Научная статья/Scientific article
УДК 004.056
http://dx.doi.org/10.26583/bit.2026.2.10
https://elibrary.ru/sinllb

ВНЕДРЕНИЕ ПОЛИТИКИ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Арсен Т. Абдуллаев[1], Сергей А. Резниченко[2]✉
[1,2]Финансовый университет при Правительстве Российской Федерации, Ленинградский пр-кт, 49, Москва, 125993, Россия
[2]Национальный исследовательский ядерный университет «МИФИ», Каширское ш., 31, Москва, 115409, Россия
✉rsa_5@bk.ru

Аннотация. Статья посвящена комплексному исследованию процесса формирования и внедрения политики реагирования на инциденты информационной безопасности в организациях, функционирующих в условиях постоянно растущего уровня как внешних, так и внутренних угроз. Обоснована необходимость системного подхода к организации процесса реагирования. Отмечается, что своевременность и корректность действий определяют масштаб возможного ущерба. Работа опирается на требования отечественных нормативно-правовых актов и международных стандартов, включая ГОСТ Р 59712-2022, ГОСТ Р ИСО/МЭК 27001 и 27035, что обеспечивает методологическую обоснованность подхода. Подробно рассмотрены функции группы реагирования на инциденты информационной безопасности, включая распределение ролей, регламенты взаимодействия, порядок уведомления и привлечение внешних структур. Значительное внимание уделено представлению жизненного цикла инцидента: от подготовки и обнаружения до восстановления и анализа последствий. Подчеркивается цикличность процесса реагирования, требование к совершенствованию мер защиты. В статье проводится анализ структуры плана реагирования, который включает общие положения, определения, порядок регистрации, классификации и расследования инцидентов, а также формы документирования результатов. Отдельно рассматриваются методы тестирования – от обзора до имитационного моделирования, что позволяют оценить готовность группы реагирования и релевантность применяемых процедур. Ключевым вкладом работы является формирование системы метрик эффективности реагирования, основанных на временных показателях и внутренних нормативах, что позволяет количественно оценивать оперативность и качество выполнения этапов обработки инцидентов. Предложенный алгоритм оценки обеспечивает адаптивность, многоуровневость и воспроизводимость анализа. Полученные результаты позволяют организациям эффективнее выстраивать процессы реагирования на инциденты, снижать ущерб от угроз и повышать устойчивость информационных систем.

Ключевые слова: *защита информации, инцидент безопасности, политика реагирования, жизненный цикл инцидента*

Для цитирования: Абдуллаев, А., Резниченко, С. (2026). Внедрение политики реагирования на инциденты информационной безопасности. *Безопасность информационных технологий,* 33(2), 94-105. doi: http://dx.doi.org/10.26583/bit.2026.2.10

IMPLEMENTATION OF AN INFORMATION SECURITY INCIDENT RESPONSE POLICY

Arsen T. Abdullaev[1], Sergey A. Reznichenko[2]✉
[1,2]Financial University under the Government of the Russian Federation, Leningradsky Ave., 49, Moscow, 125993, Russia
[2]National Research Nuclear University "MEPhI" (Moscow Engineering Physics Institute), Kashirskoe sh., 31, Moscow, 115409, Russia
✉rsa_5@bk.ru

Abstract. The article is devoted to a comprehensive study of the process of developing and implementing an information security incident response policy in organizations operating under conditions of a continuously increasing level of both external and internal threats. The necessity of a systematic approach to organizing the response process is substantiated. It is noted that the timeliness and correctness of actions determine the scale of potential damage. The work draws on the requirements of domestic regulatory acts and international standards, including GOST R 59712-2022 and GOST R ISO/IEC 27001 and 27035, ensuring the methodological soundness of the approach. The functions of an information security incident response team are examined in detail, including role allocation, interaction procedures, notification processes, and engagement of external entities. Significant attention is given to presenting the incident lifecycle – from preparation and detection to recovery and post-incident analysis. The cyclical nature of the response process and the need for continuous improvement of protective measures are emphasized. The article analyzes the structure of an incident response plan, which includes general provisions, definitions, procedures for incident registration, classification, and investigation, as well as documentation templates. Methods of testing – ranging from reviews to simulation modeling – are examined as tools for assessing the readiness of the response team and the relevance of implemented procedures. A key contribution of the study is the development of a system of response efficiency metrics based on temporal indicators and internal norms, enabling quantitative assessment of the timeliness and quality of incident handling stages. The proposed evaluation algorithm ensures adaptability, a multi-level structure, and reproducibility of analysis. The results obtained allow organizations to build more effective incident response processes, reduce threat-related damage, and increase the resilience of information systems.

Keywords: *information security, security incident, response policy, incident lifecycle*

For citation: Abdullaev, A., Reznichenko, S. (2026). Implementation of an information security incident response policy. *IT Security (Russia),* 33(2), 94-105. doi: http://dx.doi.org/10.26583/bit.2026.2.10

Введение

Своевременное выявление и корректное реагирование являются ключевыми элементами поддержания устойчивости и доверия к инфраструктуре организации в условиях нарастающих угроз [1]. Согласно ГОСТ Р 59709-2022 «Защита информации. Управление компьютерными инцидентами. Термины и определения» инцидентом информационной безопасности (ИБ) является непредвиденное или нежелательное событие или группа событий ИБ, что привели (могут привести) к нарушению функционирования информационного ресурса или возникновению угроз безопасности информации, нарушению требований по защите информации.

