Научная статья
УДК 004.056
DOI: 10.26583/bit.2025.2.04

МОДЕЛИ ДАННЫХ ДЛЯ АВТОМАТИЗАЦИИ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ

Александр В. Кузнецов
Финансовый университет при Правительстве Российской Федерации, пр-кт Ленинградский, 49/2, Москва, 125167, Россия
1283_my@mail.ru, https://orcid.org/0000-0002-7160-1845

Аннотация. Целью исследования является формирование основополагающих моделей данных: концептуальной и логической, позволяющих осуществлять реагирование на инциденты информационной безопасности в автоматизированном и полностью автоматическом режимах, первостепенно в части действий по локализации (сдерживанию) инцидентов информационной безопасности. Предложенные режимы реагирования позволят организациям сократить время на реализацию мероприятий по реагированию на возникающие инциденты информационной безопасности, т. е. своевременно затруднят или полностью приостановят развитие кибератаки и минимизируют ущерб от реализуемых атакующим действий. Методами исследования выступали анализ и синтез имеющихся материалов и достижений, в т. ч. запатентованных, а также моделирование. По результатам предложена концептуальная модель данных, которая в отличии от известных учитывает три варианта для формирования инцидента информационной безопасности (карточки инцидента информационной безопасности), а также независимо рассматривает логические и технические действия по локализации инцидентов информационной безопасности. Предложена логическая модель данных, которая детализирует концептуальную модель и в отличии от известных учитывает, что выбираемый план реагирования зависит от типа и приоритета обнаруженного инцидента информационной безопасности. Областью применения результатов выступают центры Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и центры мониторинга и реагирования на кибератаки (Security Operations Center), а также организации-владельцы крупных территориально распределенных ИТ-инфраструктур с собственными группами реагирования на инциденты информационной безопасности. В качестве развития данного исследования автором проводится формирование физической модели данных и ее апробация.

Ключевые слова: *концептуальная модель, логическая модель, автоматизированное реагирование, автоматическое реагирование, локализация инцидента.*

Для цитирования: *Кузнецов, Александр В. Модели данных для автоматизации реагирования на инциденты. Безопасность информационных технологий, [S.l.], т. 32, № 2, с. 48–58, 2025. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1774. DOI: 10.26583/bit.2025.2.04.*

Scientific article

DATA MODELS FOR INCIDENT RESPONSE AUTOMATIZATION

Aleksandr V. Kuznetcov
Financial University under the Government of the Russian Federation, Leningradsky Ave., 49/2, Moscow, 125167, Russia
1283_my@mail.ru, https://orcid.org/0000-0002-7160-1845

Abstract. The purpose of the research is to develop priority data models: conceptual and logical, which allow responding to information security incidents in automated and fully automatic modes,

primarily in terms of following action – information security incidents localization (containment). These response modes will allow organizations to reduce the time to detected information security incidents response measures implementation, i.e., they will timely complicate or completely stop of cyberattacks and minimize the damage caused by the attacker's actions. The research methods were analysis and synthesis of available materials and achievements, including patented ones, as well as modeling. According to the results, a conceptual data model is proposed, which, unlike the known ones, takes into account three options for the creation of information security incident (information security incident card), as well as independently considers logical and technical actions to information security incidents localization. A logical data model is proposed, which details the conceptual model and, unlike the known ones, takes into account that the selected response plan depends on the type and priority of the detected information security incident. The area of application of the results is the centers of the State System of Detection, Prevention and Elimination of Consequences of Computer Attacks on Information Resources of the Russian Federation and Security Operations Center, as well as organizations-owners of large geographically distributed IT infrastructures with their own computer security incident response team. As a development of this research, the author is developing a physical data model and its testing.

Keywords: *conceptual model, logic model, automated response, automatic response, incident localization.*

For citation: *KUZNETCOV, Aleksandr V. Data models for incident response automatization. IT Security (Russia), [S.l.], v. 32, no. 2, p. 48–58, 2025. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1774. DOI: 10.26583/bit.2025.2.04.*

