УДК 004.942:519.23/.25 Вестник УрФО № 3(53) / 2024, с. 61–72

Жукова М. Н., Яковлева А. О. DOI: 10.14529/secur240307

РАЗРАБОТКА РЕШЕНИЯ ДЛЯ ПРОВЕДЕНИЯ GAP АНАЛИЗА И ПРИВЕДЕНИЯ В СООТВЕТСТВИЕ УРОВНЮ ЗАЩИЩЕННОСТИ ПРИ ПРОВЕДЕНИИ ОЦЕНКИ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ ПО ЗАЩИТЕ ИНФОРМАЦИИ ДЛЯ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ

В статье представлена проблема оценки соответствия кредитно-финансовой организации требованиям по защите информации в соответствии с ГОСТ 57580.2-2018. Рассматриваются и анализируются показатели оценки, значение основных метрик и расчетных величин. Представлены требования к процессу проведения оценки соответствия, описаны показатели и требования к их значениям и расчету в соответствии с ГОСТ Р 57580.2-2018.

Описаны основные подходы, применяемые для проведения оценочных процедур. Показаны основные трудности, связанные со сложностью однозначного соответствия результатов аудита и GAP анализа, проводимого финансовой организацией в рамках предварительных процедур оценки соответствия требованиям по защите информации. Выявлены основные проблемы, представлен подход, позволяющий в рамках единой оценочной процедуры совместить расчет оценки, подбор параметров и решить задачу оптимизации при подборе средств защиты информации. Представлены обобщенные схемы программного решения по автоматизации процедуры определения базовых мер и оценки соответствия по ГОСТ 57580.1 и 57580.2. Описан алгоритм расчета оценки, позволяющий получить численные значения для каждого контура безопасности, входящего в состав целевой информационной системы финансовой организации.

Ключевые слова: *оценка соответствия, кредитно-финансовые организации, защита информации, метрики.*

DEVELOPMENT OF A SOLUTION FOR CONDUCTING GAP ANALYSIS AND ADJUSTING THE LEVEL OF SECURITY WHEN ASSESSING COMPLIANCE WITH INFORMATION SECURITY REQUIREMENTS FOR FINANCIAL INSTITUTIONS

The article presents the problem of assessing the compliance of a credit and financial institution with the requirements for information security in accordance with GOST 57580.2-2018. The assessment indicators, the meaning of the main metrics and calculated values are considered and analyzed. The requirements for the conformity assessment process are presented, the indicators and requirements for their values and calculation in accordance with GOST R 57580.2-2018 are described. The main approaches used to carry out assessment procedures are described. The main difficulties associated with the complexity of unambiguous correspondence between the audit results and the GAP analysis carried out by a financial institution within the framework of preliminary procedures for assessing compliance with information security requirements are shown. The main problems are identified, an approach is presented that allows, within the framework of a single assessment procedure, to combine the assessment calculation, the selection of parameters and solve the optimization problem when selecting information security tools. Generalized schemes of a software solution for automating the procedure for determining basic measures and assessing compliance in accordance with GOST 57580.1 and 57580.2 are presented. An algorithm for calculating an assessment is described, which allows obtaining numerical values for each security contour included in the target information system of a financial organization.

Keywords: *conformity assessment, financial institutions, information security system, metrics.*

Введение

В организациях финансовой сферы вопросам информационной безопасности уделяется большое внимание, поскольку результатом нарушения работы составляющих их систем и сервисов, посредством реализации угроз, может быть прямой ущерб интересам собственников и клиентов. Для противостояния таким угрозам и обеспечения эффективности мероприятий по ликвидации неблагоприятных последствий инцидентов ИБ (их влияния на операционный, репутационный, стратегический и иные риски) в организациях БС РФ следует обеспечить достаточный уровень ИБ [1].

Оценка ситуации в сфере инцидентов информационной безопасности, происходящих с финансовыми системами, показывает два основных направления: использование методов социальной инженерии для осуществления мошеннических действий с денежными средствами клиентов банковских систем, а также атаки на техническую сторону инфраструктуры банковских систем [2]. Таким обра-

зом, требуется обеспечение необходимого уровня защиты информации для финансовых организаций. Под финансовыми организациями принято понимать все организации, которые предоставляют финансовые услуги и должны получить разрешение Банка России о допуске на финансовый рынок. В зависимости от вида организации это может быть, как лицензия, так и включение сведений в реестр или аккредитация [3].

Подход Банка России к обеспечению безопасности финансовых систем

Инфраструктура крупной финансовой системы является сложной и многогранной, так как речь идет об особо выделяемой клиентской части, о целевой системе в которой происходит основная обработка информации по всем транзакциям и обязательном взаимодействии с базами данных и другими видами хранилищ информации, о защищаемых каналах передачи информации, процессинговом центре и тд. Требуется особый подход к формированию требований по защите информации, рассмотрению защищенности целевой системы, ее оценке и требованиях к оценочным мероприятиям [4]. История действий Банка России в части разработки нормативно-методических документов по обеспечению информационной безопасности финансовых систем имеет множество этапов — разработка и утверждение СТО ИБ ИББС, множества сопутствующих и дополняющих различные практические аспекты положений. На сегодняшний день система документов переведена в систему стандартов ГОСТ 57580.X, посвященных циклу GAP анализа, аудита защищенности финансовых систем, определению базовых мер по защите информации, оценочных процедур [5].

