Russian Technological Journal.
2024;12(6):39–47

ISSN 2782-3210 (Print)
ISSN 2500-316X (Online)

УДК 004.056.5
https://doi.org/10.32362/2500-316X-2024-12-6-39-47
EDN IYBIZH

НАУЧНАЯ СТАТЬЯ

Моделирование процессов управления инцидентами информационной безопасности на предприятии

Е.С. Митяков [@],
Е.А. Максимова,
С.В. Артемова,
А.А. Бакаев,
Ж.Г. Вегера

МИРЭА – Российский технологический университет, Москва, 119454 Россия
[@] Автор для переписки, e-mail: mityakov@mirea.ru

Резюме

Цели. Основной целью исследования является разработка модели управления инцидентами информационной безопасности на предприятии, минимизирующей ущерб и затраты на устранение инцидентов в условиях ограниченных ресурсов и времени.

Методы. В работе проведен анализ существующих подходов к управлению инцидентами информационной безопасности, включая математические и имитационные модели, стохастические дифференциальные уравнения, цепи Маркова и другие методы. Основанием для работы послужил системный подход, который включает в себя всесторонний анализ параметров инцидентов, действий по их устранению, времени реакции, а также ущерба от реализации инцидентов и вероятности успешного их устранения. Для проверки работоспособности разработанной модели использовались синтетические данные, которые отражают разнообразные типы инцидентов и возможные пути их ликвидации.

Результаты. Предложенная модель управления инцидентами позволяет оптимизировать управление инцидентами за счет минимизации ущерба и затрат. В рамках модели учитываются такие параметры, как критичность инцидентов, доступные ресурсы, время реакции и вероятность успешного устранения инцидентов. Апробация модели на синтетических данных показала, что предложенный подход существенно улучшает выбор оптимальных действий для реагирования на инциденты в ситуациях ограничений бюджета и времени, что в свою очередь повышает общую эффективность управления инцидентами.

Выводы. Внедрение предложенной модели на предприятиях позволит повысить общий уровень информационной безопасности, эффективность реагирования на инциденты и улучшить процессы защиты информации. Это обеспечит минимизацию рисков, связанных с утечками данных и другими инцидентами, и поможет предприятиям принимать обоснованные и оперативные решения в условиях ограниченных ресурсов и времени.

Ключевые слова: управление инцидентами, информационная безопасность, моделирование инцидентов, минимизация ущерба, ограниченные ресурсы, математическое моделирование, оптимизация

• **Поступила:** 12.09.2024 • **Доработана:** 30.09.2024 • **Принята к опубликованию:** 14.10.2024

Для цитирования: Митяков Е.С., Максимова Е.А., Артемова С.В., Бакаев А.А., Вегера Ж.Г. Моделирование процессов управления инцидентами информационной безопасности на предприятии. *Russ. Technol. J.* 2024;12(6):39–47. https://doi.org/10.32362/2500-316X-2024-12-6-39-47

Прозрачность финансовой деятельности: Авторы не имеют финансовой заинтересованности в представленных материалах или методах.

Авторы заявляют об отсутствии конфликта интересов.

RESEARCH ARTICLE

Modeling incident management processes in information security at an enterprise

Evgeny S. Mityakov [@],
Elena A. Maksimova,
Svetlana V. Artemova,
Anatoly A. Bakaev,
Zhanna G. Vegera

MIREA – Russian Technological University, Moscow, 119454 Russia
[@] Corresponding author, e-mail: mityakov@mirea.ru

Abstract

Objectives. The primary aim of the study is to develop a model for managing information security incidents within an enterprise that minimizes damage and costs associated with incident resolution under limited resources and time constraints.

Methods. The paper analyzes existing approaches to managing information security incidents, including mathematical and simulation models, stochastic differential equations, Markov chains, and other methods. The study is based on a systems approach, incorporating analysis of incident parameters, actions for their resolution, response times, damages due to incident occurrence, and the probability of incident elimination. To validate the developed model, synthetic data reflecting various types of incidents and possible actions were used.

Results. The proposed model optimizes incident management by minimizing damage and costs. It considers parameters such as incident criticality, available resources, response time, and the likelihood of successful incident resolution. Testing of the model on synthetic data showed that the proposed approach significantly improves the selection of optimal actions for responding to incidents in situations constrained by budget and time limitations, thereby enhancing the overall effectiveness of incident management.

Conclusions. Implementing the proposed model in enterprises will improve the overall level of information security, enhance incident response efficiency, and strengthen information protection processes. This will ensure the minimization of risks associated with data leaks and other incidents, thus helping enterprises to make informed and timely decisions under conditions of limited resources and time.

