МЕТОДОЛОГИЯ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РАСПРЕДЕЛЕННЫХ АВТОМАТИЗИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Кузнецов А. В.[1]

DOI: 10.21681/2311-3456-2025-4-65-72

Цель исследования: *формирование единой методологии, позволяющей сократить время и силы, затрачиваемые группой реагирования на инциденты информационной безопасности на локализацию (сдерживание) инцидентов информационной безопасности, возникающих в распределенных автоматизированных информационных системах.*

Метод(ы) исследования: *анализ и синтез имеющихся общедоступных материалов и достижений, в т. ч. запатентованных, по тематикам реагирования на инциденты информационной безопасности и анализа данных, а также моделирование.*

Результат(ы) исследования: *1. Предложены концептуальная модель и единая методология реагирования на инциденты информационной безопасности, которые, в отличие от известных, учитывают особенности построения и обслуживания распределенных автоматизированных информационных систем, акцентируются на активном противодействии атакующему и базируются на принципе датацентричности, что позволяет сократить время и силы, затрачиваемые группой реагирования на инциденты информационной безопасности на локализацию инцидентов информационной безопасности, т. е. повысить эффективность деятельности указанных групп. 2. Сформулированы три метода в рамках предложенной методологии, в т. ч. метод организации единой подсистемы хранения данных мониторинга информационной безопасности и данных инцидентов информационной безопасности, метод предоставления мандата на выполнение действий по локализации инцидентов информационной безопасности, а также метод обработки данных мониторинга информационной безопасности и инцидентов информационной безопасности. Последний метод, в отличие от известных, нацелен на подтверждение инцидента информационной безопасности и принятие решения о необходимости (отсутствии необходимости) его локализации, а также предусматривает проведение обязательной проверки выполнения действий по локализации, что позволяет на каждом этапе реализации предложенной методологии вносить положительный вклад в сокращение времени и сил, затрачиваемых группой реагирования на инциденты информационной безопасности на локализацию инцидентов информационной безопасности, а также удостовериться в реализации действий по локализации инцидентов информационной безопасности.*

Научная новизна: *Концептуальная модель реагирования на инциденты информационной безопасности базируется на непрерывном процессе обработки данных (data pipeline) от четырех различных типов источников данных с учетом атрибутного состава данных, релевантных для конкретной распределенной автоматизированной информационной системы. Методология реагирования на инциденты информационной безопасности акцентируется на активном противодействии атакующему, базируется на принципе датацентричности и предусматривает обязательную проверку выполнения действий по локализации инцидентов информационной безопасности.*

Ключевые слова: *управляемое обнаружение и реагирование, группа реагирования на инциденты, локализация (сдерживание) инцидента, датацентричность, данные, источник данных, метод.*

Введение

Пространственно-распределенные (географически распределенные) автоматизированные информационные системы (РАИС) применяются практически во всех без исключения отраслях экономики Российской Федерации и других стран [1]. Их отличительными особенностями являются использование гетерогенных распределенных компьютерных сетей (от различных провайдеров связи, с различными характеристиками пропускной способности и оконечного оборудования) и географически распределенных центров обработки данных, в т. ч. распределенных баз данных [2, 3], а также централизация управления [4], в случае с нашей страной – на базе одного или нескольких из 16 городов-миллионников. Для компенсации нехватки персонала на местах (удаленных площадках РАИС) и обеспечения круглосуточного режима обслуживания и обеспечения ИБ, в первую очередь, мониторинга ИБ[2], организациями-владельцами (операторами) РАИС привлекаются сторонние провайдеры услуг – Managed

1 Кузнецов Александр Васильевич, кандидат технических наук, CISM, CISSP, ООО «РТК ИБ», Финансовый университет при Правительстве Российской Федерации, Москва. E-mail: 1283_my@mail.ru

2 41% компаний испытывают нехватку специалистов в области информационной безопасности: https://www.kaspersky.ru/about/press-releases/globalnoe-issledovanie-laboratorii-kasperskogo-41-kompanij-ispytyvayut-nehvatku-specialistov-v-oblasti-informacionnoj-bezopasnosti

Detection and Response (MDR) [5], например в нашей стране: Solar JSOC, Positive Technologies ESC, Kaspersky MDR, BI.ZONE TDR, Jet CSIRT, SOC «Перспективный мониторинг», IZ:SOC и/или другие.