Основные характеристики документов приведены ниже:

1) ГОСТ Р 57580.1 – 2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер» - устанавливает защитные меры, организационные и технические, и уровни защиты информации для финансовых организаций, таких как кредитные организации, некредитные финансовые организации РФ, а также субъекты национальной платежной системы [6].

Стандарт выделяет 8 процессов и 10 подпроцессов, для которых разработаны меры защиты информации, применяемые к различным объектам информатизации, в том числе АС, которые используются для построения эффективной модели бизнес-процесса и технологического процесса, непосредственно связанных с предоставлением организацией финансовых услуг.

2) ГОСТ Р 57580.2 – 2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия» – используется чтобы определить, насколько организация соответствует требованиям ГОСТ Р 57580.1, который описывает методологию проведения оценки выбора и реализации финансовой организацией организационных и технических мер защиты информации [7].

Схематично процессы, к которым применяются меры защиты информации, и план их оценки в соответствии с ГОСТами изображены на рисунке ниже (рисунок 1).

Проведение оценки соответствия, согласно требованиям, должно проводиться независимой организацией, обладающей необходимым уровнем компетенции и имеющей лицензию ФСТЭК на деятельность по технической защите конфиденциальной информации [7].

3) ГОСТ Р 57580.3-2022 «Безопасность финансовых (банковских) операций. Управление риском реализации информационных угроз и обеспечение операционной надежности. Общие положения» [8]. Данный стандарт устанавливает требования к составу и содержанию мер по управлению риском реализации информационных угроз для уровней защиты, которые применяются финансовыми организациями в рамках планирования, реализации, контроля и совершенствования системы управления таким риском.

4) ГОСТ Р 57580.4-2022 «Безопасность финансовых (банковских) операций. Обеспечение операционной надежности. Базовый состав организационных и технических мер» [9]. Устанавливает требования к составу и содержанию мер обеспечения операционной надежности для тех уровней защиты, которые применяют финансовые организации при определении базового состава таких мер. В ГОСТе отражены 3 уровня защиты (минимальный, стандартный, усиленный) в соответствии с нормативными актами Банка России, которые зависят от вида деятельности, объема операций, размера и значимости организации для финансовой системы.

Рис. 1. Взаимосвязь стандартов

В целом архитектуру рассмотренных документов можно представить в следующем виде (рисунок 2).

На данный момент отсутствуют документы, определяющие методику оценки зрелости ГОСТ Р 57580.3-2022 и методику оценки соответствия ГОСТ Р 57580.4-2022. И определенное время эти документы не были утверждены к обязательному исполнению положениями Банка России, но рекомендованы финансовым организациям для изучения и начала работы по возможной перестройке СОИБ для будущего соответствия стандартам.

Однако, 27 марта 2024 года на сайте Банка России опубликован документ №7-МР от 21.03.2024 «Методические рекомендации по управлению риском информационной безопасности и обеспечению операционной надежности» [10] для использования кредитными и некредитными финансовыми организациями. Несмотря на то, что стандарты с методиками оценок ГОСТ Р 57580.3-2022 и ГОСТ Р 57580.4-2022 еще не выпущены, Банк России рекомендует уже сейчас готовиться к внедрению требований этих стандартов.

Требования по базовым мерам защиты информации, а также оценка соответствия (это ГОСТ 57580.1 и 57580.2) — внедрены начиная с 2018 года и работа по ним уже проведена. По оценке рисков информационной

Рис. 2. Архитектура стандартов серии 57580.X

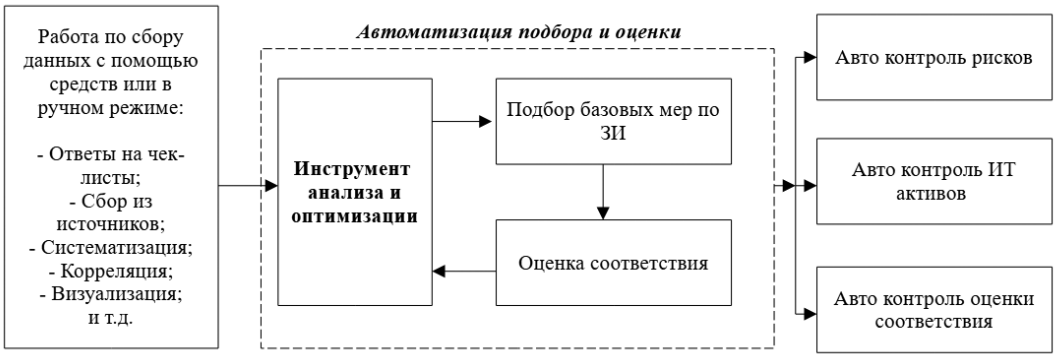

Рис. 3. Общая схема подхода к автоматизации процедур GAP-анализа

безопасности и оценке операционного риска (это ГОСТ 57580.3 и 57580.4) для всех кредитных организаций срок внедрения требований объединен и зависит от размера активов:

- если размер активов составляет 500 млрд. рублей и более - до 31 декабря 2025;

- всем остальным кредитным организациям внедрение этих стандартов рекомендовано завершить до 31 декабря 2026 года.