Keywords: incident management, information security, incident modeling, damage minimization, limited resources, mathematical modeling, optimization

• **Submitted:** 12.09.2024 • **Revised:** 30.09.2024 • **Accepted:** 14.10.2024

For citation: Mityakov E.S., Maksimova E.A., Artemova S.V., Bakaev A.A., Vegera Zh.G. Modeling incident management processes in information security at an enterprise. *Russ. Technol. J*. 2024;12(6):39–47. https://doi.org/10.32362/2500-316X-2024-12-6-39-47

Financial disclosure: The authors have no financial or proprietary interest in any material or method mentioned.

The authors declare no conflicts of interest.

ВВЕДЕНИЕ

Управление инцидентами информационной безопасности на предприятии – это процесс идентификации, анализа и реагирования на инциденты, связанные с информационными системами и данными, который включает в себя комплекс мероприятий по предотвращению, минимизации ущерба и восстановлению нормального функционирования систем после инцидентов.

В современных реалиях данный процесс выступает ключевым аспектом обеспечения информационной безопасности организации. Сегодня предприятия сталкиваются с множеством угроз – от кибератак и несанкционированного доступа к данным до утечек информации. Названные угрозы влекут за собой финансовые потери и подрыв репутации компании. Поэтому надлежащее управление инцидентами информационной безопасности на предприятии выступает неотъемлемой частью его общей стратегии безопасности. Такое управление позволяет, во-первых, обеспечить оперативную реакцию на текущие угрозы, и, во-вторых, сформировать проактивный подход к прогнозированию и предотвращению потенциальных инцидентов информационной безопасности.

В Российской Федерации управление инцидентами информационной безопасности регламентируется рядом государственных стандартов. Один из них, ГОСТ Р 59712-2022[1], посвящен управлению инцидентами компьютерной безопасности, что является более узкой областью в рамках информационной безопасности. Этот стандарт описывает структурированный подход к обнаружению, регистрации, реагированию и анализу инцидентов в рамках государственной системы ГосСОПКА[2]. В свою очередь, ГОСТ Р ИСО/МЭК ТО 18044-2007[3] охватывает более широкий спектр инцидентов информационной безопасности, устанавливая требования к их документированию, правовой экспертизе, взаимодействию с органами и адаптации к современным угрозам. Однако в названных стандартах не учитываются механизмы оценки ущерба от инцидентов и затрат на их устранение, что ограничивает их применение в условиях, когда критичны время и ресурсы.

В данной работе рассматриваются процессы управления инцидентами информационной безопасности на предприятии, с акцентом на анализ существующих подходов и моделей, направленных на оптимизацию затрат на устранение последствий, повышение оперативности реагирования на инциденты и минимизацию ущерба. Основной целью статьи является разработка модели, которая систематизирует процесс управления инцидентами и помогает повысить эффективность принятия решений в условиях ограниченных ресурсов и времени.

УПРАВЛЕНИЕ ИНЦИДЕНТАМИ В СИСТЕМЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Управление инцидентами информационной безопасности имеет решающее значение для поддержания целостности, конфиденциальности и доступности данных предприятия. Эффективное управление инцидентами включает в себя выявление, реагирование и извлечение уроков из инцидентов безопасности для улучшения общего состояния безопасности. Инцидент в контексте информационной безопасности – это любое событие или действие, которое наносит или потенциально может нанести вред конфиденциальности, целостности или доступности информации и информационных систем. Инциденты могут варьироваться от случайных ошибок до целенаправленных атак, и их последствия могут быть достаточно серьезными для организаций.

Примеры инцидентов включают вирусные атаки, утечки данных, DDoS-атаки[4], несанкционированный

[1] ГОСТ Р 59712-2022. Национальный стандарт Российской Федерации. *Защита информации. Управление компьютерными инцидентами. Руководство по реагированию на компьютерные инциденты*. М.: Стандартинформ; 2023. 20 с. [GOST R 59712-2022. National Standard of the Russian Federation. *Information protection. Computer incident management. Guide to responding to computer incident*. Moscow: Standartinform; 2023. 20 p. (in Russ.).]

[2] https://gossopka.ru/ (in Russ.). Дата обращения 15.07.2024. / Accessed July 15, 2024.

[3] ГОСТ Р ИСО/МЭК ТО 18044-2007. Национальный стандарт Российской Федерации. *Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности*. М.: Стандартинформ; 2008. 50 с. [GOST R ISO/IEC TO 18044-2007. National Standard of the Russian Federation. *Information technology. Security techniques. Information security incident management*. Moscow: Standartinform; 2008. 50 p. (in Russ.).]

[4] Distributed denial of service – распределенный отказ в обслуживании.

доступ и др. Существуют различия между инцидентами и простыми нарушениями. Инцидент является событием, которое вызывает (или может вызвать) негативные последствия для безопасного функционирования систем. В свою очередь, простые нарушения, как правило, не приводят к значительным последствиям или ущербу и могут быть устранены без воздействия на безопасность системы. Таким образом, инциденты требуют более всестороннего анализа, оперативной реакции и, потенциально, применения соответствующих мер по восстановлению и совершенствованию защиты.