Введение

Задачи обеспечения безопасности информации не только не теряют уровень своей актуальности, но и повышают его каждые несколько лет. В 2020 г. массовый переход на удаленный режим работы значительного числа организаций увеличил масштабы и площадь кибератак, изменились акценты в действиях атакующих (популярными стали техники «External remote services»[1], «Valid accounts»[2]). В данной ситуации значительная часть конечных пользователей, их устройства связи и компьютеры, подключенные к интернету, остались «один на один» с атакующими, в т. ч. в части реагирования на возникающие инциденты информационной безопасности (ИБ). В 2022 г. широкомасштабные компьютерные атаки на организации и отдельных граждан Российской Федерации (вне зависимости от страны их нахождения) сделали потенциальной целью любые информационные (автоматизированные) системы и устройства, подключенные к интернету. Акценты в действиях атакующих сместились к нанесению максимальных деструктивных воздействий (техника «Data destruction»[3]), как следствие, своевременность и корректность (точность) мероприятий по реагированию на возникающие инциденты ИБ резко возросла. И наконец, начиная с 2024 г. атакующие добавили в свой арсенал технологии искусственного интеллекта, сократили время подготовки и реализации кибератак. Как следствие, мероприятия по реагированию на инциденты ИБ вновь подлежат пересмотру и модернизации, в т. ч. переводу в автоматизированный и там, где это возможно, в полностью автоматический режим работы (согласно модели эволюции подходов к реагированию на инциденты ИБ [1]).

При это стоит отметить, что значительное число работ и исследований, относящихся к тематике управления инцидентами ИБ, в настоящее время посвящено обнаружению инцидентов ИБ. К ведущим российским исследователям в данной области можно отнести коллективы под руководством Котенко И.В. и Саенко И.Б. [2, 3], а также Милославской

[1]Техника из MITRE ATT&CK. URL: https://attack.mitre.org/techniques/T1133/ (дата обращения: 17.01.2025).
[2]Техника из MITRE ATT&CK. URL: https://attack.mitre.org/techniques/T1078/ (дата обращения: 17.01.2025).
[3]Техника из MITRE ATT&CK. URL: https://attack.mitre.org/techniques/T1485/ (дата обращения: 17.01.2025).

Н.Г. [4, 5]. Но при этом уделяется недостаточное внимание вопросам именно реагирования на обнаруженные инциденты ИБ, в т. ч. вопросам полностью автоматического реагирования и с использованием машинного обучения (технологий искусственного интеллекта). И в данном разрезе управления инцидентами ИБ на первый план выходят вопросы подготовки и обработки нужных данных, т. е. формирования и использования необходимых моделей данных.

Существующие запатентованные методы и способы автоматизации реагирования на инциденты ИБ[4], а также работы, посвященные концептуальным вопросам реагирования на инциденты ИБ [6–8], не учитывают и не предлагают модели данных, которые можно использовать для проектирования, модернизации и/или интеграции средств реагирования или для применения в рамках машинного обучения. В настоящем исследовании рассматриваются средства, используемые в составе центров Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА) и центров мониторинга и реагирования на кибератаки (Security Operations Center (SOC)).

Целью настоящего исследования является формирование первоочередных моделей данных, позволяющих осуществлять реагирование на инциденты ИБ в автоматизированном и полностью автоматическом режимах. Предложенные режимы реагирования позволят сократить время на реализацию мероприятий по реагированию на возникающие инциденты ИБ, т. е. своевременно затруднят или полностью приостановят развитие кибератаки и минимизируют ущерб от действий реализуемых атакующим.

Принимая во внимание последовательность и правила проектирования моделей и баз данных, а также формирования единых информационных пространств [9–11] для достижения поставленной цели предлагается последовательно решить следующие задачи:

1. Провести инфологическое проектирование и сформировать концептуальную модель данных.
2. Провести даталогическое проектирование и сформировать логическую модель данных.

Методами исследования выступали анализ и синтез имеющихся материалов и достижений, в т. ч. запатентованных (материалы ограниченного доступа при проведении исследования не использовались), а также моделирование.

При проведении данного исследования были приняты следующие ограничения и допущения:

1. Не проводилось деление между понятиями «инцидент ИБ»[5], «инцидент защиты информации»[6] и «компьютерный инцидент»[7], они рассматривались как синонимы.

[4]Method and system for automated incident response. URL: https://patents.google.com/patent/US10051010B2 (дата обращения: 17.01.2025). Automated emergency response method and system. URL: https://patentscope.wipo.int/search/ru/detail.jsf?docId=US42906733 (дата обращения: 17.01.2025). Automated incident response process and automated actions. URL: https://patentscope.wipo.int/search/ru/detail.jsf?docId=US309781267 (дата обращения: 17.01.2025). Способ и система принятия решения о необходимости автоматизированного реагирования на инцидент. URL: https://searchplatform.rospatent.gov.ru/doc/RU2738334C1_20201211 (дата обращения: 17.01.2025).

[5]ГОСТ Р ИСО/МЭК ТО 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности».

[6]ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер».

[7]ГОСТ Р 59709-2022 «Защита информации. Управление компьютерными инцидентами. Термины и определения».

2. В части мероприятий по реагированию на инциденты ИБ рассматривались только приоритетные действия по локализации (сдерживанию) инцидентов ИБ, развивая предыдущие исследования автора [12].

