СОИБ.

3.2. Элементы модели: объект, область, критерии, доказательства и результаты

Для корректного применения модели требуется единообразное понимание терминов. Объектом аудита является СОИБ в установленной области: совокупность ролей, документов, процедур и технических средств, обеспечивающих выполнение мер защиты. Область (границы) аудита задает перечень подразделений, процессов, информационных систем и активов, включенных в проверку. В финансово-экономической организации область обычно формируется вокруг критичных сервисов (дистанционное обслуживание, проведение операций, учет и отчетность) и сопряженных инфраструктурных компонентов.

Критерии аудита — это требования, на соответствие которым проводится оценка. Они включают внешние требования (нормативные и регуляторные, стандарты и отраслевые рекомендации) и внутренние требования (политики, регламенты, инструкции). В предложенной модели критерии дополняются критериями результативности и устойчивости, которые раскрываются через метрики и фактические артефакты исполнения процедур.

Доказательства аудита (аудиторские артефакты) — документы, записи и

данные, подтверждающие фактическое выполнение требований: приказы и регламенты, журналы событий, тикеты инцидентов, отчеты сканирования уязвимостей, выгрузки прав доступа, отчеты тестов восстановления, результаты учений по реагированию, договорная документация с подрядчиками. В деструктивных условиях наличие документа без артефактов исполнения рассматривается как фактор повышенного риска.

Результаты аудита представляются как: несоответствия (нарушение критерия), наблюдения (факторы, повышающие риск без прямого нарушения критерия) и хорошие практики (решения, повышающие устойчивость и подлежащие тиражированию). Итоговые выходы модели включают: профиль рисков по областям, оценку зрелости ключевых процессов, интегральную оценку устойчивости, а также план CAPA.

3.3. Формирование профиля деструктивных условий как входного параметра аудита

Ключевым отличием предложенной модели является использование входного параметра «профиль деструктивных условий», отражающего актуальные факторы внешней среды. Профиль фиксируется до детального планирования и определяет приоритеты и глубину проверок. Он снижает риск проведения статического аудита по неизменному чек-листу при существенном изменении угрозовой обстановки.

Построение профиля выполняется в три шага: (1) идентификация факторов (угрозовые, технологические, регуляторные, организационно-кадровые, партнерские); (2) выбор индикаторов и источников данных (статистика SOC/мониторинга, отчеты сканирования, сведения о просрочке патчей, данные о критичных сервисах у подрядчиков, показатели кадровой обеспеченности); (3) оценивание индикаторов по шкале 0–3 с фиксацией основания (какие отчеты/журналы использованы).

Оценка индикаторов может быть экспертной, однако для воспроизводимости важно фиксировать источники. Например, интенсивность

атак оценивается по росту числа инцидентов; окно уязвимости — по средней просрочке устранения критичных уязвимостей; зависимость от подрядчиков — по доле критичных сервисов у внешних поставщиков и объему привилегированного доступа подрядчиков.

Таблица 3.1 – Пример индикаторов профиля деструктивных условий и их влияние на программу аудита

Группа	Индикатор	Шкала (0–3)	Источник данных	Усиление аудита
Угрозовая	Интенсивность атак на ДБО/учетки	0–3	SOC/журналы, инциденты	Доступ, MFA, мониторинг
Технологическая	Окно устранения критичных уязвимостей	0–3	Сканирование, реестр патчей	Уязвимости, изменения
Партнерская	Доля критичных сервисов у подрядчиков	0–3	Каталог сервисов, договоры	Третьи стороны, доступ
Организационная	Кадровая обеспеченность ИБ	0–3	Штат/нагрузка	Контроль ключевых процедур
Инфраструктурная	Частота отказов/сбоев	0–3	Мониторинг доступности	BCP/DR, резервирование
Регуляторная	Интенсивность изменений требований	0–3	Комплаенс, письма/акты	Соответствие, доказуемость

Практическое правило модели: область считается приоритетной для углубленной проверки, если по ней два и более индикатора имеют оценку 2–3, либо один индикатор имеет оценку 3 и затрагивает критичные активы или сервисы.