Своевременное реагирование на инциденты способствует совершенствованию процессов управления обеспечением информационной безопасности. Тем не менее, связь между функциями реагирования на инциденты и управления безопасностью зачастую отсутствует. Поэтому предприятиям необходимо устанавливать интеграцию между этими двумя областями, иметь четкий план действий, который может повысить доверие и поддержку со стороны подрядчиков [1].

Выявление инцидентов безопасности в режиме реального времени осуществляется посредством специализированных центров управления безопасностью с использованием систем управления информацией и событиями информационной безопасности. Данные центры собирают, нормализуют, хранят и сопоставляют события безопасности, они необходимы для быстрого обнаружения инцидентов, минимизации потерь, устранения уязвимостей и восстановления ИТ-услуг [2].

В задачах управления информационной безопасностью необходимо задействовать целостный подход, включающий разработку и выполнение политик безопасности, обучение по соблюдению требований и согласование бизнеса и ИТ[5]. Например, в работе [3] отмечено, что интеграция цифровой криминалистики с обработкой инцидентов может повысить эффективность стратегий реагирования на инциденты.

В работе [4] показано, что эффективное управление инцидентами требует сочетания технологических решений и управленческих мероприятий (разработка политик безопасности, обучение и обмен информацией между департаментами и т.д.). Текущие практики управления инцидентами соответствуют стандартам ISO/IEC 27035[6], но организации зачастую сталкиваются с определенными трудностями, которые решают с помощью усовершенствованных стратегий.

Таким образом, эффективное управление инцидентами информационной безопасности на предприятиях включает в себя сочетание тщательного анализа инцидентов, стратегического использования специализированных информационных систем, целостного подхода к управлению безопасностью и интеграции технологических и управленческих решений. Устраняя пробелы в коммуникации, используя инструменты мониторинга в реальном времени и внедряя передовой опыт, организации могут улучшить свои возможности реагирования на инциденты и общее состояние безопасности [5].

СУЩЕСТВУЮЩИЕ МОДЕЛИ УПРАВЛЕНИЯ ИНЦИДЕНТАМИ

Для повышения эффективности процессов управления инцидентами в профильной научной литературе предлагаются различные модели. Например, в [6] рассматривалось когнитивное моделирование деструктивных злоумышленных воздействий на объектах критической информационной инфраструктуры и модель состояний субъектов критической информационной инфраструктуры при деструктивных воздействиях в статичном режиме.

Для описания динамики систем управления информацией и событиями безопасности используют цепи Маркова и стохастические дифференциальные уравнения [7]. Использование контролируемых цепей Маркова помогает формализовать и структурировать процесс поддержки принятия решений для управления событиями безопасности и инцидентами. Данный подход фокусируется на динамике обнаружения и предотвращения кибератак, обеспечивая своевременность, обоснованность, секретность и эффективность ресурсов [8].

В ряде исследований для моделирования управления инцидентами предложено использовать имитационные модели, которые оценивают эффективность операций по управлению инцидентами, анализируя реальные данные и различные стратегии развертывания групп реагирования на чрезвычайные ситуации. Эти модели могут прогнозировать статистические закономерности кибератак и эффективность групп реагирования на инциденты, что позволяет осуществлять динамические корректировки для поддержания требуемого уровня защиты [9].

В работе [10] показано, что реализация трехуровневой модели управления инцидентами с использованием ключевых метрик значительно повышает эффективность обработки инцидентов. Данная модель объединяет метрики процесса, технологии и обслуживания для повышения скорости, удовлетворенности пользователей и доступности каналов обработки инцидентов.

[5] Tran D.U. *Holistic Understanding of Information Security Posture:* Thesis Dr. Phil. University of Oslo, Department of Informatics, Series of Dissertations Submitted to the Faculty of Mathematics and Natural Sciences, no. 2696. 2023. https://www.duo.uio.no/bitstream/handle/10852/106520/PhD-Tran-2023.pdf?sequence=3&isAllowed=y. Дата обращения 15.07.2024. / Accessed July 15, 2024.

[6] https://www.iso.org/standard/78973.html. Дата обращения 15.07.2024. / Accessed July 15, 2024.

Кроме названных моделей в научной литературе можно встретить различные подходы, основанные на формальных языках и теории автоматов [11] (обеспечивают структурированный подход к моделированию и анализу процессов управления инцидентами, позволяя выявлять и решать системные проблемы), приоритизации инцидентов [12] (используют отзывы аналитиков для исправления ошибок в процессе оценки, гарантируя оперативное решение наиболее критических инцидентов) и др. Интегрируя механизмы обратной связи и комплексное управление событиями безопасности, организации могут поддерживать надежные процессы управления инцидентами, которые адаптируются к меняющимся угрозам и технологическим изменениям.