При этом превалирующими вариантами реагирования на инциденты ИБ, в первую очередь от MDR-провайдеров[3], являются оповещения по электронной почте [6] и/или заведение заявок в Service Desk системах организаций-заказчиков услуг [7]. При этом только время оповещения (Mean Time to Detect и Mean Time to Report) занимает от десятков минут (37,85-53,99 минут за 2024 год[4]) до нескольких часов и даже дней, и только после этого начнется отсчет времени, затрачиваемого на непосредственное реагирование, включая локализацию (сдерживание) инцидента ИБ. В дополнение к предоставленному атакующему условному временному «окну возможностей», указанные варианты реагирования (фактически – оповещения) не оказывают активного противодействия атакующему, в т. ч. не обеспечивают локализацию обнаруженных инцидентов ИБ. Реализация рекомендаций из оповещений и/или заявок (при условии их наличия, целостности и согласованности), чаще всего, находится вне зоны ответственности групп мониторинга ИБ и координации реагирования на возникающие инциденты ИБ. Таким образом, при кадровом дефиците, особенно на местах (удаленных площадках РАИС), рассчитывать на полноту, качество и, самое главное, своевременность их реализации, к сожалению, не приходится.

Фактически получается, что несколько разрозненных команд (сил), с разным уровнем доступности в 11 часовых поясах России, с разными методами (способами) и средствами (инструментами), в т. ч. каналами и средствами коммуникации, не могут оперативно (в течение нескольких минут, а в идеале – секунд) и согласованно (в рамках единого набора данных) противодействовать современным компьютерным атакам (кибератакам), в т. ч. целенаправленным кибератакам (принимая во внимание, что требуется от 30 минут и, в большей половине случаев, 1-2 шага для проникновения в ЛВС организации[5], а в некоторых случаях – от 25 минут с момента проникновения до нанесения ущерба[6]).

Усугубляет ситуацию ежегодное увеличение количества фиксируемых инцидентов ИБ[7], в т. ч. в кредитно-финансовом секторе[8].

Таким образом, на фоне роста активностей атакующих, повышение эффективности деятельности групп реагирования на инциденты ИБ (ГРИИБ) за счет оптимизации и автоматизации мероприятий по локализации инцидентов ИБ является актуальным направлением исследований, особенно для организаций-владельцев (операторов) РАИС, а также центров Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА) и координационных центров групп реагирования на компьютерные инциденты (Computer Emergency Response Team Coordination Center (CERT CC)).

Ограничения исследования

В рамках настоящего исследования автором были приняты следующие ограничения и допущения:

- не рассматриваются РАИС, построенные с использованием технологий распределенных реестров (Distributed Ledger Technology (DLT));
- в части мероприятий по реагированию на инциденты ИБ рассматривались только первоочередные действия, оказывающие активное противодействие атакующему, т. е. действия по локализации (сдерживанию) инцидентов ИБ, развивая и дополняя предыдущие исследования автора [4, 8, 9];
- не проводилось деление между понятиями «инцидент ИБ»[9], «компьютерный инцидент»[10], «инцидент защиты информации»[11] и «киберинцидент»[12], указанные понятия рассматривались автором как синонимы (результаты настоящего исследования применимы к любому указанному терминологическому аппарату).

Концептуальная датацентричная модель реагирования на инциденты ИБ

На сегодняшний день есть несколько международных и национальных стандартов по управлению, в т. ч. реагированию на инциденты ИБ[13], обзор, которых проводился автором ранее [8]. Все существующие стандарты рассматривают предмет исследования

3 Эволюция реагирования: от ручных процессов к интеллектуальным решениям: https://forumsoc.ru/program/

4 Analyst report. Managed Detection and Response: https://content.kaspersky-labs.com/fm/site-editor/b7/b7766f565d5f14783d6848364b8fde66/source/mdr-report.pdf

5 Итоги внешних пентестов – 2020: https://www.ptsecurity.com/ru-ru/research/analytics/external-pentests-2020/

6 Самый незаметный вредонос и слова-загадки из кода. В Kaspersky рассказали о рекордах хакеров: https://www.gazeta.ru/tech/2023/08/10/17407172.shtml

7 Хроники DFIR: как атаковали APT-группировки с января по октябрь 2024 года: https://rt-solar.ru/analytics/reports/4857/

8 Кибератаки на финансовый сектор в 2024 году: https://rt-solar.ru/analytics/reports/5206/

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

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

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

12 ГОСТ Р 57580.3-2022 «Безопасность финансовых (банковских) операций. Управление риском реализации информационных угроз и обеспечение операционной надежности. Общие положения».