Практика показала, что работа с вышеуказанными ГОСТами – процесс сложный, требующий от организации большого количества временных, трудовых и финансовых затрат. Сложность заключается в том, чтобы верно истолковать, корректно и в соответствующие сроки выполнить предписанные требования. Это подтверждается наличием огромного числа вопросов, задаваемых регулятору. Например, на сайте сообщества Ассоциации банков России, объединяющего коммерческие банки и другие кредитные организации, в новостях нередко упоминаются пояснения и ответы на вопросы по исполнению требований к защите информации, задаваемые ЦБ, как основному регулятору [11].

Автоматизация и контроль требований по обеспечению защищенности финансовых системам

При выполнении требований регулятора организация может столкнуться с классической проблемой периодичности контроля, когда между аудитами (особенно актуально для организаций, где постоянно происходят изменения) возможно серьезное изменение в инфраструктуре и процессах.

При отсутствии отлаженного постоянного процесса управления соответствием, при очередном аудите может выясниться, что нужна доработка систем и внедрение мер. Не говоря о том, что проблема с реализацией мер может привести к фактической реализации самих рисков информационной безопасности и прямым потерям.

Согласно информации Positive Technologies, количество успешных кибератак в финансовом секторе год от года растет: в третьем квартале 2023 года было зафиксировано вдвое больше уникальных киберинцидентов, чем в аналогичном периоде годом ранее, что говорит о пристальном внимании преступников к отрасли [2]. Это же подтверждает и ЦБ, показывая прирост объема похищенных финансовых средств почти на 30% [12].

Очевидно, что возникает потребность в автоматизации Compliance процессов в целях постоянного контроля защищенности систем участниками кредитно-финансовой сферы. Внедрение соответствующих решений по автоматизации решит проблему постоянного контроля рисков ИБ и соответствия требованиям, упростит и удешевит прохождение аудитов, поможет правильно расставлять приоритеты при реагировании на проблемы [13].

Такое решение может принести не только экономическую выгоду (сокращение серьезной статьи расходов на предварительный аудит), но и принести практическую пользу — в виде определенной помощи при принятии решений о наборе тех или иных средств защиты информации и проведении дальнейшей автоматической оценки соответствия в связи с изменениями в инфраструктуре целевой информационной системы. Общее представление о разрабатываемом подходе можно представить в следующем виде (рисунок 3).

Одной из проблем является отсутствие алгоритма действий, применяя который можно было бы выстроить в организации соответствующую критериям и требованиям и

при этом результативную систему защиты ИБ. Об этом свидетельствует вопрос Ассоциации банков России №25 из письма с вопросами по выполнению требований ГОСТ Р 57580.1 – 2017 и 57580.2 – 2018: «Планируется ли организовать разработку методички по применению ГОСТ Р 57580.2 и критериям принятия решений по оценке мер ЗИ ГОСТ Р 57580.1 для обеспечения сходных и повторяемых результатов оценки соответствия?» [11].

На сегодняшний день задача оценки соответствия решается двумя разными способами:

1) используя внутренние силы организации: самостоятельная работа по выбору мер, с учетом их применимости, и способов их реализации, а затем проведение оценки соответствия внешней организацией;

2) передача на аутсорсинг: привлечение сторонних специалистов для приведения системы к нужному уровню оценки.

Анализ первого подхода показал, что есть сложности с реализацией требований организациями самостоятельно, которые описываются как внутренними специалистами по ИБ финансовых организаций на различных вебинарах и форумах, так и различными компаниями, предлагающими передать заботы по проведению мероприятий в рамках ГОСТ Р 57580.1 – 2017 и ГОСТ Р 57580.2 – 2018 на аутсорсинг для получения высоких оценок соответствия:

• проблемы перехода с СТО БР ИББС-1.0 – 2014 на ГОСТ Р 57580.1 – 2017 по причине увеличения количества новых требований, которых не было ранее, что, соответственно, приводит к получению низких оценок;

• высокая трудоемкость проведения оценки риска информационной безопасности – определение всех информационных активов, угроз и критичности последствий реализации риска ИБ, сложности дальнейшего использования полученных результатов для оценки остаточного операционного риска, вызванного неполным или некачественным выбором и применением организационных и технических мер защиты информации;

• большой объём работы – выявление всех бизнес и технологических процессов предоставления финансовых услуг, их составляющих и характеристик, после чего определение совокупности объектов информатизации с единой степенью критичности, в отношении которых должен применяться единый перечень мер защиты информации – контуров безопасности;

• необходимость наличия опытных и компетентных аудиторов, специалистов в связи со сложностью аудита требований ЦБ в части управления рисками и операционной надежностью.