Таким образом, в задачах управления инцидентами информационной безопасности используются различные модели, включая математические, имитационные, системные динамические и формальные языковые подходы. Данные модели направлены на улучшение идентификации, классификации и реагирования на инциденты, эффективное и проактивное управление рисками безопасности [13]. Управление инцидентами информационной безопасности выступает важным процессом, который напрямую связан с обеспечением трех ключевых элементов: целостности, аутентификации и доступности данных [14]. Применение вариативных моделей позволяет улучшить процессы идентификации, классификации и устранения инцидентов. Для достижения максимальной эффективности важно учитывать специфику каждой организации, степень угроз и доступные ресурсы, чтобы адаптировать модели к реальным условиям.

МОДЕЛЬ УПРАВЛЕНИЯ ИНЦИДЕНТАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИИ

В задачах управления инцидентами информационной безопасности можно использовать модель, содержащую следующие компоненты:

1. *Множество инцидентов информационной безопасности* $\mathrm{I} = \{I_1, I_2, \ldots, I_n\}$, где I_i – инцидент информационной безопасности, зафиксированный в организации. При этом каждый инцидент характеризуется параметрами времени обнаружения, степени критичности, вероятности реализации угрозы и т.д.
2. *Множество действий по управлению инцидентами* $\mathrm{A} = \{A_1, A_2, \ldots, A_m\}$, где A_j – определенное действие по устранению инцидента или минимизации его последствий. К таким действиям можно отнести блокировку доступа, восстановление данных, внедрение дополнительных защитных мер на предприятии и т.д.
3. *Время реакции на инцидент* $T(I_i)$. Данный компонент модели зависит от уровня критичности инцидента и ресурсов, доступных для реагирования. В идеале, чем выше критичность инцидента, тем меньше должно быть время реакции.
4. *Функция ущерба от инцидента* $D(I_i)$ оценивает реальные или возможные потери для организации в результате инцидента I_i (финансовые потери, ущерб репутации, нарушение конфиденциальности данных и т.д.).
5. *Функция вероятности устранения инцидента* $P(A_j, I_i)$ показывает вероятность успеха действия A_j по отношению к инциденту I_i. Вероятность зависит от различных факторов (квалификация сотрудников, время выполнения, тип инцидента и др.).
6. *Затраты на устранение инцидента* $C(A_j, I_i)$ отражают сколько ресурсов (финансовых, временных и человеческих) нужно потратить на реализацию действия A_j для устранения инцидента I_i.

Ключевой целью модели выступает решение задачи минимизации общего ущерба от инцидентов информационной безопасности и затрат на их устранение. Для решения названной задачи целесообразно минимизировать следующую целевую функцию:

$$Z = \sum_{i=1}^{n}\sum_{j=1}^{m}\left[D(I_i)(1 - P(A_j, I_i)) + C(A_j, I_i)\right] \to \min,$$

где Z – это совокупность ущерба и затрат на все инциденты. При этом целесообразен учет ограничений на доступные ресурсы, время реакции и уровню риска:

$$T(I_i) \le T_{\max},$$

$$\sum_{i=1}^{n}\sum_{j=1}^{m} C(A_j, I_i) \le R,$$

$$P(A_j, I_i) \ge P_{\min},$$

$$I_i \in \mathrm{I},\ A_j \in \mathrm{A},$$

где $T_{\max}$ – максимальное допустимое время реакции на инцидент (может быть установлено политикой безопасности предприятия), R – общий доступный бюджет (количество ресурсов), выделенный на устранение инцидентов информационной безопасности, $P_{\min}$ – минимально допустимая вероятность успешного устранения инцидента.

Использование приведенной модели подразумевает следующие шаги:

1. *Обнаружение инцидента.*
2. *Сбор данных об инциденте* (критичность, возможный ущерб, затраты на устранение).
3. *Оценка вероятности успешного устранения инцидента* с учетом временных и финансовых ограничений.

4. *Оптимизация действий* (на основе представленной модели находится минимизирующее ущерб и затраты действие A_j).
5. *Мониторинг и корректировка* (после выполнения всех необходимых действий по устранению инцидента модель может быть скорректирована для дальнейшего анализа и предотвращения инцидентов в будущем).

Предложенная модель помогает систематизировать процесс управления инцидентами информационной безопасности и принять оптимальные решения по их устранению. Однако модель содержит ряд ограничений и допущений. К ограничениям можно отнести необходимость точных и актуальных данных, трудности в оценках ущерба и вероятности, а также игнорирование человеческого фактора. Допущения модели включают линейность функций ущерба и затрат, независимость инцидентов, однозначное определение критичности и др. Предприятиям целесообразно учитывать эти аспекты, адаптируя модель к собственным условиям информационной безопасности.