Разработка нормативной документации в сфере ИБ не ограничивается созданием политики ИБ. Нейтрализация инцидентов информационной безопасности, расследование причин реализации угроз и поддержание работоспособности системы защиты – основа политики реагирования на инциденты информационной безопасности [2, 3]. Специалистами профильного отдела организации формируются положения и регламенты, планы и инструкции, проводится проверка соответствия требованиям законодательных актов, ведутся журналы учёта объектов информационной системы (ИС).

Одна из функций ИС – мониторинг действий и операций, осуществляемых с конечных устройств в корпоративной сети организации. Отметим, что наличие аппаратных и программных средств защиты информации (СЗИ) не исключает возникновение инцидентов ИБ [4]. Необходимо не только фиксировать факт инцидента, но и оперативно, корректно реагировать на возникшее событие. Политика реагирования на инциденты ИБ обеспечивает согласованность действий между отделами организации, что способствует повышению готовности сотрудников к внештатным ситуациям и служит основой для совершенствования мер защиты [5].

Целью работы является рассмотрение процесса внедрения политики реагирования на инциденты информационной безопасности в организации, анализ этапов реагирования на инциденты и исследование оценки эффективности политики, основанной на совокупности

временных метрик, указанных в ГОСТ Р 59712-2022 и отражающих оперативность, согласованность и результативность действий при устранении инцидентов на всех этапах жизненного цикла инцидента. Также ставится цель определить унифицированный алгоритм оценки эффективности реагирования на инциденты ИБ.

1. Особенности формирования политики реагирования на инциденты информационной безопасности

Политика реагирования на инциденты информационной безопасности – комплексный нормативно-управленческий документ, регламентирующий порядок выявления, анализа и устранения инцидентов [5]. Существует ряд законодательных актов и методических документов, на которые стоит ориентироваться в ходе составления политики реагирования на инциденты ИБ (табл. 1).

Таблица 1. Перечень нормативных актов и стандартов в области ИБ

Документ	Основные положения
Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации»	Устанавливает общие принципы защиты информации, права и обязанности субъектов, требования к обеспечению конфиденциальности и доступности информации
Федеральный закон № 152-ФЗ «О персональных данных»	Определяет порядок получения, хранения, передачи и уничтожения персональных данных (ПДн), устанавливает обязанности операторов ПДн и меры защиты в зависимости от уровня угроз
Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»	Вводит классификацию объектов критической информационной инфраструктуры, обязанности операторов по мониторингу, защите и реагированию на инциденты, устанавливает взаимодействие с уполномоченными органами
Постановление Правительства РФ № 1119	Определяет требования к уровням защищенности ИСПДн, а также перечень организационных и технических мер по защите ПДн при их обработке
Приказ ФСТЭК России № 235	Описывает порядок построения систем безопасности, принципы функционирования и контроль за обеспечением защиты значимых объектов
ГОСТ Р ИСО/МЭК 27001-2021	Устанавливает требования к созданию, внедрению, поддержанию и совершенствованию системы менеджмента информационной безопасности (СМИБ), определяет подход к управлению рисками и выбору мер защиты информации, служит основой для сертификации систем ИБ организаций.
ГОСТ Р ИСО/МЭК 27035-1, 27035-2	Устанавливают методологию выявления, регистрации, анализа и реагирования на инциденты, а также порядок восстановления нормального функционирования ИТ-систем.
ГОСТ Р 59710-2022, ГОСТ Р 59711-2022, ГОСТ Р 59712-2022	Устанавливают единый комплекс требований к управлению компьютерными инцидентами: определяют общие принципы и этапы жизненного цикла инцидентов, регламентируют организацию деятельности (политика, план реагирования, распределение ролей, взаимодействие и учения), а также представляют порядок практического выявления, регистрации, анализа, реагирования, устранения последствий и восстановления нормального функционирования информационных систем.

На основе представленных документов организация разрабатывает внутренние регламенты, определяющие процедуры уведомления, классификации и расследования

инцидентов, порядок взаимодействия ответственных лиц, а также механизмы документирования и анализа последствий [3]. Отметим, что перечень актов и стандартов не является исчерпывающим, может дополняться в зависимости от отрасли.

Неотъемлемой частью любой политики являются лица, ответственные за реализацию предусмотренных мероприятий, координацию действий при возникновении инцидентов, принятие решений в критических ситуациях, а также за контроль исполнения установленных требований и процедур. Группа реагирования на инциденты информационной безопасности (ГРИИБ) состоит из специалистов, обладающих необходимыми компетенциями для выявления, анализа, локализации, устранения и документирования инцидентов [1, 2].

Состав группы включает специалистов по информационной безопасности, системных администраторов, юристов и представителей бизнес-подразделений. Каждый участник несёт ответственность за свою область – от технического анализа и устранения угроз до правового сопровождения и оценки влияния на бизнес-процессы. В структуре группы назначается координатор, уполномоченный принимать решения об эскалации инцидента и своевременно информировать руководство. Взаимодействие между членами ГРИИБ осуществляется по заранее утверждённым регламентам с использованием защищённых каналов связи. Проводятся регулярные тренировки, моделирование инцидентов и расследование произошедших инцидентов с целью совершенствования процедур реагирования [6, 7].