Постоянные изменения законодательства и проверки ЦБ РФ сильно затрудняют контроль соответствия актуальным требованиям, а аудиты часто заканчиваются неудовлетворительной оценкой [14]. При этом, начиная с 2023 года большинству организаций требуется иметь оценку соответствия не ниже 4 уровня – 85%. Этот показатель является довольно высоким, причем его достижение, зачастую, требуется в кратчайшие сроки — это требует кадровых и финансовых ресурсов компании, количество которых всегда ограничено [15].

Таким образом, очевидным преимуществом должен обладать второй подход — привлечение сторонних компаний, обладающих профессиональными компетенциями. Работа внешних компаний строится по практически одинаковому сценарию:

1) сбор информации и обследование IT-инфраструктуры;

2) предварительная оценка (GAP-анализ), на котором проводят предварительную оценку, из которой становится известным список проблемных областей и областей для улучшения;

3) устранение недостатков, разработка внутренней нормативной документации (ВНД), внедрение средств защиты информации (СЗИ);

4) итоговая оценка, целью которой является оценка эффективности проработки проблемных областей и анализ полученных результатов;

5) формирование отчета по требованиям регулятора и согласование совместно с заказчиком [13].

Интересным является характеристика подходов к повышению оценки по затратам и возможным приростам показателей оценки, представленным в таблице 1.

Анализ результатов применения второго подхода — привлечения сторонних компаний на оценку и формированию мер по защите информации, показывает, что, как правило, все сводится к реализации набора наиболее выгодных, имеющих наибольший вклад в получение итогового показателя, решений. Например, реализация технической меры с использованием облачного решения для повы-

Таблица 1.

Характеристики подходов повышения оценки

(BI.ZONE «Как повысить оценку ГОСТ 57580: быстро, эффективно, с первого раза» [15])

Подход	Размер бюджета*	Срок проекта	Повышение оценки
Разработка ОРД	Малый	1-2 мес.	0,16
Разработка ОРД и полное внедрение процесса	Средний	3-5 мес.	0,57
Подключение сервисов кибербезопасности, внедрение СЗИ	Большой	2-6 мес.	0,37

шения итоговой оценки, поскольку такой способ позволяет существенно и в короткие сроки достичь результата. Однако дальнейшая судьба реализованных, таким способом, процессов информационной безопасности финансовой организации остается неизвестной. Процедура оценки соответствия – процедура периодическая и очень сложно гарантировать, что подключенные сервисы, повышающие оценку, останутся функционировать и после ее проведения. В любом случае, обеспечение их дальнейшего сопровождения является затратным с финансовой точки зрения.

Рассмотрение существующих подходов, а также задачи автоматизации и контроля соответствия требованиям нормативных документов Банка России в области обеспечения информационной безопасности показывают наличие определенных проблем:

1) отсутствие подхода к анализу соответствия результатов аудита и применяемых оценочных процедур в рамках GAP анализа;

2) необходимость применения или разработки алгоритмов оптимизации для подбора и оценки эффекта от внедрения тех или иных мер по защите информации, в соответствии с требованиями ГОСТ 57580.1

3) необходимость разработки модели анализа и оценки применимости информации из целевой информационной системы для формирования дополнительных сведений при процедуре аудита и оценки финансовой системы.

Разработка решения по анализу соответствия результатов аудита и применяемых оценочных процедур в рамках GAP анализа для кредитно-финансовой сферы

В большинстве случаев сложности возникают из-за несоответствия результатов оценки, либо из-за неоднозначности трактовки реализованных мер по защите информации различными аудиторскими компаниями. Это может зависеть от квалификации специалистов, от того набора мер, которые они привыкли «видеть» в других финансовых системах и еще от целого спектра других причин. Конечно, данные разногласия в оценке не будут прямо противоположными по оценке (0 или 1), но в данном случае речь может идти о достаточно серьезных изменениях в общей оценке (когда по 0,5 ставится по нескольким мерам в разных подпроцессах и это имеет накопительный эффект).

Требуется подход, позволяющий работать с требованиями и принимать решения по обеспечению защиты финансовых организаций, причем, как самостоятельно при реализации проекта, так и используя его в качестве механизма контроля действий внешних специалистов. В общем виде основные этапы такого решения представлены на рисунке 4.