Для эффективной апробации модели использован набор синтетических данных, имитирующих различные типы инцидентов и возможные пути их ликвидации. Выбор синтетических данных взамен реальных обусловлен ограниченной доступностью последних, поскольку предприятия зачастую не могут или не желают делиться информацией о своих инцидентах по соображениям безопасности и конфиденциальности. Кроме того, применение синтетических данных позволяет строить более полные и надежные модели на основе разнообразных гипотетических сценариев. Такой подход в сочетании с теоретическим анализом и разработкой создает основу для более глубокого понимания механизмов реагирования на инциденты и управления ими в области информационной безопасности. Таким образом, использование синтетических данных представляет собой обоснованный метод в условиях нехватки реальной информации и направлено на обеспечение качественной и надежной апробации модели.

Пусть в ходе анализа на предприятии выявлен ряд инцидентов информационной безопасности, каждый из которых требует различных действий для устранения, которые ограничены по ресурсам и времени. Исходные данные для расчетов представлены в табл. 1.

Допустим, у предприятия ограниченные ресурсы для реагирования: бюджет на устранение инцидентов составляет R = 50000 у.е., а максимальное время реакции на все инциденты – 6 ч. Пусть для каждого инцидента существует несколько возможных действий с разной стоимостью, вероятностью устранения и временем выполнения (табл. 2).

Таблица 1. Исходные данные

Инцидент	Потенциальный ущерб (D), у.е.	Время реакции (T), ч	Критичность
Утечка данных клиентской базы	200000	2	Высокая
Вирусная атака на серверы	100000	5	Средняя
Неправомерный доступ к сети	50000	1	Низкая

Таблица 2. Возможные действия по устранению инцидентов информационной безопасности

Инцидент	Действие	Стоимость (C), у.е.	Вероятность успеха (P)
Утечка данных (I_1)	Отключение внешних соединений (A_1)	15000	0.7
	Уведомление клиентов и правка уязвимости (A_2)	25000	0.9
Вирусная атака (I_2)	Перезагрузка серверов и запуск антивируса (A_3)	10000	0.8
	Замена оборудования и восстановление данных (A_4)	20000	0.95
Неправомерный доступ (I_3)	Отключение сессии нарушителя (A_5)	5000	0.6
	Аудит сети и исправление конфигурации (A_6)	8000	0.85

Для минимизации ущерба с учетом ограничений нужно выбрать действия для каждого инцидента. Рассмотрим альтернативы.

Для I_1. Действие A_1 дешевле, однако, имеет вероятность успеха 0.7, тогда как действие A_2 дороже, но вероятность успеха выше (0.9). Учитывая критичность инцидента, целесообразно выбрать действие A_2, т.к. утечка данных несет высокий ущерб.

Для I_2. Действие A_3 дешевле и имеет достаточно высокую вероятность успеха (0.8). Учитывая бюджетные ограничения, выбираем действие A_3.

Для I_3. Действие A_5 самое дешевое, однако, вероятность его успеха равна всего 0.6. В данном случае целесообразнее выбрать действие A_6, т.к. его вероятность успеха значительно выше (0.85), и можно уложиться в бюджет.

Построим модель по исходным данным. Целевая функция и ограничения модели будут иметь следующий вид:

$$Z = \sum_{i=1}^{3}\sum_{j=1}^{2}\left[D(I_i)(1 - P(A_j, I_i)) + C(A_j, I_i) \right],$$
$$C(A_1, I_1) + C(A_3, I_2) + C(A_5, I_3) \le 50000 \text{ у.е.},$$
$$T(I_1) + T(I_1) + T(I_1) \le 6 \text{ ч.}$$

Окончательное модельное решение примет следующий вид:

- A_2 для инцидента 1 (стоимость равна 25000 у.е., вероятность успеха – 0.9).
- A_3 для инцидента 2 (стоимость равна 10000 у.е., вероятность успеха – 0.8).
- A_6 для инцидента 3 (стоимость равна 8000 у.е., вероятность успеха – 0.85).

Рассчитав общие затраты и ущерб, получим Z = 90500 у.е. Таким образом, применение модели позволило выбрать оптимальные действия для устранения инцидентов с минимальными затратами и ущербом в рамках имеющегося бюджета и времени реакции.

ЗАКЛЮЧЕНИЕ

Предложенная в статье модель управления инцидентами помогает минимизировать ущерб и затраты за счет оптимального выбора действий в условиях ограниченных ресурсов. Хотя модель имеет свои ограничения, ее использование на практике может существенно повысить уровень информационной безопасности предприятия.

В рамках работы предложена модель управления инцидентами информационной безопасности, направленная на минимизацию ущерба и затрат. Однако ее практическое использование вызывает ряд вопросов, связанных с упрощениями: линейность функций ущерба и затрат, независимость инцидентов и однозначное определение их критичности. Эти допущения не всегда отражают сложность реальных ситуаций, где инциденты взаимосвязаны, а последствия могут быть нелинейными. Кроме того, модель не учитывает человеческий фактор и сложности получения точных данных на этапах реагирования. Реальные условия предполагают ограниченность ресурсов, стрессовые ситуации и необходимость приоритизации.