Группа привлекает внешних подрядчиков, уведомляет государственные регуляторы и взаимодействует с правоохранительными органами в соответствии с установленными требованиями и сроками уведомления. ГРИИБ задействована на всех этапах жизненного цикла инцидента ИБ (рис. 1). Отметим, что схема этапов жизненного цикла инцидентов основана на положениях ГОСТ Р 59712-2022, но представлена в более наглядной и логически сгруппированной форме, что позволяет отразить цикличность процесса и практическую последовательность действий.

Рис. 1. Этапы жизненного цикла инцидента ИБ

Рассмотрим элементы цикла:

1. *Подготовка к реагированию*. На данном этапе организацией определяются характеристики ИС, вид обрабатываемой информации, СЗИ, управление доступом к информации, создаются политики, регламенты и т.д.

2. *Обнаружение*. Момент, когда фиксируются признаки возможного инцидента информационной безопасности. Может быть выявлен средствами мониторинга, анализом журналов событий, сообщениями от сотрудников.

3. *Сбор информации*. Фиксируются журналы событий, сетевые логи, данные систем защиты и иные цифровые доказательства, позволяющие установить причины, ход и участников инцидента. На данном этапе необходимо соблюдать юридические нормы для дальнейшей обработки результатов.

4. *Реагирование*. Члены группы подтверждают подлинность инцидента, проводится первичная оценка источника, масштабов. Проводится классификация инцидента по степени критичности, оцениваются потенциальные риски для информационных ресурсов.

5. *Сдерживание*. Принимаются меры по ограничению распространения инцидента и минимизации его влияния на информационные ресурсы. Поражённые системы изолируются, блокируются уязвимые учетные записи или сетевые соединения, временно ограничивается доступ к затронутым сервисам.

6. *Оповещение*. Информируются пострадавшие пользователи, руководство организации и иные заинтересованные стороны о факте и характере инцидента. При необходимости уведомляются внешние структуры (регуляторы, партнёры или правоохранительные органы) в соответствии с установленными законодательными требованиями и внутренними процедурами. Необходимо обеспечить прозрачность и согласованность действий.

7. *Восстановление*. Подверженная компрометации часть ИС восстанавливается, при необходимости проходит процесс настройки. После завершения работ осуществляется проверка стабильности функционирования систем и подтверждается полное устранение инцидента.

8. *Документирование*. Регистрируются действия и решения для последующего анализа. Проводится оценка нанесённого ущерба и эффективности применённых процедур, что позволяет выявить слабые места и совершенствовать процесс управления инцидентами.

9. *Управление последствиями*. После оценки инцидента и на основе выявленных уязвимостей и нарушений рассматривается вопрос о совершенствовании методов защиты ИС. Также осуществляется оценка реагирования: как быстро и точно была локализована угроза, насколько адекватно были приняты меры по сдерживанию и восстановлению, какие решения оказались наиболее результативными.

Цикличность процесса заключается в постоянном внедрении и разработке мер противодействия угрозам – обновляются внутренние регламенты и инструкции, политики и планы, процедуры и средства защиты.

2. Формирование политики реагирования на инциденты информационной безопасности

При формировании документации в любой сфере деятельности стоит понимать, что в отличие от инструкций и руководств, политика – ориентир для принятия управленческих решений [5]. В ней закрепляются как ключевые определения и термины, так и цели и задачи, очерчиваются границы применения и распределяются сферы ответственности между участниками процесса. Неотъемлемой частью исследуемой политики является составление плана реагирования на инциденты, что включает детальное описание действий на различных этапах. Охватывается весь жизненный цикл инцидента, процедуры и уровни воздействия, схемы и координация действий между участниками процесса.

Документ одобряется руководством, включает способы обнаружения инцидента, анализа, локализации, ликвидации последствий, восстановление работоспособности после устранения угрозы. Актуализация политики реагирования на инциденты ИБ и тестирование плана должны проводится на регулярной основе в целях поддержания эффективности, соответствия текущим угрозам и изменениям в инфраструктуре организации [8].

План реагирования на инциденты представлен рядом разделов, структура плана может включать:

− *Общие положения*. Определяются цель и назначение документа, правовая основа для формирования политики. Указываются применимые законодательные акты, стандарты и внутренние документы, регулирующие обеспечение ИБ, а также область действия политики и категории информации, на которые она распространяется.

− *Определения*. Даётся определение ключевым терминам, что используются в сфере информационной безопасности и реагирования на инциденты, приводятся ключевые определения, с учётом терминологии, закреплённой в действующих стандартах и нормативных актах.

− *Область применения*. В данном разделе описывается область действия и полномочия политики, устанавливаются границы применения, а также порядок взаимодействия и взаимосвязь с другими внутренними документами организации, регулирующими вопросы информационной безопасности и управления инцидентами.

− *Ответственные лица.* Определяется круг должностных лиц, входящих в ГРИИБ. Участники группы отвечают за обработку инцидентов, поддержание и актуализацию документации. Прописываются права и обязанности сотрудников, согласно их должностным регламентам.

− *Регистрация инцидентов ИБ*. Раздел определяет, какие инциденты подлежат учёту, кто отвечает за их регистрацию и какие данные фиксируются. Обнаружение может осуществляться как автоматически (средствами мониторинга, антивирусами, системами IDS/IPS), так и вручную через сообщения сотрудников, результаты аудитов или уведомления внешних источников.

− *Реагирование на инциденты и устранение последствий*. Локализацию и первичные меры может выполнять ответственный администратор ИБ, а при комплексных инцидентах – ГРИИБ. Проводится оценка, устраняются последствия и разрабатываются меры по предотвращению.