Последовательность действий, представленная на схеме, выглядит следующим образом:

1) сведения об имеющейся системе защиты финансовой организации загружаются специалистом в базовый модуль, который представляет собой «калькулятор», позволяющий вычислить оценку уровня защиты на текущий момент;

2) по результатам работы базового модуля выводятся результаты аудита, которые содержат информацию о параметрах, имеющих низкую оценку (потенциальные места доработки), в форме базового отчета, который можно сразу отдать лицу, принимающему решение (ЛПР) и на этом закончить работу, а можно загрузить в модуль подбора;

3) в модуле подбора возможны следующие сценарии: потенциальные места доработки, полученные в модуле результатов аудита, можно сравнить со списком решений,

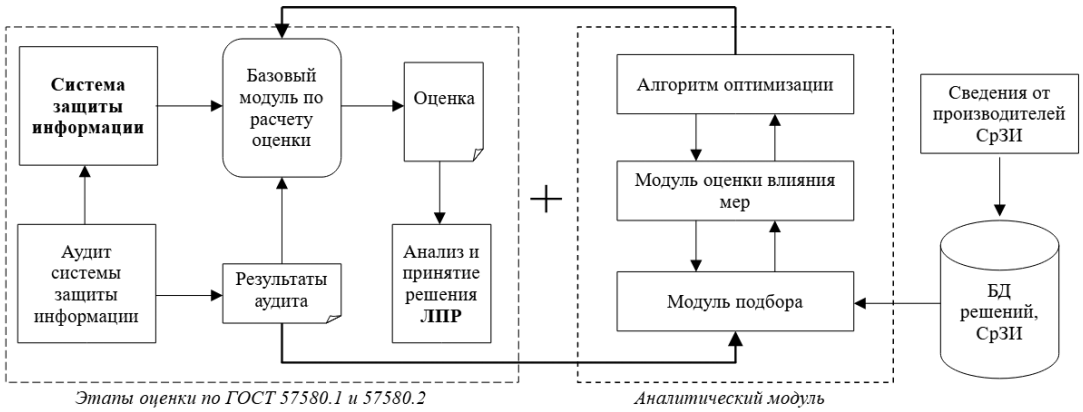

Рис. 4. Общая схема решения по анализу соответствия результатов аудита и применяемых оценочных процедур в рамках GAP анализа

предлагаемых производителями, которые закрывают те или иные требования и результаты этой работы в виде предложений отдать ЛПР, либо загрузить полученную информацию в аналитический модуль;

4) в аналитическом модуле в отличие от простого сравнения списков минусов и решений выполняется анализ возможностей дополнительной настройки существующих средств и систем в организации, а также оптимизированный подбор решений в зависимости от их стоимости или количества возможного закрытия недоработанных мест (максимальный охват закрытия требований), а уже затем передача этой информации ЛПР.

Разрабатывается программное решение для расчета базовых мер по требованиям ГОСТ 57580.1. Это решение реализовано в виде «калькулятора» для подбора необходимых базовых мер, чтобы лица, принимающие решение о внесении изменений в систему защиты информации, могли получить сводную информацию об уровне соответствия требуемому уровню защищенности, определенному для контура (контуров) безопасности соответствующими нормативно-правовыми актами.

В результате работы первого блока решения должен быть выполнен подбор базовых мер и проведения их предварительная оценка.

Для каждого контура безопасности проводится расчет оценки Ei, более подробно процедура расчета представлена на рисунке 5. Расчет оценки является одним из внутренних модулей, результат выполнения которого дает требуемый минимальный уровень оценки и определяет минимально необходимый набор базовых мер.

Таким образом, в результате работы первого модуля программного средства будет получен автоматизированный процесс оценки внесения изменений в целевую информационную систему и получен, соответствующий требованиям ГОСТ 57580.1, набор базовых мер по защите информации. Все меры рассчитаны в соответствии с требованиями ГОСТ 57580.2 по оценке соответствия базовых мер необходимому уровню показателя защищенности финансовой системы.

Заключение

Обеспечение защищенности финансовых систем сложная и трудоемкая задача. Это касается не только практической реализации защитных мер, внедрения и установки разнообразных средств защиты информации. Но и разработки методологических основ по формированию единого базиса, который мог бы охватывать и практические средства, и оценку рисков, в том числе операционных, а также унифицировать подходы к общей оценке соответствия финансовых систем требованиям по обеспечению информационной безопасности [16].

Банк России, как главный регулятор в кредитно-финансовой сфере, со своей стороны прикладывает максимальные усилия в сфере разработки методологических основ, их пересмотру и соответствию современным тенденциям, выпуску положений по различным практическим аспектам обеспечения защищенности тех или иных сегментов финансовой информационной системы. Выпущенная серия ГОСТ 57580.X призвана упорядочить процессы формирования защитных мер и последующей оценки соответствия требо-