Несмотря на указанные ограничения, предложенная модель значительно развивает существующие стандарты и модели управления инцидентами информационной безопасности. Модель включает приоритизацию инцидентов, оценку критичности и распределение ресурсов, что позволяет принимать более обоснованные и оперативные решения в условиях ограниченного времени и ресурсов.

Таким образом, модель может дополнить существующие подходы, предложив инструменты для более точного анализа и эффективного управления инцидентами, ориентированного на снижение их последствий и повышение общей устойчивости предприятия к угрозам информационной безопасности.

В дальнейших исследованиях планируется проведение апробации на реальных данных, что позволит более точно оценить эффективность разработанной модели. Кроме того, дальнейшие исследования могут быть связаны с интеграцией моделей управления инцидентами с другими процессами управления информационной безопасностью. Также крайне важно дать оценку влияния человеческого фактора на инциденты и сформировать действенные механизмы обучения сотрудников.

Вклад авторов

Е.С. Митяков – провел основную часть исследования, включая разработку концепции модели управления инцидентами, определение ключевых элементов модели, анализ существующих подходов и формирование практических рекомендаций.

Е.А. Максимова – внесла вклад в обзор литературы, формализацию модели, определение этапов управления инцидентами.

С.В. Артемьева – участвовала в анализе существующих моделей управления инцидентами, сборе и систематизации информации о практике применения моделей в различных организациях.

А.А. Бакаев – курировал процесс исследования, предоставил рекомендации по формулировке проблемы и разработке модели, провел экспертную оценку полученных результатов.

Ж.Г. Вегера – провела численные расчеты по модели, внесла вклад в интерпретацию результатов моделирования, участвовала в подготовке статьи к публикации.

Authors' contributions

E.S. Mityakov – conducted the majority of the research, including the development of the concept of the incident management model, the definition of the model's key elements, the analysis of existing approaches, and the formulation of practical recommendations.

E.A. Maksimova – contributed to the literature review, formalization of the model, and the definition of incident management stages.

S.V. Artemova – participated in the analysis of existing incident management models, collecting and systematizing information about the practice of applying models in various organizations.

A.A. Bakaev – supervised the research process, provided guidance on problem formulation and model development, and conducted an expert evaluation of the obtained results.

Zh.G. Vegera – conducted numerical calculations based on the model, contributed to the interpretation of the modeling results, and participated in preparing the article for publication.

СПИСОК ЛИТЕРАТУРЫ

1. Żywiolek J., di Taranto A. Creating value added for an enterprise by managing information security incidents. *System Safety: Human – Technical Facility – Environment.* 2019;1(1):156–162. https://doi.org/10.2478/CZOTO-2019-0020
2. Zidan K., Alam A., Allison J., Al-sherbaz A. Assessing the challenges faced by Security Operations Centers (SOC). In: Arai K. (Ed.). *Advances in Information and Communication. FICC 2024. Lecture Notes in Networks and Systems*. Springer; 2024. V. 920. P. 256–271. https://doi.org/10.1007/978-3-031-53963-3_18
3. Sackey A. Information Security Incident Handling in the Cloud. In: *Book Chapter Series on Research Nexus in IT, Law, Cyber Security & Forensics*. 2022. P. 103–108. https://doi.org/10.22624/AIMS/CRP-BK3-P17
4. Дёмина А.К. Управление инцидентами информационной безопасности. *Международный журнал гуманитарных и естественных наук.* 2024;5–1(92):227–231. https://doi.org/10.24412/2500-1000-2024-5-1-227-231, URL: https://elibrary.ru/aizkwa
5. Khorev P.B., Karpeeva V.A. Software tools for analyzing information security incidents based on monitoring of information resources. In: *2022 6th International Conference on Information Technologies in Engineering Education* (*Inforino*). IEEE; 2022. https://doi.org/10.1109/Inforino53888.2022.9782979, URL: https://elibrary.ru/qjfmzi
6. Максимова Е.А. Когнитивное моделирование деструктивных злоумышленных воздействий на объектах критической информационной инфраструктуры. *Труды учебных заведений связи*. 2020;6(4):91–103. https://doi.org/10.31854/1813-324X-2020-6-4-91-103, URL: https://elibrary.ru/lirtxz
7. Котенко И.В., Паращук И.Б. Модель системы управления информацией и событиями безопасности. *Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика*. 2020;2:84–94. https://doi.org/10.24143/2072-9502-2020-2-84-94, URL: https://elibrary.ru/owaldx
8. Kotenko I., Parashchuk I. An approach to modeling the decision support process of the security event and incident management based on Markov chains. *IFAC-PapersOnLine.* 2019;52(13):934–939. https://doi.org/10.1016/j.ifacol.2019.11.314, URL: https://elibrary.ru/eqccxc
9. Dohtieva I., Shyian A. Simulation of the work of the information security incident response team during cyberattacks. *Herald of Khmelnytskyi National University.* 2021;303(6):115–123.
10. Микрюков А.А., Куулар А.В. Разработка модели управления инцидентами в информационной системе предприятия на основе трехуровневой архитектуры с использованием ключевых (релевантных) метрик. *Открытое образование.* 2020;24(3):78–86. https://doi.org/10.21686/1818-4243-2020-3-78-86, URL: https://elibrary.ru/fcqjjr
11. Mouratidis H., Islam S., Santos-Olmo A., Sanchez L.E., Ismail U.M. Modelling language for cyber security incident handling for critical infrastructures. *Comput. Secur.* 2023;128(8):103139. https://doi.org/10.1016/j.cose.2023.103139
12. Renners L., Heine F., Kleiner C., Rodosek G. Design and evaluation of an approach for feedback-based adaptation of incident prioritization. In: *2019 2nd International Conference on Data Intelligence and Security* (*ICDIS*). IEEE: 2019. P. 28–35. https://doi.org/10.1109/ICDIS.2019.00012
13. Maksimova E., Sadovnikova N. Proactive modeling in the assessment of the structural functionality of the subject of critical information infrastructure. In: Kravets A.G., Shcherbakov M., Parygin D., Groumpos P.P. (Eds.). *Creativity in Intelligent Technologies and Data Science* (*CIT&DS 2021*). *Communications in Computer and Information Science*. Springer; 2021. V. 1448. P. 436–448. https://doi.org/10.1007/978-3-030-87034-8_31
14. Alin Z., Sharma R. Cybersecurity management for incident response. *Romanian Cyber Security Journal.* 2022;4(1):69–75. URL: https://elibrary.ru/ihxntg