− *Расследование инцидентов.* Администратор ИБ и ГРИИБ выявляют недостатки в системе защиты, проводят сбор и анализ информации, устанавливают каналы атаки и уязвимости. Ответственность за инцидент могут нести как сотрудники организации, так и внешние нарушители.

− *Оформление результатов реагирования на инциденты.* Формируется акт об инциденте с детальным описанием произошедшего, способа реализации, причин, воздействия, связанных активов, даты возникновения и устранения, типом угрозы. Разрабатываются рекомендации по совершенствованию организационных и технических мер защиты информации. Информация об инциденте заносится в Журнал учета инцидентов информационной безопасности (Журнал учета событий информационной безопасности).

− *Приложения.* Документация может содержать шаблоны для заполнения информации об инцидентах. Необходимо включить в план: карточку инцидента ИБ, форму журнала учета инцидентов ИБ (Форму отчета об инциденте ИБ).

Внедрение плана реагирования не обходится без обучения сотрудников, тестирования ИС и моделирования инцидентов. Обучение позволяет отработать действия при реализации инцидентов различного уровня, а элементы тестирования предназначены для выявления уязвимостей. Рекомендуется устанавливать регулярный интервал пересмотра (например, один раз в год), а также внеплановый пересмотр по решению ответственных лиц в случае существенных изменений в архитектуре ИС или политике ИБ.

Помимо этого, руководство по реагированию включает не только пошаговые инструкции, но и описания типовых сценариев атак, схем взаимодействия между ответственными лицами и критерии принятия решений в условиях неопределенности [9]. Предусматривается градация типов инцидентов по уровню критичности и потенциальному ущербу. Руководство содержит перечень используемых инструментов и технических средств, рекомендации по их применению на различных этапах реагирования. Также описываются процедуры анализа после восстановления ИС.

3. Оценка эффективности политики реагирования на инциденты информационной безопасности

Периодическое тестирование составленного плана реагирования на инциденты ИБ является ключевым условием для определения эффективности политики реагирования. В первую очередь, стоит оценить объем охватываемых типов данных. Проверка также заключается в анализе релевантности сценариев нарушений, методов реагирования, актуальности процедур восстановления, типов доказательств реализации инцидентов.

Существуют следующие виды тестирования:

− *Обзор*. Пошаговое рассмотрение пунктов. Поиск ошибок, процедурных проблем. Однако, данный тест не позволяет проверить возможности ГРИИБ и оценить эффективность инструкций реагирования на инциденты [6, 13].

− *Мозговой штурм*. Данный способ представляет собой обсуждение, сосредоточенное на ролях и зонах ответственности членов ГРИИБ, на регламентацию действий в случае реализации инцидентов. По результатам тестирования формулируются должностные обязанности сотрудников, вносятся корректировки в план реагирования при необходимости. Ограничения состоят в общем взгляде на план, навыках и ресурсах членов ГРИИБ.

− *Имитационное моделирование.* Производится полный пошаговый разбор плана, имитируется ситуация реализации инцидента в тестовой среде, участвуют члены ГРИИБ [7, 12].

Целью тестирования является выявление слабых сторон плана и коммуникации между участниками. Целью также может быть проверка компетентности членов ГРИИБ, корректность распределения ролей и полномочий, эффективность управления инцидентом в рамках бизнес-процессов.

Следует предусмотреть и непредвиденные события в сценариях, т.к. расследование инцидента редко проходит без сбоев. Внештатные ситуации могут быть связаны с коммуникацией внутри команды и одобрением мер по локализации инцидента. Отвлекающий элемент – ограничения по времени, ресурсам. Возможны проблемы с технической точки зрения, утечка информации в СМИ. Тестирования позволяют проверить реакцию ГРИИБ и устойчивость процессов реагирования в условиях неопределенности.

Метрики эффективности измеряют результативность составленного плана [10]. Сбор и анализ показателей позволяют выявить тенденции (нехватка ресурсов, отсутствие полномочий, уровня знаний в области). Документирование и расчет, детализация метрик и введение новых критериев оценки позволяют получить более глубокое понимание работы плана реагирования на инциденты ИБ [11, 14].

Показатели для оценки эффективности политики реагирования на инциденты ИБ выглядят следующим образом:

Среднее время проведения проверки признаков возможного возникновения инцидентов. Этот показатель определяет среднее время от момента получения первичных данных (логов) до момента подтверждения/опровержения наличия признаков инцидентов. Если есть количество инцидентов n, для каждого известна длительность проверки возникновения:

$$T_{\text{проверки}} = \frac{1}{n}\sum_{i=1}^{n}(t_i^{\text{конец проверки}} - t_i^{\text{начало проверки}}).$$

Среднее время определения вовлечённых в инцидент элементов ИС. Отражает среднее время, затрачиваемое на определение всех систем, узлов, сервисов, пользователей и иных элементов, вовлечённых в инцидент, начиная от момента подтверждения инцидента. Если для каждого инцидента известно время начала и завершения определения вовлечённых элементов, тогда:

$$T_{\text{идентификации}} = \frac{1}{n}\sum_{i=1}^{n}(t_i^{\text{конец идентификации}} - t_i^{\text{начало идентификации}}).$$