13 NIST SP 800-61 Rev. 3 (Initial Public Draft) «Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile», ISO/IEC 27035-1:2023 «Information technology — Information security incident management — Part 1: Principles and process», ГОСТ Р 59710-2022 «Защита информации. Управление компьютерными инцидентами. Общие положения», Рекомендации в области стандартизации Банка России РС БР ИББС-2.5-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Менеджмент инцидентов информационной безопасности».

через процессный подход, ориентированный на цикл непрерывного совершенствования, и не рассматривают основополагающим принцип датацентричности [10, 11], без которого невозможно реализовать data-driven подход к реагированию на инциденты ИБ.

Здесь же стоит отметить, что существует несколько открытых проектов: фреймворк для техник реагирования на инциденты ИБ RE&CT[14] и модель (база) знаний ERM&CK[15], которые ориентированы на практическую, точечную автоматизацию, но не предлагают взаимосвязанного набора методов решения задач, возникающих в рамках обработки разрозненных данных.

В завершении обзора существующих вариантов решения, стоит отметить ряд запатентованных способов автоматизации реагирования на инциденты ИБ[16], которые предлагают только отдельные технические решения (системы), не формируя единую методологию решения возникшей проблемы.

Методология рассматривается автором как совокупность методов, имеющих общие принципы, условия реализации и предназначенные для достижения цели настоящего исследования[17], при этом основным принципом для данной методологии будет выступать датацентричность.

Принимая во внимание недостатки существующих подходов и решений автором предлагается следующая концептуальная модель реализации мероприятий по реагированию на инциденты ИБ, представленная в нотации Event-Driven Process Chain (рис. 1).

В основе данной модели лежит предложенный автором непрерывный процесс (конвейер) обработки данных (data pipeline) [9]. Предлагаемая модель позволяет перейти к автономности ГРИИБ (не привлечению приходящих системных администраторов, местных подрядчиков и т. п.) и работе на основе актуальных и релевантных для конкретной РАИС данных (сгенерированных в рамках функционирования РАИС и ее подсистемы обеспечения ИБ), а не на экспертизе отдельных специалистов (в т. ч. специалистов MDR-провайдеров) или использовании данных, относящихся к другим организациям, отраслям экономики и/или регионам страны.

На модели отмечены основные временные характеристики, используемые при описании процессов обнаружения и реагирования на инциденты ИБ

14 RE&CT: https://atc-project.github.io/atc-react/index_RU/
15 ERMACK: https://github.com/Security-Experts-Community/ERMACK
16 US20090296898 – Automated incident response method and system: https://patentscope.wipo.int/search/ru/detail.jsf?docId=US42906733. US10051010B2 – Method and system for automated incident response: https://patents.google.com/patent/US10051010B2

17 Манушин Д. В. Уточнение понятия «методология» // Финансы и кредит. 2015. № 41 (665). С. 50–66