3.4. Риск-ориентированное планирование аудита и выбор глубины проверок

Риск-ориентированное планирование опирается на профиль деструктивных условий и карту критичности активов/процессов. Планирование

включает: определение границ аудита, ранжирование областей, выбор глубины процедур, формирование программы аудита (календарь, процедуры, выборки, запросы артефактов).

Для обеспечения единообразия решений модель предлагает использовать приоритет области P, зависящий от значимости активов A, критичности сервиса S, угрозовой интенсивности T, сложности/уязвимости среды C и внешней зависимости V. Значения A и S задаются по шкале 1–5, значения T, C и V — по шкале 0–3. Приоритет P может определяться как взвешенная сумма; важно наличие фиксированного правила, обеспечивающего сопоставимость аудитов между периодами.

На основе приоритета выбирается глубина аудита: базовый контур (документы + интервью), стандартный (добавляются выборки и анализ артефактов), углубленный (анализ журналов за период, расширенные выборки, проверка тестов и сценариев устойчивости).

Таблица 3.2 – Выбор глубины аудита в зависимости от приоритета области

Приоритет области	Контур аудита	Типовые процедуры	Типовые доказательства
Низкий	Базовый	Документы + интервью	Политики, регламенты, приказы
Средний	Стандартный	Документы + интервью + выборки	Заявки, выгрузки прав, отчеты
Высокий	Углубленный	Стандартный + анализ журналов + тесты	Логи, тикеты, отчеты DR, разбор инцидентов

3.5. Процедуры проведения аудита и правила достаточности доказательств

Процедуры аудита в модели включают: документальную проверку, интервью, анализ технических артефактов (журналы, тикеты, отчеты) и

выборочные проверки (sampling). Документальная проверка устанавливает, какие требования действуют и как распределена ответственность. Интервью уточняют фактическое выполнение процедур и выявляют разрывы между документами и практикой. Анализ артефактов подтверждает исполнение за выбранный период. Выборки позволяют проверить соблюдение регламентов на конкретных примерах.

Критерий достаточности доказательств — наличие подтверждений как требований (документы), так и исполнения (записи/журналы/выборки). Если доказательства исполнения отсутствуют, фиксируется низкая доказуемость, что трактуется как фактор риска и отдельный предмет для CAPA (например, внедрение централизованного учета заявок или логирования).

Таблица 3.3 – Пример вопросов интервью по ключевым процессам ИБ (фрагмент)

Процесс	Вопрос аудитора	Ожидаемое доказательство
Управление доступом	Как выдаются/отзываются права? Как пересматриваются привилегии?	Регламент, заявки, выгрузки прав, протокол пересмотра
Инциденты	Какие SLA? Кто отвечает за расследование? Как фиксируются уроки?	Плейбуки, тикеты, отчеты расследований
Уязвимости	Как планируются патчи? Как фиксируются исключения и меры?	Отчеты сканирования, план патчей, реестр исключений
Непрерывность	Когда тестировали восстановление? Достижимы ли RTO/RPO?	DRP/BCP, отчет теста, журналы бэкапов
Подрядчики	Какие требования по ИБ в договорах? Как контролируется доступ?	Договоры, списки доступов, журналы работ

3.6. Метрики и оценочные шкалы: получение измеримого результата без программной реализации

Чтобы обеспечить измеримость результатов без разработки программного обеспечения, модель использует сочетание шкал оценки (0–3/0–4), метрик из существующих источников (тикеты, отчеты SOC, отчеты сканирования, журналы бэкапов) и экспертных оценок с фиксацией основания.

Оценка соответствия может выполняться по шкале 0–3: 0 — требование не реализовано; 1 — реализовано частично или документально без подтверждения исполнения; 2 — реализовано и подтверждено выборкой, но есть отклонения; 3 — реализовано и стабильно исполняется. Аналогично оцениваются результативность и устойчивость, где максимальный уровень соответствует достижению целевых значений метрик и подтвержденной устойчивой практике.