Среднее время локализации инцидентов. Показывает, сколько времени требуется для локализации инцидента – остановки его распространения. Если известны моменты обнаружения инцидента и завершения локализации:

$$T_{\text{локализации}} = \frac{1}{n}\sum_{i=1}^{n}(t_i^{\text{завершения локализации}} - t_i^{\text{обнаружение}}).$$

Среднее время выявления последствий инцидентов. Определяет время, требуемое для анализа последствий (ущерба, затронутых данных, масштабов воздействия). Если известны время начала и окончания анализа последствий:

$$T_{\text{выявления последствий}} = \frac{1}{n}\sum_{i=1}^{n}(t_i^{\text{конец анализа}} - t_i^{\text{начало анализа}}).$$

Среднее время ликвидации последствий инцидентов. Время, требуемое для устранения последствий инцидента и восстановления нормального функционирования информационной системы. Если известны время начала и окончания работ по ликвидации:

$$T_{\text{ликвидации}} = \frac{1}{n}\sum_{i=1}^{n}(t_i^{\text{конец ликвидации}} - t_i^{\text{начало ликвидации}}).$$

Среднее время реагирования на инциденты. Характеризует общее время от момента получения первичного уведомления до полного закрытия инцидента. Если известны моменты поступления сообщения и завершения реагирования:

$$T_{\text{реагирования}} = \frac{1}{n}\sum_{i=1}^{n}(t_i^{\text{закрытие инцидента}} - t_i^{\text{обнаружение инцидента}}).$$

Процент компьютерных инцидентов, для которых были нарушены сроки выполнения этапов реагирования. Если долю инцидентов, по которым хотя бы один из этапов реагирования (проверка, анализ, локализация, ликвидация) был выполнен дольше установленного норматива. Если k – число инцидентов с нарушениями сроков, а n – общее число инцидентов, то:

$$P_{\text{нарушений}} = \frac{k}{n} \times 100\%.$$

На основе временных метрик, что закреплены в ГОСТ Р 59712-2022, можно составить следующий алгоритм оценки эффективности реагирования на инциденты ИБ, который будет единообразен вне зависимости от рода деятельности организации (рис. 2). В отличие от традиционной оценки, которая ограничивается фиксацией длительности отдельных этапов, представленный алгоритм рассматривает процесс реагирования как взаимосвязанную систему, включающую подготовку, взаимодействие участников, использование инструментов и последующее улучшение регламентов [13].

Для воспроизведения алгоритма требуется наличие системы мониторинга и сбора данных в организации. В свою очередь, алгоритм оценивает способность организации стабильно обеспечивать своевременное реагирование при различных условиях: изменении нагрузки, сложности атаки, ограниченности ресурсов или неполноте исходных данных.

Выделим ключевые принципы алгоритма:

- *Многоуровневость*. Каждый этап жизненного цикла инцидента ИБ рассматривается как отдельный измеряемый процесс, а итоговая оценка формируется с учётом взаимосвязи этапов [14, 15];
- *Нормируемые критерии качества*. Определяются не только временные нормативы, но и критерии качества выполнения (полнота собранных данных, корректность классификации инцидента, обоснованность выбранных мер сдерживания);
- *Адаптивность.* Алгоритм предполагает возможность корректировки нормативов и процедур на основе результатов анализа инцидентов, изменений инфраструктуры и появления новых угроз, обеспечивая непрерывное совершенствование процесса реагирования.