3. Не осуществлялся и не обосновывался выбор системы управления базами данных и формирование физической модели данных.

1. Концептуальная модель данных

Рассматриваемая модель сформирована по результатам проведенного инфологического проектирования [9-11].

Концептуальная модель данных характеризует предметную область реагирования на инциденты ИБ с использованием цифровых данных, т. е. предусматривает применение Data Driven Decision Making подхода в обеспечении безопасности информации.

Концептуальная модель (рис. 1) содержит следующие объекты (сущности):

1. События безопасности из журналов регистрации событий общесистемного и прикладного программного обеспечения, а также средств защиты информации [13].
2. Информационные бюллетени, получаемые от Национального координационного центра по компьютерным инцидентам (НКЦКИ) [14], ФинЦЕРТ, центров ГосСОПКА и/или коммерческих SOC.
3. Обращения (заявки) пользователей, в т. ч. сформированные с использованием программных апплетов в клиентских приложениях электронной почты и/или чат-ботов [15].
4. Инциденты ИБ.
5. Планы (сценарии) реагирования (playbook).
6. Логические действия по локализации инцидентов ИБ (например: включить, выключить, разблокировать, заблокировать, импортировать, экспортировать, возобновить, приостановить, перенести, удалить, перевести в другой режим и т. п.).
7. Средства (механизмы) реагирования в составе общесистемного и/или прикладного программного обеспечения, а также средств защиты информации.
8. Технические действия по локализации инцидентов ИБ (например: ifconfig <interface name> down), с указанием атрибутов объектов, являющихся первичными ключами (ID_<имя атрибута>), и взаимосвязей объектов: «один к одному» (1:1), «один ко многим» (1:M) или «многие ко многим» (M:N).

В качестве объектов, являющихся триггерами для запуска дальнейшей обработки и формирования новых объектов, представленных в формате цифровых данных, выступают «События безопасности», «Информационные бюллетени» и «Обращения пользователей» [13–15]. Указанные объекты могут возникать как по отдельности (один из трех объектов), в комбинациях (два из трех объектов), так и все вместе (три из трех объектов). С точки зрения распределения по временной шкале объекты в большинстве случаев появляются последовательно, т. е. дополняют уже сформированный ранее предыдущим объектом инцидент ИБ. В единичных случаях объекты могут возникнуть в один момент времени (в заданной дельта-окрестности временной точки), тем самым формируя два и более инцидентов ИБ, связанных с одной реальной ситуацией. Такие случаи потребуют дополнительного анализа и агрегации сформированных инцидентов ИБ, где приоритетным (родительским) должен выступать инцидент ИБ, сформированный на базе события(ий) безопасности, т. к. именно события безопасности в ИТ-инфраструктуре выступают объективными свидетельствами произошедшего.