Таблица 3.4 – Метрики результативности и устойчивости (пример)

Область	Метрика	Источник	Цель/порог (пример)	Интерпретация
Инциденты	MTTD/MTTR	Тикеты/SOC	MTTR ≤ 24 ч (крит.)	Превышение — снижение результативности
Доступ	Доля пересмотра привилегий	Протоколы/выгрузки	≥ 95%/квартал	Низкое значение — риск эскалации
Уязвимости	Окно устранения CVSS≥9	Сканирование/план	≤ 30 дней	Просрочка — рост вероятности атак
Непрерывность	Достижение RTO/RPO	Отчеты DR	100% крит. сервисов	Недостижение — низкая устойчивость
Подрядчики	Срок уведомления об ИБ-инциденте	Договор/SLA	≤ 2 ч	Нет SLA — позднее реагирование

Мониторинг	Охват журналированием	Схема логов	≥ 90% крит. систем	Низкий охват — «слепые зоны»

3.7. Оценка зрелости ключевых процессов ИБ и требования к устойчивости

Устойчивость СОИБ в финансово-экономической организации определяется зрелостью ключевых процессов: управление доступом и привилегиями, управление уязвимостями, управление инцидентами, мониторинг событий, управление изменениями, обеспечение непрерывности и управление рисками третьих сторон. Низкая зрелость означает зависимость от отдельных сотрудников и ручных операций, что критично при кадровом дефиците и росте атак.

В модели применяется шкала зрелости 0–4: 0 — процесс отсутствует; 1 — начальный; 2 — определен; 3 — управляемый; 4 — улучшаемый. Для воспроизводимости каждому уровню соответствуют признаки и артефакты (регламенты, RACI, KPI/KRI, отчеты, планы улучшений).

Таблица 3.5 – Карта зрелости ключевых процессов ИБ (пример критериев уровней 2–4)

Процесс	Уровень 2	Уровень 3	Уровень 4
Доступ/привилегии	Регламенты, заявки, матрица ролей	Пересмотр прав, MFA, KPI	Анализ нарушений, улучшение ролей
Инциденты	Процедура обработки, классификация	SLA, плейбуки, учения, метрики	Улучшение по урокам и аналитике
Уязвимости	Реестр, план устранения	Контроль сроков, реестр исключений	Оптимизация и автоматизация контроля
Непрерывность	DRP/BCP, резервное копирование	Тесты DR, контроль RTO/RPO	Улучшение планов по результатам тестов

Подрядчики	Требования в договорах	Контроль доступов, аудит	Оценка цепочки поставок, улучшение SLA

3.8. Классификация несоответствий по риску и управление CAPA

Модель предусматривает классификацию несоответствий по критичности и процедуру управления CAPA. Критичность определяется на основе риска: последствия, вероятность эксплуатации, охват критичных активов и наличие компенсирующих мер. В деструктивных условиях допускается повышение критичности недостатков в тех зонах, где профиль контекста указывает высокую угрозовую интенсивность.

Используется шкала критичности: К1 — критическое несоответствие; К2 — значимое; К3 — умеренное; К4 — низкое. Для воспроизводимости применяется матрица «вероятность × последствия», пример приведен в таблице 3.6.

Таблица 3.6 – Пример матрицы критичности несоответствий (вероятность × последствия)

Последствия \ Вероятность	Низкая	Средняя	Высокая	Очень высокая
Низкие	К4	К4	К3	К3
Средние	К4	К3	К2	К2
Высокие	К3	К2	К1	К1
Критические	К2	К1	К1	К1

Поток преобразования результатов аудита в план CAPA представлен на рисунке 3.1.

Контекст аудита (профиль деструктивных условий)
↓
Планирование: область аудита, приоритеты, программа, выборки
↓
Проведение: сбор доказательств → оценка по критериям и метрикам
↓ Отчет → классификация несоответствий → CAPA → контроль

исполнения

Рисунок 3.1 – Логика функционирования модели аудита: от контекста к CAPA

Детализированная блок-схема процесса аудита СОИБ приведена в приложении А.

3.9. Форматы отчетности и визуализация результатов для руководства

Отчет по аудиту должен быть понятен руководству и содержать приоритеты, а также связь между несоответствиями и рисками. Модель рекомендует двухуровневую структуру: управленческое резюме (контекст, ключевые выводы, топ-риски и топ-CAPA, динамика показателей) и детальная часть (методика, область, доказательства, перечень несоответствий и наблюдений).