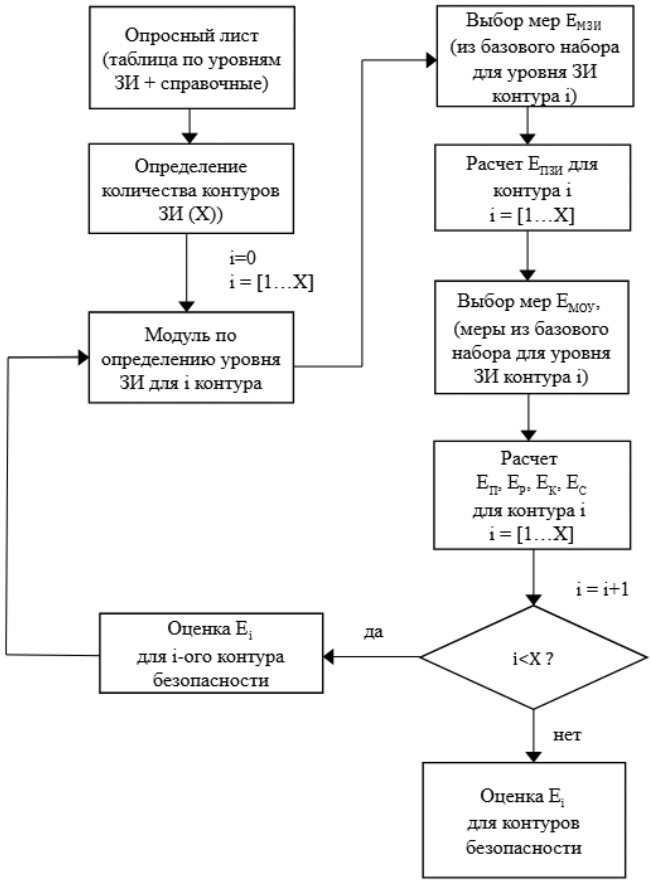

Рис. 5. Алгоритм расчета оценки Ei для каждого контура безопасности

ваниям по защите информации. Внедрение требований ГОСТ показывает достаточно хорошие практические результаты и позволяет пользоваться единой системой оценки соответствия.

Однако, часть оценочных процедур имеет неоднозначность при сопоставлении результатов внутреннего GAP анализа и последующего аудита сторонней компанией. Это может (и приводит) к серьезным разногласиям по оценке внедренных защитных мер, финансовым и репутационным потерям, существенному объему последующих работ по устранению разногласий (или выполнению рекомендаций аудитора). Пропустить этап предварительного GAP анализа со стороны финансовой компании также будет являться ошибочным — чаще всего это приведет к неготовности организации проходить процедуру оценки соответствия требованиям по защите информации.

Таким образом, требуется решение, снимающее неоднозначность оценки после прохождения аудита и результатов GAP анализа. Данное решение должно полностью выполнять требования ГОСТ 57580.1 и 57580.2 и в то же время обладать внутренним механизмом, позволяющим приводить в соответствие результаты двух выполненных работ. Представленный в статье подход предлагает решение, основанное на сочетании двух расширенных модулей: первый модуль полностью реализовывает требования ГОСТ и позволяет провести подбор необходимых базовых мер и провести внутреннюю оценку соответствия; второй модуль предлагает решение задачи подбора защитных мер не только в соответствии с требованиями ГОСТ, но и в том числе в зависимости от выбранного критерия оптимизации (стоимость, количество закрываемых мер), либо в зависимости от величины показателя оценки, который может дать реализация той или иной меры с помощью различных средств защиты информации. Данное решение реализовано в программном виде и находится на этапе апробации в нескольких финансовых системах.

Литература

1. СТО БР ИББС-1.0-2014 (дата введения от 17.09.2014) [Электронный ресурс]. URL: https://www.garant.ru/products/ipo/prime/doc/70567254/?ysclid=lmel9rs33r25543875 (дата обращения: 13.08.2024).

2. Киберугрозы финансовой отрасли: промежуточные итоги 2023 года [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/financial-industry-security-interim-2023/ (дата обращения: 26.08.2024).

3. Как проверить участника финансового рынка [Электронный ресурс]. URL: https://cbr.ru/finorg/ (дата обращения: 13.09.2024).

4. Козьминых, С. И. Моделирование систем и процессов защиты информации на объектах кредитно-финансовой сферы / С. И. Козьминых // Информационная безопасность финансово-кредитных организаций в условиях цифровой трансформации экономики / Под ред. С.И. Козьминых. – Москва: Общество с ограниченной ответственностью "Издательство Прометей", 2020. – С. 320-412.

5. Ситская, А. В. Автоматизация процесса проведения аудита посредством приложения "Аудит57580" / А. В. Ситская, В. В. Селифанов // Интеллектуальный потенциал Сибири: Сборник научных трудов 29-ой Региональной научной студенческой конференции, посвященной Году науки и технологий в России. В 5-ти частях, Новосибирск, 17–21 мая 2021 года / Под редакцией Д.О. Соколовой. Том Часть 5. – Новосибирск: Новосибирский государственный технический университет, 2021. – С. 607-614.

6. ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер» (Дата введения 08.08.2018) [Электронный ресурс]. URL: https://docs.cntd.ru/document/1200146534 (дата обращения: 15.09.2024).