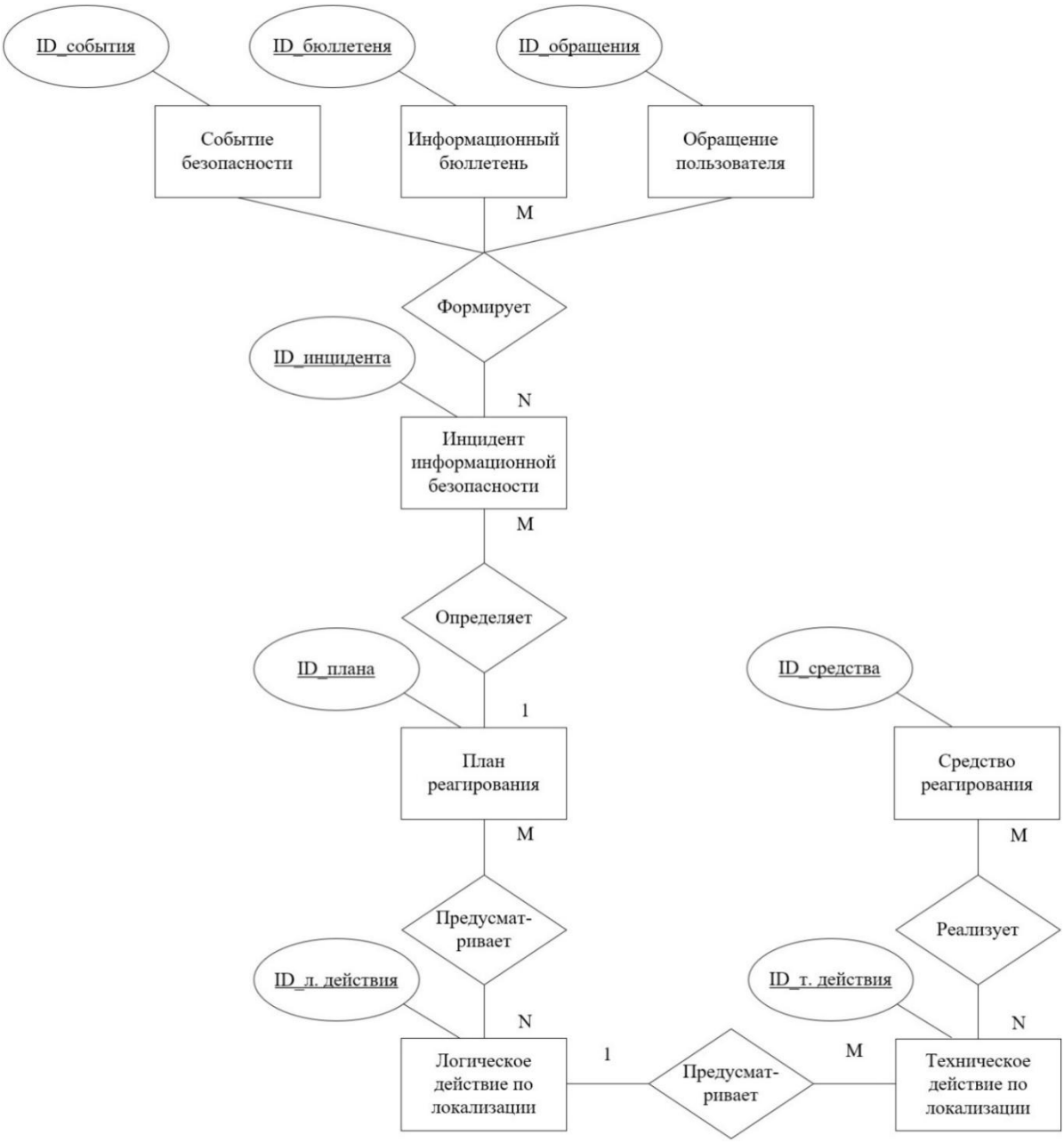

Рис. 1. Концептуальная модель данных

Здесь же стоит отметить, что в качестве источников данных о событиях безопасности рассматриваются:

- средства виртуализации (гипервизоры);
- операционные системы;
- системы управления базами данных;
- веб-серверы;
- почтовые серверы;
- иное прикладное программное обеспечение;
- активное сетевое оборудование;
- межсетевые экраны;
- криптошлюзы;

– системы обнаружения/предотвращения вторжений уровня узла или сети;
– средства антивирусной защиты;
– сканеры безопасности;
– системы предотвращения утечек данных,

а в качестве систем для централизованного сбора и анализа событий безопасности – системы класса Security Information and Event Management или Extended Detection and Response.

В качестве объекта «Инцидент ИБ» рассматривается формируемая на основе объектов-триггеров карточка инцидента ИБ (например: карточка-запись в системе класса Security Orchestration, Automation and Response или Incident Response Platform; заявка-запись в система класса Service Desk или Help Desk). Инцидент ИБ, а точнее ряд его атрибутов: тип и приоритет (поля в карточке инцидента ИБ), определяют подлежащий реализации план реагирования.

В составе мероприятий по реагированию (содержательная часть плана реагирования) могут быть предусмотрены различные действия, практическая реализация (исполнение) которых напрямую зависит от доступных в области реагирования технических средств (оборудования, в т. ч. активного сетевого оборудования) и механизмов защиты информации как общесистемного, так и прикладного программного обеспечения. Например, ограничение доступа к сети передачи данных для компьютера может быть реализовано несколькими способами:

– физическое отключение компьютера от сети передачи данных (отключение пассивного сетевого оборудования от сетевого разъема компьютера);
– программное выключение сетевого интерфейса компьютера на уровне общесистемного программного обеспечения (операционной системы);
– программное выключение сетевого интерфейса компьютера на уровне прикладного программного обеспечения (межсетевого экрана уровня узла);
– выключение сетевого интерфейса на активном сетевом оборудовании (коммутаторе);
– перенаправление исходящего от компьютера сетевого трафика по другому маршруту на активном сетевом оборудовании (маршрутизаторе);
– ограничение исходящего и входящего сетевого трафика от/к компьютеру на активном сетевом оборудовании (межсетевом экране уровня логических границ сети);
– перевод компьютера в отдельный сегмент сети.

Как следствие, требуется независимо рассматривать логические и технические действия реагированию, в т. ч. по локализации инцидентов ИБ.