Для визуализации результатов предлагаются формы, не требующие программной реализации: таблица «область — приоритет — оценка — критичные несоответствия», карта зрелости процессов (0–4), матрица рисков, статус выполнения CAPA (план/факт).

Таблица 3.7 – Рекомендуемая структура отчета по аудиту СОИБ (по модели)

Раздел	Содержание	Кому адресовано
1. Резюме	Контекст, ключевые выводы, топ-риски, топ-CAPA	Руководство
2. Область и методика	Границы, период, процедуры, ограничения	Внутренний контроль/аудит
3. Оценка по критериям	Соответствие/результативность/устойчивость/зрелость	ИБ/ИТ/руководство
4. Несоответствия	Описание, доказательства, критичность, причины	Владельцы процессов
5. План CAPA	Мероприятия, сроки, ответственные, приемка	Руководство/контроль
6. Приложения	Выборки, протоколы интервью, отчеты тестов	Аудиторская группа

3.10. Апробация модели: пример применения на типовой финансово-экономической организации

Для апробации модели рассматривается условная финансово-экономическая организация, предоставляющая дистанционное обслуживание и выполняющая платежные операции. Инфраструктура включает периметр, серверы приложений, базы данных, рабочие места и компоненты у внешнего провайдера. Подразделение ИБ взаимодействует с ИТ-службой и внутренним контролем, при этом отмечается высокая загрузка специалистов.

Шаг 1: формируется профиль контекста (рост фишинга, просрочка устранения части критичных уязвимостей, высокая зависимость от подрядчика, кадровые ограничения). Шаг 2: на основе контекста и значимости активов определяется приоритет областей и глубина проверок; формируется программа аудита. Шаг 3: выполняются процедуры (документы, интервью, анализ артефактов и выборки) и рассчитываются оценки по критериям и метрикам. Шаг 4: результаты классифицируются по критичности и формируется CAPA с критериями приемки. Шаг 5: задаются контрольные метрики и проверяется динамика на следующем цикле аудита.

Таблица 3.8 – Сводная форма результатов аудита по модели (пример)

Область	Приоритет	Оценка (0–3)	Зрелость (0–4)	Критичные результаты
Доступ/привилегии	Высокий	1,5	2	К1: нет пересмотра; К2: контроль сервисных учеток
Инциденты	Высокий	2,0	2	К2: нет плейбуков; наблюдение: кадровый дефицит
Уязвимости	Высокий	1,8	2	К2: нет реестра исключений;

				просрочка патчей
Непрерывность	Средний	2,2	2	К1: отсутствует тест восстановления одного сервиса
Подрядчики	Высокий	2,0	1–2	К2: нет SLA уведомления; К3: нет журнала работ

3.11. Комплект типовых форм и документов для проведения аудита (без автоматизации)

Чтобы модель могла применяться в организации без разработки программных средств, рекомендуется набор типовых форм: запрос документов и данных, протокол интервью, рабочий лист оценки, реестр несоответствий/наблюдений, карточка CAPA, журнал контроля выполнения. Стандартизация форм снижает зависимость от конкретных аудиторов и повышает воспроизводимость результатов.

Компактные примеры шаблонов приведены в таблицах 3.9–3.11, а расширенные формы для практического использования (под печать и внедрение) представлены в приложениях Б–З.

В частности: блок-схема процесса аудита приведена в приложении А; форма программы аудита — в приложении Б; форма запроса документов и данных — в приложении В; протокол интервью — в приложении Г; рабочий лист оценки — в приложении Д; реестр несоответствий/наблюдений — в приложении Е; карточка CAPA — в приложении Ж; матрица критичности несоответствий — в приложении З.

Таблица 3.9 – Форма запроса документов и данных для аудита (пример)

Область	Что запросить	Период	Примечание
Доступ/привилегии	Матрица ролей, выгрузка прав,	Квартал	Включить сервисные

	выборка заявок		учетные записи
Инциденты	Журнал инцидентов/тикеты, отчеты расследований	Квартал	Выделить критичные инциденты
Уязвимости	Отчеты сканирования, план патчей, исключения	Квартал	Указать CVSS-порог
Непрерывность	DRP/BCP, отчеты тестов, журналы бэкапов	Год/квартал	Критичные сервисы
Подрядчики	Договоры/SLA, список доступов, журналы работ	Актуально	Уведомления об инцидентах