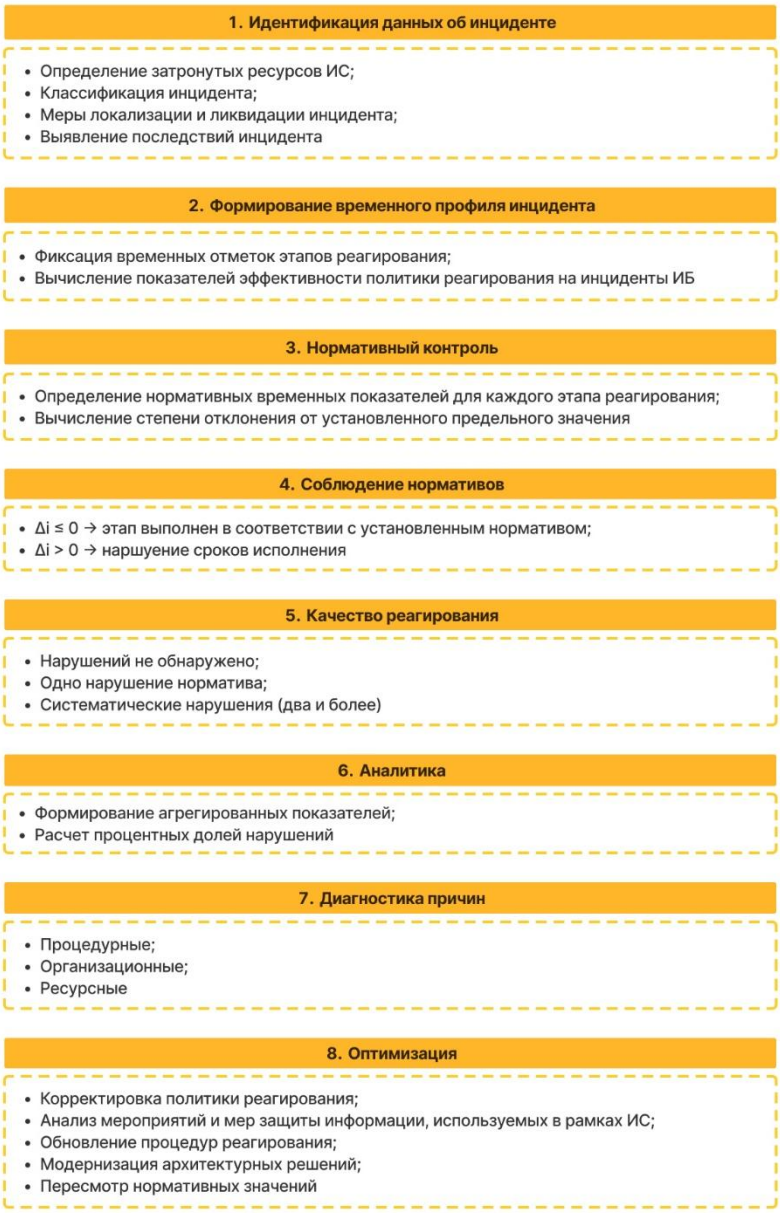

Рис. 2. Алгоритм оценки эффективности реагирования на инциденты

В рассматриваемом алгоритме представлены нормативы – инструмент количественной оценки эффективности реагирования. Нормативы S_i, определяющие предельно допустимые сроки выполнения этапов реагирования на инциденты ИБ, устанавливаются организацией самостоятельно. Формирование данных нормативов осуществляется с учётом уровня критичности информационных активов и бизнес-процессов, объёма и структуры ИС, а также ресурсов и функциональных возможностей ГРИИБ. В процессе разработки нормативов учитываются статистические данные о фактическом времени обработки инцидентов, классификация событий по уровням критичности, возможности автоматизации и квалификация персонала.

Нормативы S_i устанавливаются специалистами ГРИИБ: оцениваются оптимальные сроки для выполнения каждого этапа реагирования на инциденты с учетом уровня критичности инцидента, особенностей ИС, воздействия на рабочие процессы. В условиях недостаточности статистических данных экспертная оценка позволяет учесть специфику организации. Чем выше уровень критичности, тем нормативы будут более строгими [16]. При проведении оценки специалисты ГРИИБ должны учитывать уровень автоматизации процессов предприятия. На основе полученных оценок команда реагирования на инциденты проводит обсуждение и определяет общие нормативы для каждого этапа. Документ,

содержащий установленные нормативы, утверждается руководством. Регулярный пересмотр нормативов позволяет адаптировать алгоритм как к изменениям в ИС организации, так и к новым угрозам и выявленным уязвимостям.

Для оценки соответствия длительности каждого этапа установленным внутренним нормативам предлагается использовать показатель фактического превышения норматива. В отличие от абсолютных временных метрик, отражающих лишь продолжительность этапа реагирования, данный показатель позволяет количественно определить степень отклонения от установленного предельного значения S_i, заданного организацией для соответствующего этапа обработки инцидента. Фактическое превышение норматива для отдельного инцидента рассчитывается по формуле:

$$\Delta_i = t_i - S_i,$$

где t_i – фактическое время выполнения i-го этапа; S_i – установленный норматив времени выполнения данного этапа.

Интерпретация показателя Δ_i:

- $\Delta_i < 0$ (этап выполнен быстрее установленного норматива);
- $\Delta_i = 0$ (этап завершён строго в пределах установленного времени);
- $\Delta_i > 0$ (норматив превышен, нарушение сроков выполнения).

Использование данного показателя позволяет не только фиксировать факт нарушения нормативов, но и количественно оценивать величину отклонения времени реагирования на инциденты.

Таким образом, представленная система метрик и унифицированный алгоритм их применения позволяют перейти от декларативной оценки эффективности реагирования к объективно измеримому и воспроизводимому анализу процессов. Использование временных нормативов, показателей превышения и комплексного сопоставления этапов жизненного цикла инцидента обеспечивает прозрачность результатов, повышает точность выявления уязвимых элементов ИС, политик ИБ и реагирования на инциденты ИБ, способствует формированию адаптивной модели управления инцидентами ИБ.

Заключение

В ходе исследования проведён комплексный анализ теоретических и практических основ формирования и внедрения политики реагирования на инциденты информационной безопасности. В соответствии с задачей анализа этапов реагирования уточнена и структурирована модель жизненного цикла инцидента, основанная на положениях ГОСТ Р 59712-2022. Детализированы функции группы реагирования, принципы распределения ролей и взаимодействия между участниками, что сформировало целостное понимание организационного и нормативного аспекта построения процесса реагирования.

Сформирована комплексная система измеряемых показателей, охватывающая все этапы жизненного цикла инцидента и позволяющая объективно оценивать оперативность и результативность действий группы реагирования. Предложенный многоуровневый алгоритм оценки эффективности реагирования на инциденты ИБ, основанный на нормативах и показателях, создаёт основу для адаптивного управления процессами реагирования.

Полученные результаты могут быть использованы при формировании политики реагирования на инциденты ИБ, разработке планов реагирования и регламентов работы группы реагирования. Представленные рекомендации и предложенные методические подходы обеспечивают повышение устойчивости информационных систем, снижение последствий реализации угроз и повышение уровня защищённости организаций.

СПИСОК ЛИТЕРАТУРЫ/REFERENCES:

1. Дёмина А.К., Управление инцидентами информационной безопасности. Международный журнал гуманитарных и естественных наук. 2024, № 5-1(92), с. 227-231. DOI: https://doi.org/10.24412/2500-1000-2024-5-1-227-231.