REFERENCES

1. Żywiolek J., di Taranto A. Creating value added for an enterprise by managing information security incidents. *System Safety: Human – Technical Facility – Environment.* 2019;1(1):156–162. https://doi.org/10.2478/CZOTO-2019-0020
2. Zidan K., Alam A., Allison J., Al-sherbaz A. Assessing the challenges faced by Security Operations Centers (SOC). In: Arai K. (Ed.). *Advances in Information and Communication. FICC 2024. Lecture Notes in Networks and Systems*. Springer; 2024. V. 920. P. 256–271. https://doi.org/10.1007/978-3-031-53963-3_18
3. Sackey A. Information Security Incident Handling in the Cloud. In: *Book Chapter Series on Research Nexus in IT, Law, Cyber Security & Forensics*. 2022. P. 103–108. https://doi.org/10.22624/AIMS/CRP-BK3-P17
4. Demina A.K. Information security incident management. *Mezhdunarodnyi zhurnal gumanitarnykh i estestvennykh nauk = International Journal of Humanities and Natural Sciences*. 2024;5–1(92):227–231 (in Russ.). https://doi.org/10.24412/2500-1000-2024-5-1-227-231, available from URL: https://elibrary.ru/aizkwa
5. Khorev P.B., Karpeeva V.A. Software tools for analyzing information security incidents based on monitoring of information resources. In: *2022 6th International Conference on Information Technologies in Engineering Education* (*Inforino*). IEEE; 2022. https://doi.org/10.1109/Inforino53888.2022.9782979, available from URL: https://elibrary.ru/qjfmzi
6. Maksimova E.A. Cognitive modeling of destructive malicious impacts on critical information infrastructure objects. *Trudy uchebnykh zavedenii svyazi = Proceedings of Telecommunication Universities*. 2020;6(4):91–103 (in Russ). https://doi.org/10.31854/1813-324X-2020-6-4-91-103, available from URL: https://elibrary.ru/lirtxz
7. Kotenko I.V., Parashchuk I.B. Model of security information and event management system. *Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriya: Upravlenie, vychislitel'naya tekhnika i informatika = Vestnik of Astrakhan State Technical University. Series: Management, Computer Science and Informatics*. 2020;2:84–94 (in Russ). https://doi.org/10.24143/2072-9502-2020-2-84-94, available from URL: https://elibrary.ru/owaldx
8. Kotenko I., Parashchuk I. An approach to modeling the decision support process of the security event and incident management based on Markov chains. *IFAC-PapersOnLine.* 2019;52(13):934–939. https://doi.org/10.1016/j.ifacol.2019.11.314, available from URL: https://elibrary.ru/eqccxc