Таблица 3.10 – Протокол интервью (шаблон)

Дата/время	Участники и роли	Ключевые ответы	Ссылки на доказательства/заметки
___	___	___	___

Таблица 3.11 – Карточка CAPA (шаблон)

Поле	Значение
ID несоответствия	___
Описание	___
Критичность	К1/К2/К3/К4
Риск/последствие	___
Причина (root cause)	___
Корректирующее действие	___
Предупреждающее действие	___
Ответственный	___
Срок	___
Критерий приемки	___
Подтверждающие артефакты	___

3.12. Обеспечение качества аудита и управление ограничениями достоверности

В деструктивных условиях аудит сталкивается с ограничениями: неполные данные, отсутствие централизованных журналов, ограничения доступа к системам, дефицит времени и экспертов. Чтобы результаты

оставались обоснованными, модель вводит правила управления качеством и достоверностью.

Фиксируются ограничения (какие артефакты не предоставлены, какие системы не включены, какие процедуры выполнены сокращенно) и определяется уровень уверенности (assurance level) по каждой области: высокий, средний или низкий. Уровень уверенности зависит от полноты доказательств (документы + артефакты исполнения + выборки) и репрезентативности выборок. Пример приведен в таблице 3.12.

Таблица 3.12 – Уровни уверенности (достоверности) выводов аудита (пример)

Уровень уверенности	Условие	Как отражается в отчете
Высокий	Документы + артефакты исполнения + выборки/журналы	Выводы подтверждены
Средний	Документы и часть артефактов; выборки ограничены	Указываются ограничения; CAPA по доказуемости
Низкий	Только документы или интервью без подтверждения	Выводы предварительные; приоритет — сбор доказательств

3.13. Рекомендации по внедрению модели в организации и организационные роли

Внедрение модели целесообразно выполнять поэтапно: (1) утверждение критериев, шкал и форм; (2) пилотный аудит 1–2 приоритетных областей; (3) масштабирование на комплексные проверки; (4) регулярный цикл улучшений с анализом динамики метрик. Роли и ответственность рекомендуется закреплять в матрице RACI и связывать CAPA с внутренним контролем и комплаенс.

Пример дорожной карты внедрения приведен в таблице 3.13.

Таблица 3.13 – Дорожная карта внедрения модели аудита СОИБ (пример)

Этап	Содержание	Результат	Срок (пример)

	работ		
1. Подготовка	Утверждение критериев, шкал, форм, перечня артефактов	Методика и шаблоны	2–4 недели
2. Пилот	Пилотный аудит приоритетных областей, корректировка	Отчет, CAPA, уточнение	4–6 недель
3. Масштабирование	Комплексные аудиты, интеграция с контролем	Регулярный цикл, метрики	Квартал
4. Улучшение	Анализ динамики, обучение, обновление контекста	Рост зрелости и устойчивости	Постоянно

3.14. Теоретическая оценка эффекта применения модели

Эффект применения модели проявляется в повышении управляемости рисков, доказуемости выполнения требований и устойчивости процессов ИБ. Риск-ориентированное планирование концентрирует ресурсы аудита на областях с высоким приоритетом. Метрики и шкалы обеспечивают измеримость и сопоставимость результатов между периодами. Механизм CAPA переводит отчет аудитора в управляемый план мероприятий с критериями приемки и контролем выполнения.

Связь элементов модели с ожидаемым эффектом приведена в таблице 3.14.

Таблица 3.14 – Связь элементов модели с ожидаемым эффектом (пример)

Элемент модели	Проблема	Ожидаемый эффект
Профиль контекста	Статический аудит не учитывает угрозовую обстановку	Приоритизация проверок по риску

Шкалы и метрики	Субъективность выводов, нет измеримости	Сопоставимость результатов по периодам
Уровни уверенности	Неполные данные дают ложную уверенность	Прозрачность достоверности выводов
CAPA и контроль	Отчет не приводит к изменениям	Реальные улучшения и снижение рисков
Карта зрелости	Нет понимания, куда развиваться	Дорожная карта развития процессов

3.15. Ограничения модели и условия корректного применения

Предложенная модель является теоретической и предполагает ограничения. Качество результатов зависит от доступности доказательств: при отсутствии журналов, реестров и систем учета невозможно получить высокий уровень уверенности без развития доказательной базы. Часть оценок (например, приоритизация областей) может включать экспертный компонент, поэтому важно фиксировать основания и применять единые шкалы.