Теоретическая значимость предлагаемой модели заключается в том, что учитывает три варианта для формирования инцидента ИБ (карточки инцидента ИБ), а также независимо рассматривает логические и технические действия по локализации инцидентов ИБ.

2. Логическая модель данных

Рассматриваемая модель сформирована по результатам проведенного даталогического проектирования [9–11].

Логическая модель данных (рис. 2) расширяет и детализирует сформированную концептуальную модель данных, каждый объект получает минимально необходимый атрибутный состав (атрибутную модель), выделяются идентифицирующие и

неидентифицирующие связи, а также для объектов-потомков указываются внешние ключи (foreign keys, FK).

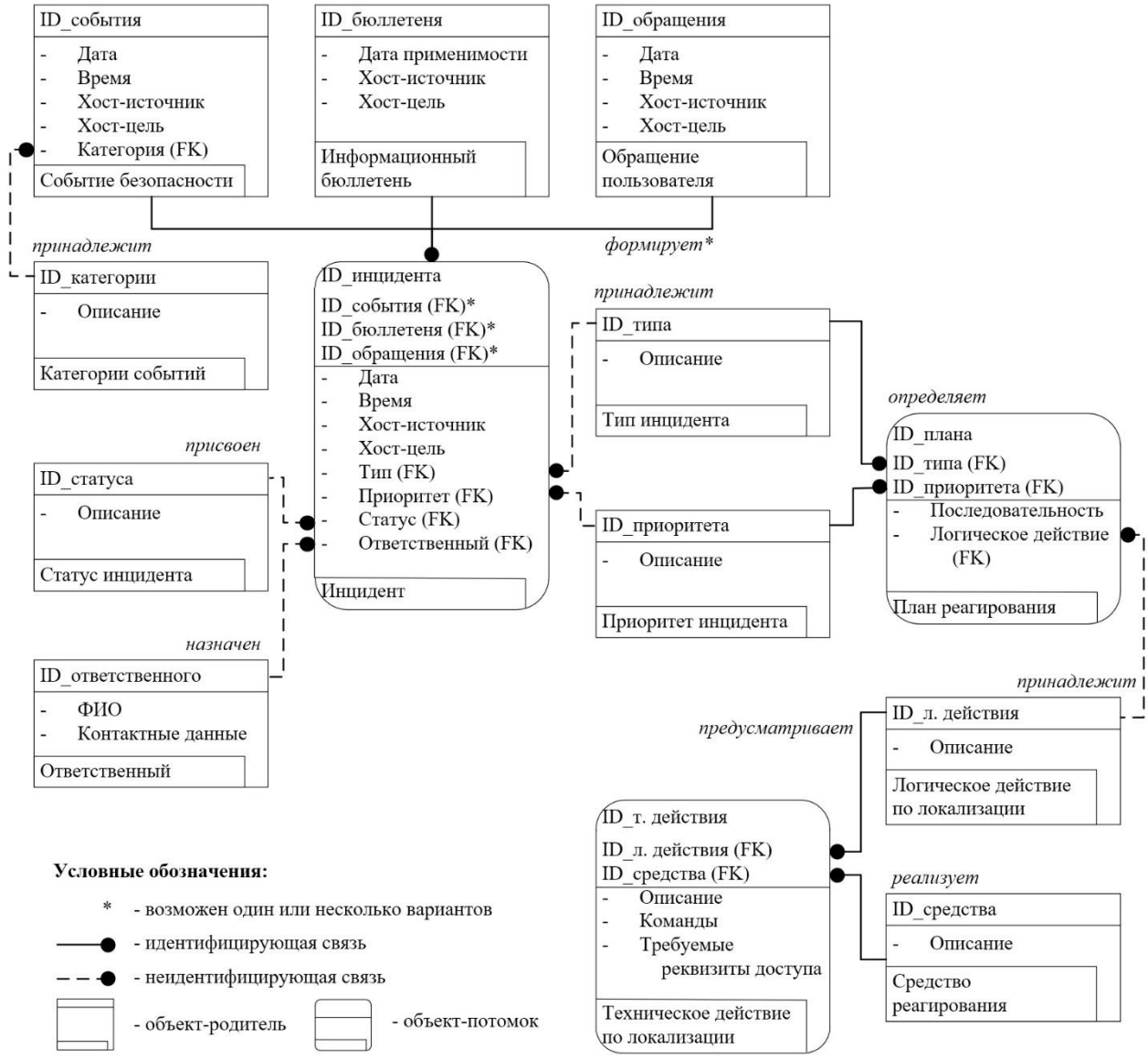

Рис. 2. Логическая модель данных

Объекты концептуальной модели данных представлены одной или несколькими объектами-таблицами логической модели данных (табл. 1), где каждый атрибут выступает отдельным столбцов в объекте-таблице.