Demina A.K., Information security incident management. International Journal of Humanities and Natural Sciences. 2024, no. 5-1(92), pp. 227-231. DOI: https://doi.org/10.24412/2500-1000-2024-5-1-227-231 (in Russian).
2. Кузнецов А.В., Методология реагирования на инциденты информационной безопасности в распределенных автоматизированных информационных системах. Вопросы кибербезопасности. 2025, № 4(68), с. 65-72. DOI: https://doi.org/10.21681/2311-3456-2025-4-65-72.
Kuznetsov A.V., The methodology of information security incidents response within distributed automated information systems. Cybersecurity issues. 2025, no. 4(68), pp. 65-72. DOI: https://doi.org/10.21681/2311-3456-2025-4-65-72 (in Russian).
3. Олейникова А.А., Золотарев В.В., Концепция управления информационной безопасностью на основе цикла непрерывного детектирования и реагирования на инциденты безопасности информации. Известия ЮФУ. Технические науки. 2023, № 5(235), с. 66-81. DOI: https://doi.org/10.18522/2311-3103-2023-5-66-81.
Oleinikova A.A., Zolotarev V.V., The concept of information security management based on a cycle of continuous detection and response to information security incidents. Izvestiya SFU. Technical sciences. 2023, no. 5(235), pp. 66-81. DOI: https://doi.org/10.18522/2311-3103-2023-5-66-81 (in Russian).
4. Козьминых С.И., Борисов С.А. Обеспечение комплексной защиты объектов информатизации. Москва: КноРус. 2024. 248 с. ISBN 978-5-406-11906-8. EDN: XGWZOL.
Kozminykh S.I., Borisov S.A., Obespechenie kompleksnoy zashchity obektov informatizatsii. Moscow: KnoRus. 2024. 248 p. ISBN 978-5-406-11906-8. EDN: XGWZOL (in Russian).
5. Милославская Н.Г., Толстой А.И., Управление рисками информационной безопасности 3-е изд. Москва: Горячая линия-Телеком. 2023. 224 с. ISBN 978-5-9912-0962-5.
Miloslavskaya N.G., Tolstoy A.I., Upravlenie riskami informatsionnoy bezopasnosti. 3rd ed. Moscow: Goryachaya Liniya-Telekom. 2023. 224 p. ISBN 978-5-9912-0962-5 (in Russian).
6. Прокушев Я.Е., Пономаренко С.В., Шишов Н.В. Моделирование процессов проектирования систем защиты информации в критических информационных инфраструктурах. Computational nanotechnology. 2022, № 9(2), с. 45-55. DOI: https://doi.org/10.33693/2313-223x-2022-9-2-45-55.
Prokushev Y.E., Ponomarenko S.V., Shishov N.V., The Modeling of Processes of Design of Information Protection Systems in Critical Information Infrastructures. Computational nanotechnology. 2022, no. 9(2), pp. 45-55. DOI: https://doi.org/10.33693/2313-223x-2022-9-2-45-55 (in Russian).
7. Прокушев Я.Е., Пономаренко С.В., Максимов Р.Р. Моделирование процессов проектирования систем защиты информации в банковских информационных системах. Computational nanotechnology. 2023, № 10(4), с. 23-38. DOI: https://doi.org/10.33693/2313-223x-2023-10-4-23-38.
Prokushev Y.E., Ponomarenko S.V., Maksimov R.R., The Modeling of Processes of Design of Information Protection Systems in Financial Information Systems. Computational nanotechnology. 2023, no. 10(4), pp. 23-38. DOI: https://doi.org/10.33693/2313-223x-2023-10-4-23-38 (in Russian).
8. Brezavšček A., Baggia A. Recent Trends in Information and Cyber Security Maturity Assessment: A Systematic Literature Review. Systems. 2025, no.13(52), pp. 1-42. DOI: https://doi.org/10.3390/systems13010052.
9. Pigola, A., da Costa, P.R., Vils, L., Meirelles, F. de S. Enhancing information security management and performance through social and relational factors: a structural equation modelling approach. Behaviour & Information Technology. 2025, pp. 1-23. DOI: https://doi.org/10.1080/0144929X.2025.2522206.
10. Рытов М.Ю., Голембиовская О.М., Кондрашова Е.В., Порядок оценки уровня эффективности системы непрерывного противодействия инцидентам информационной безопасности на объекте. Информация и безопасность. 2024, №27(1), с. 135-142. DOI: https://doi.org/10.36622/1682-7813.2024.27.1.011.
Rytov M. Yu., Golembiovskaya O.M., Kondrashova E.V., The procedure for assessing the level of effectiveness of the system of continuous counteraction to information security incidents at the facility. Information and Security. 2024, no. 27(1), pp. 135-142. DOI: https://doi.org/10.36622/1682-7813.2024.27.1.011 (in Russian).
11. Резниченко С.А., Турабов Д.Р., Методология выбора критериев эффективности системы информационной безопасности при имитационных атаках Red Team. Вестник Дагестанского государственного технического университета. Технические науки. 2025, 52(3), с. 135-151. DOI: https://doi.org/10.21822/2073-6185-2025-52-3-135-151.
Reznichenko S.A., Turabov D.R. Methodology for selecting effectiveness criteria of information Security Systems during Red Team simulated attacks. Herald of Dagestan State Technical University. Technical Sciences. 2025, 52(3), pp. 135-151. DOI: https://doi.org/10.21822/2073-6185-2025-52-3-135-151 (in Russian).
12. Хуранова, К., Кологоров, И., Резниченко, С., Кессаринский, Л. (2025). Применение среды AnyLogic для моделирования и анализа процесса аудита информационной безопасности. Безопасность информационных технологий, 32(2), 21-31. DOI: https://doi.org/10.26583/bit.2025.2.02.
Khuranova, K., Kologorov, I., Reznichenko, S., Kessarinskiy, L. (2025). Using the AnyLogic environment for modeling and analysis of the information security audit process. IT Security (Russia), 32(2), 21-31. DOI: https://doi.org/10.26583/bit.2025.2.02 (in Russian).
13. Трофимов Д.О., Шепелев М.С., Резниченко С.А., Организация реагирования на инциденты информационной безопасности. Вестник Дагестанского государственного технического университета. Технические науки. 2023;50(4):148-157. DOI: https://doi.org/10.21822/2073-6185-2023-50-4-148-157.