Модель не заменяет специализированные технические оценки (пентест, анализ кода), а дополняет их как методическая основа аудита процессов и контролей. При применении модели необходимо учитывать режим конфиденциальности: выборки и артефакты предоставляются в объеме, достаточном для вывода, без избыточного раскрытия информации.

3.16. Выводы по главе 3

В главе 3 разработана теоретическая модель аудита СОИБ финансово-экономической организации, ориентированная на работу в деструктивных условиях окружающей среды. Определены назначение и область применения модели, выделены основные элементы (контекст, критерии, доказательства, результаты), предложен подход к формированию профиля деструктивных условий и риск-ориентированному планированию аудита.

Сформирована система критериев оценки, включающая соответствие, результативность, устойчивость и зрелость процессов. Предложены метрики и

шкалы, позволяющие получать измеримый результат без программной реализации за счет анализа существующих артефактов. Разработан механизм классификации несоответствий по критичности и процедура управления CAPA, обеспечивающая перевод результатов аудита в управляемый план улучшений.

Предложен комплект типовых форм, правила обеспечения качества и управления ограничениями достоверности, а также рекомендации по внедрению модели в организации. Пример апробации на условной финансово-экономической организации показал применимость модели и ее управленческую ценность.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [Электронный ресурс]. — Официальный интернет-портал правовой информации. — Режим доступа: https://pravo.gov.ru/proxy/ips/?docbody=&nd=102108264 (дата обращения: 28.01.2026).
2. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» [Электронный ресурс]. — Официальный интернет-портал правовой информации. — Режим доступа: https://pravo.gov.ru/proxy/ips/?docbody=&nd=102108261 (дата обращения: 28.01.2026).
3. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [Электронный ресурс]. — Официальный интернет-портал правовой информации. — Режим доступа: https://publication.pravo.gov.ru/document/view/0001201707260023 (дата обращения: 28.01.2026).
4. Приказ ФСТЭК России от 18.02.2013 № 21 (ред. от 14.05.2020) «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [Электронный ресурс]. — 20 с. — Режим доступа: https://mpt.tatarstan.ru/file/File/Prikaz%20FSTE%60K%20Rossii%20ot%2018.02.2013%20N%2021%20%28red.%20ot%2023.03.2017%29.pdf (дата обращения: 28.01.2026).
5. Положение Банка России от 30.01.2025 № 851-П «Об установлении обязательных для кредитных организаций, иностранных банков, осуществляющих деятельность на территории Российской Федерации через свои филиалы, требований к обеспечению защиты информации при

осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента» [Электронный ресурс]. — М.: Банк России, 2025. — 33 с. — Режим доступа: https://cbr.ru/Queries/UniDbQuery/File/90134/6262 (дата обращения: 28.01.2026).

6. ГОСТ Р 57580.1–2017. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер [Электронный ресурс]. — Введ. 01.01.2018. — 66 с. — Режим доступа: https://protect.gost.ru/document1.aspx?control=31&id=218176 (дата обращения: 28.01.2026).
7. ГОСТ Р 57580.2–2018. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия [Электронный ресурс]. — Введ. 01.09.2018. — 28 с. — Режим доступа: https://protect.gost.ru/document1.aspx?baseC=6&control=31&id=230678 (дата обращения: 28.01.2026).
8. Аверченков В. И. Аудит информационной безопасности: учебное пособие. — М.: ФЛИНТА, 2011. — 269 с. — ISBN 978-5-9765-1256-6.
9. Грекул В. И. Аудит информационных технологий: учебник для вузов. — М.: Горячая линия — Телеком, 2015. — 154 с. — ISBN 978-5-9912-0528-3.
10. Шилов А. К. Управление информационной безопасностью: учебное пособие. — Ростов-на-Дону, Таганрог: Южный федеральный университет, 2018. — 121 с. — ISBN 978-5-9275-2742-7.
11. Глыбовский П. А., Тимашов П. В., Чернышов В. И. Метод обеспечения и проведения внутреннего аудита информационной безопасности организаций на основе риск-ориентированного подхода // Проблемы информационной безопасности. Компьютерные системы. — 2023. — № 3. — С. 9–24.

12. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. — Geneva: ISO, 2022. — 19 p. [Электронный ресурс]. — Режим доступа: https://www.iso.org/standard/27001 (дата обращения: 28.01.2026).
13. ISO 19011:2018. Guidelines for auditing management systems. — Geneva: ISO, 2018. — 46 p. [Электронный ресурс]. — Режим доступа: https://www.iso.org/standard/70017.html (дата обращения: 28.01.2026).
14. NIST Special Publication 800-53 Rev. 5. Security and Privacy Controls for Information Systems and Organizations. — Gaithersburg, MD: National Institute of Standards and Technology, 2020. — 492 p. [Электронный ресурс]. — DOI: 10.6028/NIST.SP.800-53r5. — Режим доступа: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf (дата обращения: 28.01.2026).
15. NIST Special Publication 800-30 Rev. 1. Guide for Conducting Risk Assessments. — Gaithersburg, MD: National Institute of Standards and Technology, 2012. — 95 p. [Электронный ресурс]. — DOI: 10.6028/NIST.SP.800-30r1. — Режим доступа: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf (дата обращения: 28.01.2026).

ПРИЛОЖЕНИЕ А

Блок-схема процесса аудита СОИБ по разработанной модели

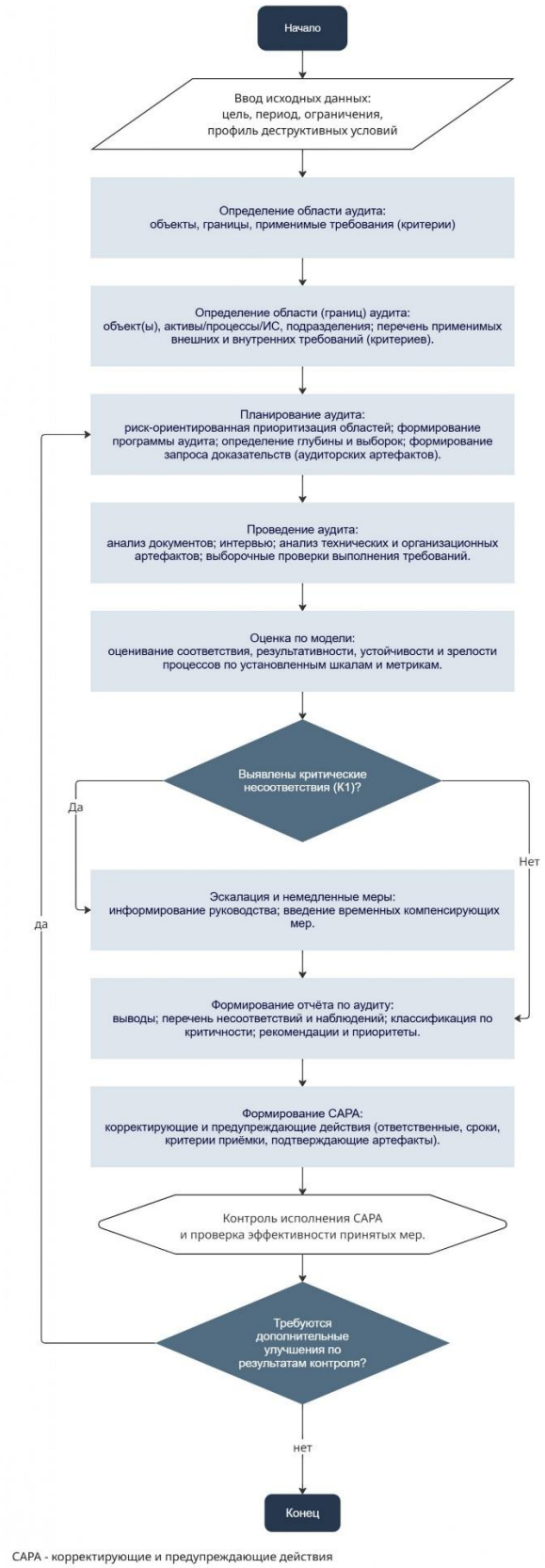

Рисунок А.1 – Блок-схема процесса аудита СОИБ (модель главы 3)

ПРИЛОЖЕНИЕ Б

Форма программы аудита СОИБ (шаблон)

Назначение: фиксирует цель, область, критерии и план процедур аудита, согласуемый с руководством.