Таблица 1. Взаимосвязь объектов сформированных моделей данных

Объект концептуальной модели	Объект(ы) логической модели
Событие безопасности	Событие безопасности. Категории событий
Информационный бюллетень	Информационный бюллетень
Обращение пользователя	Обращение пользователя
Инцидент ИБ	Инцидент. Статус инцидента. Ответственный. Тип инцидента. Приоритет инцидента
План реагирования	План реагирования
Логическое действие по локализации	Логическое действие по локализации
Средство реагирования	Средство реагирования
Техническое действие по локализации	Техническое действие по локализации

Прилагаемая модель данных представлена в одной из популярных нотаций – Integration Definition for Information Modeling Extended (IDEF1X) [16]. Данная нотация была выбрана, т. к. она является достаточно строгой, что позволяет избежать различной трактовки сформированной модели данных разными специалистами [17], а также не требует специализированного программного обеспечения для ее формирования (визуализации).

Предлагаемая модель имеет практическое значение, т. к. она приведена к третьей нормальной форме (3NF) [9], т.е. все атрибуты имеют простые значения, в ней нет частичных или транзитивных зависимостей. Модель учитывает, что план реагирования выбирается с учетом типа и приоритета инцидента ИБ, назначение конкретного ответственного не влияет на реализацию выбранного плана реагирование, т. к. целевым вариантом ее применения является полностью автоматический режим реагирования. Таким образом, корректная типизация (классификация) и приоритизация инцидентов ИБ также влияют на своевременность и корректность (точность) реагирования.

3. Рекомендации по формированию физической модели данных

Физическое проектирование (формирование физической модели данных) рекомендуется проводить для конкретной (выбранной в организации) системы управления базами данных, которая может обладать своими правилами и ограничениями на именование объектов и их атрибутов (таблиц и столбцов), поддерживаемые типы данных и т. п.

Рекомендуется также предусмотреть использование системы управления базами данных, включенной в реестр российского программного обеспечения[8] и реестр сертифицированных средств защиты информации[9].

Заключение

По результатам настоящего исследования, получены первоочередные модели данных, позволяющие осуществлять реагирование на инциденты ИБ в автоматизированном и полностью автоматическом режимах, которые по сравнению с аналогами:

[8]Единый реестр российских программ для электронных вычислительных машин и баз данных. URL: https://reestr.digital.gov.ru/ (дата обращения: 17.01.2025).
[9]Государственный реестр сертифицированных средств защиты информации. URL: https://reestr.fstec.ru/reg3 (дата обращения: 17.01.2025).

1. Концептуальная модель данных принимает во внимание три варианта для формирования инцидента ИБ (карточки инцидента ИБ), а также независимо рассматривает логические и технические действия по локализации инцидентов ИБ.

2. Логическая модель данных детализирует концептуальную модель и принимает во внимание, что план реагирования зависит от типа и приоритета обнаруженного инцидента ИБ.

Для каждой модели данных указаны используемые ключи: для концептуальной модели данных – первичные ключи, для логической модели данных – первичные и внешние ключи. Логическая модель данных приведена к третьей нормальной форме, что в совокупности с предложенными автором рекомендациями по формированию физической модели данных позволяет перейти к ее практической реализации в отдельно взятой ИТ-инфраструктуре.

Приоритетной областью применения результатов настоящего исследования выступают центры ГосСОПКА и/или коммерческие SOC, а также организации-владельцы крупных территориально распределенных ИТ-инфраструктур с собственными группами реагирования на инциденты ИБ (ГРИИБ, computer security incident response team (CSIRT)), для них положительный эффект достигается за счет сокращения времени, затрачиваемого на реагирование на инциденты ИБ.

В качестве развития данного исследования автором проводится формирование физической модели данных и ее апробация на базе первого и крупнейшего в Российской Федерации коммерческого SOC – «Ростелеком-Солар JSOC», а также формирование методологического аппарата и технического инструментария для реагирования на инциденты ИБ с использованием технологий искусственного интеллекта.