Trofimov D.O., Shepelev M.S., Reznichenko S.A. Organization of response to information security incidents. Herald of Dagestan State Technical University. Technical Sciences. 2023;50(4):148-157. DOI: https://doi.org/10.21822/2073-6185-2023-50-4-148-157 (in Russian).

14. Александрова П.С., Червинчук А.С., Резниченко С.А., Проверка соответствия банковской системы требованиям к защите информации в платежной системе. Вестник РГГУ. Серия: Информатика. Информационная безопасность. Математика. 2024, № 3, с. 39-55. DOI: https://doi.org/10.28995/2686-679X-2024-3-39-55.
Alexandrova P.S., Chervinchuk A.S., Reznichenko S.A., Checking the compliance of the banking system with the requirements for the protection of information in the payment system. Vestnik RGGU. Seriya: Informatika. Informatsionnaya bezopasnost. Matematika [RGGU Bulletin. Series: Informatics. Information Security. Mathematics]. 2024, no. 3, pp. 39-55. DOI: https://doi.org/10.28995/2686-679X-2024-3-39-55 (in Russian).
15. Гавришев А.А., Резниченко С.А., Упрощённый концептуальный проект системы беспроводной идентификации и контроля доступа на критически важных объектах. Технологии техносферной безопасности. 2024, № 1(103), с. 164-177. DOI: https://doi.org/10.25257/TTS.2024.1.103.164-177.
Gavrishev A.A., Reznichenko S.A. Simplified conceptual design of a wireless identification and access control system for critical facilities. Tekhnologii tekhnosfernoi bezopasnosti [Technologies for Technosphere Safety]. 2024, no.1(103), pp. 164-177. DOI: https://doi.org/10.25257/TTS.2024.1.103.164-177 (in Russian).
16. Salfati, E., Pease, M., Digital Forensics and Incident Response (DFIR) Framework for Operational Technology (OT), NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg. 2022. DOI: https://doi.org/10.6028/NIST.IR.8428.

Конфликт интересов. *Авторы заявляют об отсутствии конфликта интересов.*
Conflict of interest. *The authors declare no conflict of interest.*

Вклад авторов

Абдуллаев А.Т.: *разработка методов и процедур; написание первоначального текста статьи, создание графиков, схем, иллюстраций.*

Резниченко С.А.: *формулирование идеи, гипотезы, цели исследования; редактирование, доработка текста.*

Author Contributions

Abdullaev A.T.: *methodology, writing – original draft, visualization.*

Reznichenko A.A.: *Conceptualization, writing – review & editing.*

ИНФОРМАЦИЯ ОБ АВТОРАХ:

Арсен Темирланович Абдуллаев, *магистр, Финансовый университет при Правительстве Российской Федерации.*
e-mail: 241289@edu.fa.ru,
https://orcid.org/0009-0001-6839-2501
SPIN-код: 7388-6546
Researcher ID: PMQ-8377-2026

Сергей Анатольевич Резниченко, *к.т.н., доцент; доцент, Финансовый университет при Правительстве Российской Федерации; доцент, Национальный исследовательский ядерный университет «МИФИ».*
e-mail: rsa_5@bk.ru,
https://orcid.org/0000-0002-1539-0457,
Scopus Author ID: 57255344400,
SPIN-код: 6229-0476,
Researcher ID: PMQ-8315-2026

INFORMATION ABOUT THE AUTHORS:

Arsen Temirlanovich Abdullaev, *Master's student, Financial University under the Government of the Russian Federation.*
e-mail: 241289@edu.fa.ru,
https://orcid.org/0009-0001-6839-2501
SPIN-code: 7388-6546
Researcher ID: PMQ-8377-2026

Sergey Anatolyevich Reznichenko, *PhD (Tech.), Associate Professor; Associate Professor, Financial University under the Government of the Russian Federation; Associate Professor, National Research Nuclear University MEPhI (Moscow Engineering Physics Institute).*
e-mail: rsa_5@bk.ru,
https://orcid.org/0000-0002-1539-0457,
Scopus Author ID: 57255344400,
SPIN-code: 6229-0476,
Researcher ID: PMQ-8315-2026

Статья поступила в редакцию 21.12.2025; одобрена после рецензирования 27.02.2026; принята к публикации 26.03.2026
The article was submitted 21.12.2025; approved after reviewing 27.02.2026; accepted for publication 26.03.2026