Наименование организации/подразделения	
Период и дата проведения аудита	
Цель аудита	
Область (границы) аудита	
Критерии и нормативная база	
Команда аудита и роли (RACI при необходимости)	
Перечень процедур и выборок (кратко)	
Требуемые доказательства/артефакты	
Ожидаемые результаты (формат отчета, CAPA)	

ПРИЛОЖЕНИЕ В

Форма запроса документов и данных (Evidence Request List)

Назначение: перечень запрашиваемых документов, данных и артефактов исполнения по областям аудита.

№	Область/контроль	Документ/данные	Период	Владелец	Формат/канал	Примечание

ПРИЛОЖЕНИЕ Г

Протокол интервью (шаблон)

Назначение: фиксирует участников, вопросы и ключевые ответы, а также ссылки на подтверждающие доказательства.

Дата/время	
Подразделение/роль	
ФИО интервьюируемого	
Тема/область	
Ключевые вопросы (кратко)	
Ключевые ответы и доказательства (ссылки на артефакты)	

Таблица вопросов (при необходимости):

№	Вопрос	Ответ (кратко)	Примечание/доказательство

ПРИЛОЖЕНИЕ Д

Рабочий лист оценки контроля/процесса (шаблон)

Назначение: документирует оценку по критериям (соответствие, результативность, устойчивость, зрелость) и расчет итоговой оценки.

Контроль/процесс	Критерий	Описание требования	Доказательства	Оценка (балл)	Вес	Итог (балл×вес)	Комментарий

ПРИЛОЖЕНИЕ Е

Реестр несоответствий и наблюдений (шаблон)

Назначение: единый реестр выявленных несоответствий/наблюдений с указанием доказательств, критичности и статуса устранения.

ID	Область	Критерий/требование	Описание	Доказательства	Критичность (К1–К4)	Риск	Рекомендация	Ответственный	Статус/срок

ПРИЛОЖЕНИЕ Ж

Карточка CAPA (Corrective and Preventive Actions) (шаблон)

Назначение: оформляет корректирующие и предупреждающие действия, критерии приемки и контроль выполнения.

ID CAPA	
Связанные несоответствия/наблюдения (ID)	
Описание проблемы	
Корневая причина (5 Why / Ishikawa – кратко)	
Корректирующие действия	
Предупреждающие действия	
Владелец (ответственный)	
Сроки (план/факт)	
Необходимые ресурсы/зависимости	
Критерии приемки (как проверить)	
Риски при невыполнении	
Статус и отметка о проверке эффективности	

ПРИЛОЖЕНИЕ 3

Матрица критичности несоответствий (вероятность × последствия)

Назначение: единый подход к присвоению критичности (К1–К4) в условиях ограниченных доказательств.

Шкалы (пример):

Вероятность	Описание
1 — низкая	Эксплуатация маловероятна; сильные компенсирующие меры
2 — средняя	Возможна при определенных условиях; контролями закрыта частично
3 — высокая	Есть рабочий вектор; компенсирующие меры слабые
4 — очень высокая	Эксплуатация ожидаема/наблюдается; массовый вектор

Последствия	Описание
1 — низкие	Локальное влияние без значимого ущерба
2 — умеренные	Снижение качества сервиса/ограниченный финансовый ущерб
3 — значимые	Нарушение критичных процессов/существенные потери/регуляторные риски
4 — критические	Остановка ключевых операций/масштабная утечка/угроза устойчивости

Матрица критичности (пример присвоения):

Вероятность \ Последствия	1	2	3	4
1	К4	К4	К4	К3
2	К4	К3	К3	К2
3	К4	К3	К2	К1
4	К3	К2	К1	К1

Примечание: при наличии признаков активной эксплуатации и/или повышенной интенсивности угроз допускается повышение критичности на

один уровень (например, К3→К2).