СПИСОК ЛИТЕРАТУРЫ:

1. Кузнецов А.В. Эволюция реагирования на инциденты информационной безопасности. Защита информации. Инсайд. 2024, № 5 (119), с. 14–20. – EDN: BHTBVA.
2. Котенко И.В., Саенко И.Б., Лаута О.С., Крибель А.М. Методика обнаружения аномалий и кибератак на основе интеграции методов фрактального анализа и машинного обучения. Информатика и автоматизация. 2022, т. 21, № 6, с. 1328–1358. DOI: https://doi.org/10.15622/ia.21.6.9. – EDN: IWILXQ.
3. Саенко И.Б., Котенко И.В., Аль-Барри М.Х. Применение искусственных нейронных сетей для выявления аномального поведения пользователей центров обработки данных. Вопросы кибербезопасности. 2022, № 2(48), с. 87–97. DOI: 10.21681/2311-3456-2022-2-87-97. – EDN: MFIPIF.
4. Милославская Н.Г. Центры управления информационной безопасностью. Безопасность информационных технологий. 2016, т. 23, № 4, с. 38–51. URL: https://bit.mephi.ru/index.php/bit/article/view/257 (дата обращения: 17.01.2025). – EDN: XIELKX.
5. Месенгисер, Якоб Я.; Малахов, Марк А.; Милославская, Наталья Г. Центры управления сетевой безопасностью как силы ГосСОПКА. Безопасность информационных технологий, [S.l.], т. 29, № 1, с. 94–107, 2022. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2022.1.09. – EDN: BVUFKT.
6. 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. – EDN: KKJTDV.
7. Абрамов С.Е. Построение комплексной системы реагирования на компьютерные инциденты с использованием центра управления информационной безопасностью (SOC). В книге: Радиоэлектроника, электротехника и энергетика. Тезисы докладов Двадцать восьмой международной научно-технической конференции студентов и аспирантов. Москва, 2022, с. 254. – EDN: MKVUHU.
8. Трофимов Д.О., Шепелев М.С., Резниченко С.А. Организация реагирования на инциденты информационной безопасности. Вестник Дагестанского государственного технического университета. Технические науки. 2023, т. 50, № 4, с. 148–157. DOI: https://doi.org/10.21822/2073-6185-2023-50-4-148-157. – EDN: DHORSJ.
9. Осипов Д.Л. Технологии проектирования баз данных. М.: ДМК Пресс, 2019. с. 112–160. – ISBN 978-5-97060-737-4. – EDN: MTSXNP.

10. Горшков Д.А., Кутепова Л.А. Исследование современных методов проектирования баз данных. Успехи современного естествознания. 2011, № 7, с. 98. – EDN: NUTSBX.
11. Симанков В.С., Дриленко М.В. Интеграция информационных ресурсов ситуационных центров. Программные системы и вычислительные методы. 2021, № 4, с. 58–67. DOI: 10.7256/2454-0714.2021.4.34845. – EDN: YCFVXZ.
12. Кузнецов А.В. Конвейер данных для автоматической локализации компьютерных инцидентов. В сборнике: Кибернетика и информационная безопасность «КИБ-2024». Сборник научных трудов Второй Всероссийской научно-технической конференции. Москва. 2024, с. 120–121. – EDN: LJPIKM.
13. Подтопельный В.В. Особенности работы компонентов системы регистрации событий безопасности. В сборнике: Балтийский морской форум. Материалы XI Международного Балтийского морского форума. В 8-ми томах. Калининград. 2023, с. 306–311. – EDN: JRCLEF.
14. Фомин А.В. Особенности работы системы управления инцидентами и взаимодействия с НКЦКИ. Вестник науки. 2023, т. 2, № 5(62), с. 433–436. – EDN: YWJPAY.
15. Башарина О.Ю., Буценко Е.В., Похомчикова Е.О., Шильникова И.С. Технология корпоративной защиты персональных данных и конфиденциальной информации. Современные наукоемкие технологии. 2024, № 2, с. 8–14. DOI: 10.17513/snt.39924. – EDN: JMCXPA.
16. Холкин А.В. Построение модели данных с использованием нотации Ричарда Баркера, IDEF1X, UML. В сборнике: Юность и Знания - гарантия Успеха – 2022. сборник научных статей 9-й Международной молодежной научной конференции: в 3 т. Курск. 2022, с. 282–286. – EDN: AJFPVK.
17. Главацкая О.В. Исследование структурных свойств в моделях БД в нотации IDEF1X. В сборнике: Научное обеспечение технического и технологического прогресса. Сборник статей Международной научно-практической конференции. 2018, с. 18–23. – EDN: YSGFLI.