7. ГОСТ Р 57580.2-2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия» (Дата введения 28.03.2018) [Электронный ресурс]. URL: https://docs.cntd.ru/document/1200158801 (дата обращения: 15.09.2024).

8. ГОСТ Р 57580.3-2022 «Безопасность финансовых (банковских) операций. Управление риском реализации информационных угроз и обеспечение операционной надежности. Общие положения» (Дата введения 01.02.2023) [Электронный ресурс]. URL: https://docs.cntd.ru/document/1200194981 (дата обращения: 25.10.2024).

9. ГОСТ Р 57580.4-2022 «Безопасность финансовых (банковских) операций. Обеспечение операционной надежности. Базовый состав организационных и технических мер» (Дата введения 01.02.2023) [Электронный ресурс]. URL: https://docs.cntd.ru/document/1200194981 (дата обращения: 25.10.2024).

10. МП №7 «Методические рекомендации по управлению риском информационной безопасности и обеспечению операционной надежности" (Дата публикации 21.03.2024) [Электронный ресурс]. URL: https://cbr.ru/Crosscut/LawActs/File/7712 (дата обращения: 25.10.2024).

11. Банк России ответил на вопросы по исполнению требований к защите информации [Электронный ресурс]. URL: https://asros.ru/dialog/information-security/the-bank-of-russia-answered-the-questions-in-compliance-with-the-requirements-to-information-protect/ (дата обращения: 21.08.2024).

12. ЦБ оценил объем похищенных кибермошенниками денег в 4,5 млрд руб [Электронный ресурс]. URL: https://tass.ru/ekonomika/18194805 (дата обращения: 26.09.2024).

13. Лившиц, И. И. Оценка уровня обеспечения информационной безопасности в кредитной организации / И. И. Лившиц // Стандарты и качество. – 2020. – № 7. – С. 44-49.

14. Иванов, А. В. Проблемы оценки доверия к процессам аудита информационной безопасности / А. В. Иванов, И. А. Огнев // Вопросы кибербезопасности. – 2024. – № 3(61). – С. 40-50. – DOI 10.21681/2311-3456-2024-3-40-50.

15. Как повысить оценку ГОСТ 57580: быстро, эффективно, с первого раза [Электронный ресурс]. URL: https://bi.zone/expertise/events/kak-povysit-otsenku-gost-57580-bystro-effektivno-s-pervogo-raza/ (дата обращения: 12.09.2024).

16. Беляев, Е. А. Модель управления информационной безопасностью кредитных организаций / Е. А. Беляев, И. И. Лившиц // Управление финансовыми рисками. – 2023. – № 3. – С. 180-194. – DOI 10.36627/2221-7541-2023-3-3-180-194.

References

1. STO BR IBBS-1.0-2014 (data vvedeniya ot 17.09.2014) [E`lektronny`j resurs]. URL: https://www.garant.ru/products/ipo/prime/doc/70567254/ysclid=lmel9rs33r25543875 (data obrashheniya: 13.08.2024).

2. Kiberugrozy` finansovoj otrasli: promezhutochny`e itogi 2023 goda [E`lektronny`j resurs]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/financial-industry-security-interim-2023/ (data obrashheniya: 26.08.2024).

3. Kak proverit` uchastnika finansovogo ry`nka [E`lektronny`j resurs]. URL: https://cbr.ru/finorg/ (data obrashheniya: 13.09.2024).

4. Koz`miny`x, S. I. Modelirovanie sistem i processov zashhity` informacii na ob``ektax kreditno-finansovoj sfery` / S. I. Koz`miny`x // Informacionnaya bezopasnost` finansovo-kreditny`x organizacij v usloviyax cifrovoj transformacii e`konomiki / Pod red. S.I. Koz`miny`x. – Moskva: Obshhestvo s ogranichennoj otvetstvennost`yu "Izdatel`stvo Prometej", 2020. – S. 320-412.

5. Sitskaya, A. V. Avtomatizaciya processa provedeniya audita posredstvom prilozheniya "Audit57580" / A. V. Sitskaya, V. V. Selifanov // Intellektual`ny`j potencial Sibiri: Sbornik nauchny`x trudov 29-oj Regional`noj nauchnoj studencheskoj konferencii, posvyashhennoj Godu nauki i texnologij v Rossii. V 5-ti chastyax, Novosibirsk, 17–21 maya 2021 goda / Pod redakciej D.O. Sokolovoj. Tom Chast` 5. – Novosibirsk: Novosibirskij gosudarstvenny`j texnicheskij universitet, 2021. – S. 607-614.

6. GOST R 57580.1-2017 «Bezopasnost` finansovy`x (bankovskix) operacij. Zashhita informacii finansovy`x organizacij. Bazovy`j nabor organizacionny`x i texnicheskix mer» (Data vvedeniya 08.08.2018) [E`lektronny`j resurs]. URL: https://docs.cntd.ru/document/1200146534 (data obrashheniya: 15.09.2024).