9. Dohtieva I., Shyian A. Simulation of the work of the information security incident response team during cyberattacks. *Herald of Khmelnytskyi National University.* 2021;303(6):115–123.
10. Mikryukov A.A., Kuular A.V. Development of an incident management model in an enterprise information system based on a three-tier architecture using key (relevant) metrics. *Otkrytoe obrazovanie = Open Education*. 2020;24(3):78–86 (in Russ.). https://doi.org/10.21686/1818-4243-2020-3-78-86, available from URL: https://elibrary.ru/fcqjjr
11. Mouratidis H., Islam S., Santos-Olmo A., Sanchez L.E., Ismail U.M. Modelling language for cyber security incident handling for critical infrastructures. *Comput. Secur.* 2023;128(8):103139. https://doi.org/10.1016/j.cose.2023.103139
12. Renners L., Heine F., Kleiner C., Rodosek G. Design and evaluation of an approach for feedback-based adaptation of incident prioritization. In: *2019 2nd International Conference on Data Intelligence and Security* (*ICDIS*). IEEE: 2019. P. 28–35. https://doi.org/10.1109/ICDIS.2019.00012
13. Maksimova E., Sadovnikova N. Proactive modeling in the assessment of the structural functionality of the subject of critical information infrastructure. In: Kravets A.G., Shcherbakov M., Parygin D., Groumpos P.P. (Eds.). *Creativity in Intelligent Technologies and Data Science* (*CIT&DS 2021*). *Communications in Computer and Information Science*. Springer; 2021. V. 1448. P. 436–448. https://doi.org/10.1007/978-3-030-87034-8_31
14. Alin Z., Sharma R. Cybersecurity management for incident response. *Romanian Cyber Security Journal.* 2022;4(1):69–75. Available from URL: https://elibrary.ru/ihxntg

Об авторах

Митяков Евгений Сергеевич, д.э.н., профессор, и.о. заведующего кафедрой КБ-9 «Предметно-ориентированные информационные системы», Институт кибербезопасности и цифровых технологий, ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78). E-mail: mityakov@mirea.ru. Scopus Author ID 55960540500, SPIN-код РИНЦ 5691-8947, https://orcid.org/0000-0001-6579-0988

Максимова Елена Александровна, д.т.н., доцент, заведующий кафедрой КБ-4 «Интеллектуальные системы информационной безопасности», Институт кибербезопасности и цифровых технологий, ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78). E-mail: maksimova@mirea.ru. Scopus Author ID 57219701980, SPIN-код РИНЦ 6876-5558, https://orcid.org/0000-0001-8788-4256

Артемова Светлана Валерьевна, д.т.н., доцент, заведующий кафедрой КБ-1 «Защита информации», Институт кибербезопасности и цифровых технологий, ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78). E-mail: artemova_s@mirea.ru. Scopus Author ID 6508256085, SPIN-код РИНЦ 3775-6241, https://orcid.org/0009-0006-8374-8197

Бакаев Анатолий Александрович, д.и.н., к.ю.н., доцент, директор Института кибербезопасности и цифровых технологий, ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78). E-mail: bakaev@mirea.ru. Scopus Author ID 57297341000, SPIN-код РИНЦ 5283-9148, https://orcid.org/0000-0002-9526-0117

Вегера Жанна Геннадьевна, к.ф.-м.н., доцент, заведующий кафедрой высшей математики, Институт кибербезопасности и цифровых технологий, ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78). E-mail: vegera@mirea.ru. Scopus Author ID 57212931836, SPIN-код РИНЦ 9076-5678, https://orcid.org/0000-0001-7312-3341

About the authors

Evgeny S. Mityakov, Dr. Sci. (Econ.), Professor, Acting Head of the “Subject-Oriented Information Systems” Department, Institute of Cybersecurity and Digital Technologies, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow, 119454 Russia). E-mail: mityakov@mirea.ru. Scopus Author ID 55960540500, RSCI SPIN-code 5691-8947, https://orcid.org/0000-0001-6579-0988

Elena A. Maksimova, Dr. Sci. (Eng.), Associate Professor, Head of the “Intelligent Information Security Systems” Department, Institute of Cybersecurity and Digital Technologies, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow, 119454 Russia). E-mail: maksimova@mirea.ru. Scopus Author ID 57219701980, RSCI SPIN-code 6876-5558, https://orcid.org/0000-0001-8788-4256

Svetlana V. Artemova, Dr. Sci. (Eng.), Associate Professor, Head of the “Information Protection” Department, Institute of Cybersecurity and Digital Technologies, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow, 119454 Russia). E-mail: artemova_s@mirea.ru. Scopus Author ID 6508256085, RSCI SPIN-code 3775-6241, https://orcid.org/0009-0006-8374-8197

Anatoly A. Bakaev, Dr. Sci. (Hist.), Cand. Sci. (Juri.), Associate Professor, Director of the Institute of Cybersecurity and Digital Technologies, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow, 119454 Russia). E-mail: bakaev@mirea.ru. Scopus Author ID 57297341000, RSCI SPIN-code 5283-9148, https://orcid.org/0000-0002-9526-0117

Zhanna G. Vegera, Cand. Sci. (Phys.-Math.), Associate Professor, Head of the Department of Higher Mathematics, Institute of Cybersecurity and Digital Technologies, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow, 119454 Russia). E-mail: vegera@mirea.ru. Scopus Author ID 57212931836, RSCI SPIN-code 9076-5678, https://orcid.org/0000-0001-7312-3341