REFERENCES:

[1] Kuznetsov A.V. The evolution of information security incident response. Zašita informacii. Inside. 2024, № 5(119), p. 14–20. – EDN: BHTBVA (in Russian).
[2] Kotenko I.V., Saenko I.B., Lauta O.S., Kriebel A.M. Anomaly and cyber attack detection technique based on the integration of fractal analysis and machine learning methods. Informatika i avtomatizaciya. 2022, v. 21, no. 6, p. 1328–1358. DOI: https://doi.org/10.15622/ia.21.6.9. – EDN: IWILXQ (in Russian).
[3] Saenko I.B., Kotenko I.V., All-barri M.H. Application of artificial neural networks to reveal abnormal behavior of data center users. Voprosy kiberbezopasnosti. 2022, no. 2(48), p. 87–97. DOI: 10.21681/2311-3456-2022-2-87-97. – EDN: MFIPIF (in Russian).
[4] Miloslavskaya N.G. Information security control centers. Information technology security. IT Security (Russia). 2016, v. 23, no. 4. p. 38–51. URL: https://bit.mephi.ru/index.php/bit/article/view/257 (accessed: 17.01.2025). – EDN: XIELKX (in Russian).
[5] Mesengiser, Yakob Y.; Malakhov, Mark A.; Miloslavskaya, Natalia G. Network security centers as the GosSOPKA forses. It Security (Russia), [S.L.], v. 29, n. 1, p. 94–107, 2022. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2022.1.09. – EDN: BVUFKT (in Russian).
[6] Oleynikova A.A., Zolotarev V.V. The concept of information security management based on a cycle of information security incidents continuous detection and response. Izvestiya YuFU. Technical Sciences. 2023, no. 5(235). p. 66–81. – EDN: KKJTDV (in Russian).
[7] Abramov S.E. Building an integrated computer incident response system using an information security control center (SOC). V knige: Radioelektronika, elektrotekhnika i energetika. tezisy dokladov Dvadcat' vos'moj mezhdunarodnoj nauchno-tekhnicheskoj konferencii studentov i aspirantov. Moskva. 2022, p. 254. – EDN: MKVUHU (in Russian).
[8] 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, v. 50, no. 4, p. 148–157. DOI: https://doi.org/10.21822/2073-6185-2023-50-4-148-157. – EDN: DHORSJ (in Russian).
[9] Osipov D.L. Database design technologies. M.: DMK Press. 2019. p. 112–160. – ISBN 978-5-97060-737-4. – EDN: MTSXNP (in Russian).
[10] Gorshkov D.A., Kutepova L.A. Research of modern methods of database design. Uspekhi sovremennogo estestvoznaniya. 2011, no. 7, p. 98. – EDN: NUTSBX (in Russian).
[11] Simankov V.S., Drilenko M.V. Integration of information resources of situational centers. Programmnye sistemy i vychislitel'nye metody. 2021, no. 4, p. 58–67. DOI: 10.7256/2454-0714.2021.4.34845. – EDN: YCFVXZ (in Russian).
[12] Kuznetsov A.V. Data pipeline for automatic localization of computer incidents. V sbornike: Kibernetika i informacionnaya bezopasnost' "KIB-2024". Sbornik nauchnyh trudov Vtoroj Vserossijskoj nauchno-tekhnicheskoj konferencii. Moskva. 2024, p. 120–121. – EDN: LJPIKM (in Russian).

[13] Podtopelny V.V. Operating features of digital systems segments when recording security events. V sbornike: Baltijskij morskoj forum. Materialy XI Mezhdunarodnogo Baltijskogo morskogo foruma. V 8-mi tomah. Kaliningrad. 2023, p. 306–311. – EDN: JRCLEF (in Russian).
[14] Fomin A.V. Features of incident management system and interaction with the NCICC. Vestnik nauki. 2023, v. 2, no. 5(62), p. 433–436. – EDN: YWJPAY (in Russian).
[15] Basharina O.Yu., Butsenko E.V., Pokhomchikova E.O., Shilnikova I.S. Technology for corporate protection of personal data and confidential information. Modern High Technologies. 2024, no. 2, p. 8–14. DOI: 10.17513/snt.39924. – EDN: JMCXPA (in Russian).
[16] Holkin A.V. Building a data model using Richard Barker's notation, IDEF1X, UML. V sbornike: Yunost' i Znaniya - garantiya Uspekha – 2022. sbornik nauchnyh statej 9-j Mezhdunarodnoj molodezhnoj nauchnoj konferencii: v 3 t. Kursk. 2022, p. 282–286. – EDN: AJFPVK (in Russian).
[17] Главацкая О.В. Study of structural properties in DB models in IDEF1X notation. V sbornike: Nauchnoe obespechenie tehnicheskogo I tehnologicheskogo progressa. Sbornik statej Mezhdunarodnoj nauchno-prakticheskoj konferencii. 2018, p. 18–23. – EDN: YSGFLI (in Russian).

Статья поступила в редакцию 19.01.2025; одобрена после рецензирования 27.03.2025; принята к публикации 14.05.2025
The article was submitted 19.01.2025; approved after reviewing 27.03.2025; accepted for publication 14.05.2025