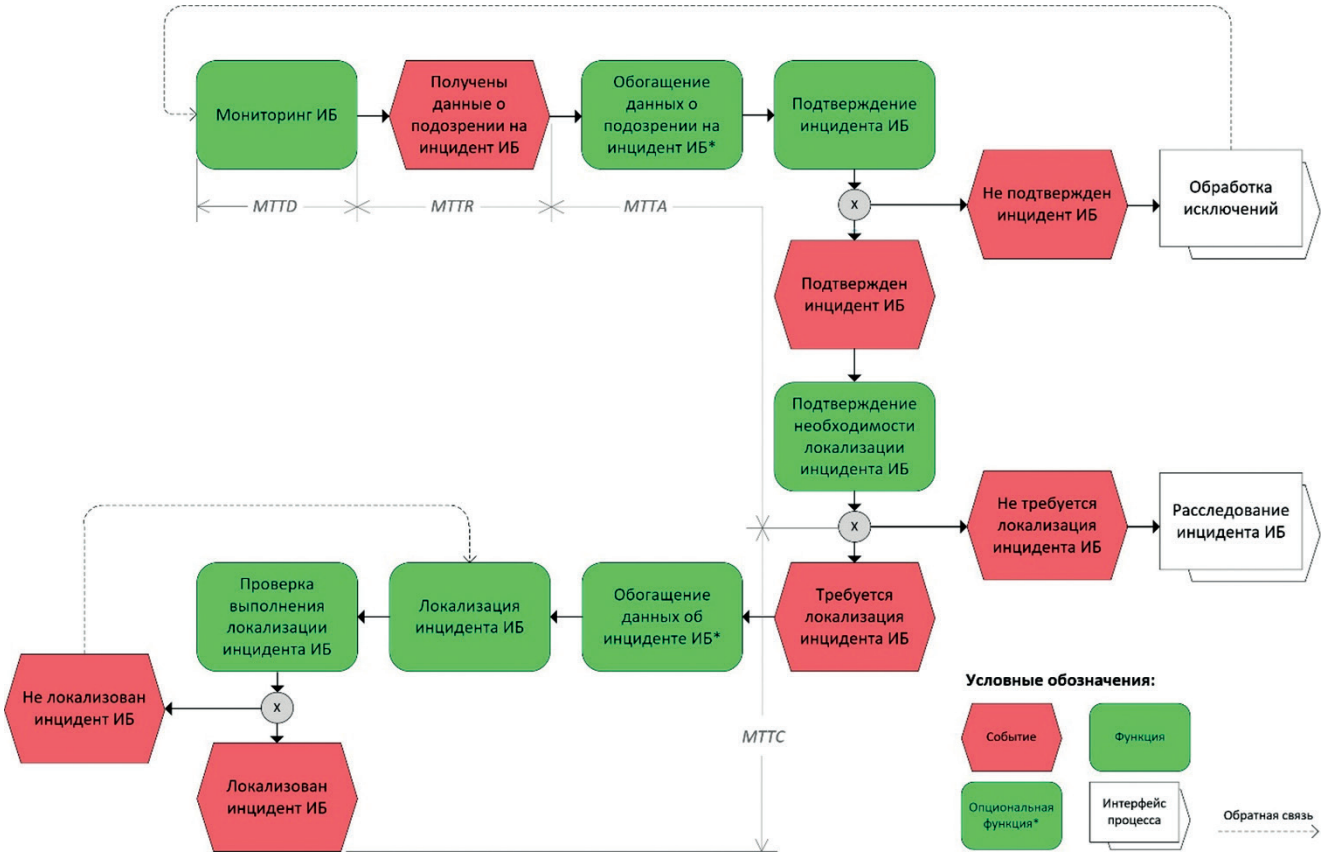

Рис. 1. Концептуальная датацентричная модель реагирования на инциденты ИБ (локализации инцидентов ИБ)

в Security Operations Center (SOC) [12], а также ГРИИБ и CERT CC:

- Mean Time to Detect/Discover (MTTD): среднее время, необходимое для обнаружения (выявления) инцидента ИБ, отсчитываемое с момента выполнения несанкционированных действий атакующим в отношен РАИС и до момента их детектирования (распознавания) системами обнаружения или персоналом организации; в ряде случаев дополнительно учитывается время, затрачиваемое на корреляцию событий (данных) системами обнаружения, в т. ч. SIEM-системами;
- Mean Time to Report (MTTR): среднее время, необходимое для формирования и реализации оповещения с использованием соответствующих каналов и средств коммуникации, отсчитываемое с момента обнаружения и до момента получения оповещения (регистрации подозрения на инцидента ИБ в формате карточки);
- Mean Time to Acknowledge (MTTA): среднее время, необходимое для подтверждения санкционированности или несанкционированности действий, отсчитываемое с момента получения оповещения и до момента вынесения вердикта по подозрению на инцидент ИБ («Подтвержденный», «Ложный» или «Санкционированное действие»);
- Mean Time to Respond/Contain (MTTC): среднее время, необходимое для локализации (сдерживания) инцидента ИБ, отсчитываемое с момента вынесения вердикта «Подтвержденный» и до определения и ограничения функционирования информационных ресурсов (компонентов РАИС), на которых обнаружены признаки зарегистрированного инцидента ИБ, с целью предотвращения его дальнейшего распространения (указанная временная характеристика представляет наибольший интерес в рамках настоящего исследования).