7. GOST R 57580.2-2018 «Bezopasnost` finansovy`x (bankovskix) operacij. Zashhita informacii finansovy`x organizacij. Metodika ocenki sootvetstviya» (Data vvedeniya 28.03.2018) [E`lektronny`j resurs]. URL: https://docs.cntd.ru/document/1200158801 (data obrashheniya: 15.09.2024).

8. GOST R 57580.3-2022 «Bezopasnost` finansovy`x (bankovskix) operacij. Upravlenie riskom realizacii informacionny`x ugroz i obespechenie operacionnoj nadezhnosti. Obshhie polozheniya» (Data vvedeniya 01.02.2023) [E`lektronny`j resurs]. URL: https://docs.cntd.ru/document/1200194981 (data obrashheniya: 25.10.2024).

9. GOST R 57580.4-2022 «Bezopasnost` finansovy`x (bankovskix) operacij. Obespechenie operacionnoj nadezhnosti. Bazovy`j sostav organizacionny`x i texnicheskix mer» (Data vvedeniya 01.02.2023) [E`lektronny`j resurs]. URL: https://docs.cntd.ru/document/1200194981 (data obrashheniya: 25.10.2024).

10. MP №7 «Metodicheskie rekomendacii po upravleniyu riskom informacionnoj bezopasnosti i obespecheniyu operacionnoj nadezhnosti" (Data publikacii 21.03.2024) [E`lektronny`j resurs]. URL: https://cbr.ru/Crosscut/LawActs/File/7712 (data obrashheniya: 25.10.2024).

11. Bank Rossii otvetil na voprosy` po ispolneniyu trebovanij k zashhite informacii [E`lektronny`j resurs]. URL: https://asros.ru/dialog/information-security/the-bank-of-russia-answered-the-questions-in-compliance-with-the-requirements-to-information-protect/ (data obrashheniya: 21.08.2024).

12. CzB ocenil ob``em poxishhenny`x kibermoshennikami deneg v 4,5 mlrd rub [E`lektronny`j resurs]. URL: https://tass.ru/ekonomika/18194805 (data obrashheniya: 26.09.2024).

13. Livshicz, I. I. Ocenka urovnya obespecheniya informacionnoj bezopasnosti v kreditnoj organizacii / I. I. Livshicz // Standarty` i kachestvo. – 2020. – № 7. – S. 44-49.

14. Ivanov, A. V. Problemy` ocenki doveriya k processam audita informacionnoj bezopasnosti / A. V. Ivanov, I. A. Ognev // Voprosy` kiberbezopasnosti. – 2024. – № 3(61). – S. 40-50. – DOI 10.21681/2311-3456-2024-3-40-50.

15. Kak povy`sit` ocenku GOST 57580: by`stro, e`ffektivno, s pervogo raza [E`lektronny`j resurs]. URL: https://bi.zone/expertise/events/kak-povysit-otsenku-gost-57580-bystro-effektivno-s-pervogo-raza/ (data obrashheniya: 12.09.2024).

16. Belyaev, E. A. Model` upravleniya informacionnoj bezopasnost`yu kreditny`x organizacij / E. A. Belyaev, I. I. Livshicz // Upravlenie finansovy`mi riskami. – 2023. – № 3. – S. 180-194. – DOI 10.36627/2221-7541-2023-3-3-180-194.

ЖУКОВА Марина Николаевна, кандидат технических наук, доцент, доцент кафедры «Безопасность информационных технологий» федерального государственного бюджетного образовательного учреждения высшего образования «Сибирский государственный университет науки и технологий имени академика Ф.М. Решетнева». 660037, Красноярский край, г. Красноярск, проспект имени газеты «Красноярский рабочий», д. 31. E-mail: zhukova@sibsau.ru

ЯКОВЛЕВА Анастасия Олеговна, аспирант федерального государственного бюджетного образовательного учреждения высшего образования «Сибирский государственный университет науки и технологий имени академика Ф.М. Решетнева». 660037, Красноярский край, г. Красноярск, проспект имени газеты «Красноярский рабочий», д. 31. E-mail: petrova_ao@sibsau.ru

ZHUKOVA Marina Nikolaevna, Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Information Technology Security of the Federal State Budgetary Educational Institution of Higher Education "Siberian State University of Science and Technology named after Academician F.M. Reshetnev". 660037, Krasnoyarsk Territory, Krasnoyarsk city, Avenue named after the newspaper "Krasnoyarsk Rabochiy", no. 31. E-mail: zhukova@sibsau.ru

IAKOVLEVA Anastasia Olegovna, post-graduate student of the Federal State Budgetary Educational Institution of Higher Education "Siberian State University of Science and Technology named after Academician F.M. Reshetnev". 660037, Krasnoyarsk Territory, Krasnoyarsk city, Avenue named after the newspaper "Krasnoyarsk Rabochiy", no. 31. E-mail: petrova_ao@sibsau.ru