Безусловно, без качественного и своевременного обнаружения инцидентов ИБ невозможно проводить какие-либо мероприятия по реагированию (неважно в ручном или автоматическом режиме [8]). Но сразу стоить отметить, что тематике обнаружения (мониторинга ИБ), в т. ч. на основе больших данных, с использованием машинного обучения и систем искусственного интеллекта (ИИ) посвящено значительное число работ. К ведущим коллективам российских ученых, работающим в данном направлении, можно отнести коллективы под руководством Милославской Н. Г. [13], а также Котенко И. В. и Саенко И. Б. [14, 15]. Как следствие, указанная предметная область в полном объеме не входит в предмет настоящего исследования, но требует фиксации, в т. ч. синтеза необходимых входных условий (данных) для формирования единой датацентричной методологии.

Таким образом, в части обнаружения инцидентов ИБ на основе данных необходимо определить все типы источников данных, которые могут выступать «триггерами» для регистрации инцидентов ИБ, и атрибутный состав данных (неотъемлемая часть логической модели данных). На практике выделяют два основных источника данных: источники событий безопасности [16] и персонал, но этого недостаточно. Автором предлагается следующий набор типов источников данных мониторинга ИБ с указанием атрибутного состава данных:

- обращения пользователей: дата и время обращения, источник несанкционированной активности (источник), цель несанкционированной активности (цель), тип несанкционированной активности;
- данные о событиях безопасности: дата и время обнаружения, источник, цель, тип события безопасности;
- данные киберразведки: хронологические метки даты и времени, источник и/или цель, значение индикатора компрометации (описание техники и/или описание уязвимости, и/или хэш-значение);
- данные об уязвимостях: цель, описание уязвимости, класс уязвимости, степень опасности уязвимости.

Предложенный вариант, в отличие от известных, расширяет типы источников данных до четырех, что позволяет снизить статистическую вероятность (относительную частоту) пропуска инцидентов ИБ (ошибок второго рода) или несвоевременности их обнаружения.

В части категоризации вариантов реализации действий по локализации инцидентов ИБ автором предлагаются следующие варианты:

- полностью автоматическая локализация: выполнение действий без привлечения специалистов ГРИИБ;
- полуавтоматическая локализация: выполнение действий с привлечением специалистов ГРИИБ для явного подтверждения (в единой консоли управления карточками инцидентов ИБ) их дальнейшего автоматического выполнения;
- ручная локализация: выполнение действий непосредственно специалистами ГРИИБ с использованием информационных ресурсов (компонентов РАИС) и/или средств реагирования (например: непосредственное подключение к консоли управления средства реагирования);
- физическая локализация: выполнение действий специалистами ГРИИБ или специалистами на удаленных площадках без использования информационных ресурсов (компонентов РАИС) и средств реагирования (например: физическое выключение электропитания).

Для полностью автоматической и полуавтоматической локализации требуется наличие мандата на выполнение действия – цифровой записи, содержащей идентификационную информацию, характеризующую условия локализации инцидентов ИБ, с учетом заданных критериев [17].

При этом стоит отметить, что не все инциденты ИБ требуют незамедлительной локализации, часть требует проведения мероприятий по расследованию инцидентов ИБ (forensic) [18], но данные мероприятия находятся за рамками настоящего исследования, т. к. не оказывают активного противодействия атакующему.

Методы, предназначенные для достижения цели настоящего исследования

Автором предлагается следующий набор взаимоувязанных методов, объединенных принципом датацентричности, направленных на достижение цели настоящего исследования, формирующих единую методологию реагирования на инциденты ИБ в РАИС: M_1, M_2 и M_3.

M_1: метод организации единой подсистемы хранения данных мониторинга ИБ и данных инцидентов ИБ, который, в отличие от известных, учитывают доступную ширину полосы пропускания используемого канала связи между компонентами сбора данных (коллекторами) и компонентами «горячего» и «холодного» хранения данных (на основе работы автора [19]).

Обозначив $L_1 = \{l_{1i}\}$ – множеством всех площадок РАИС, $S \in [0;+\infty)$ – размером одной порции данных, $E \in [0;+\infty)$ – усредненным за сутки потоком данных, $B_i \in [0;+\infty)$ – доступной шириной полосы пропускания используемого канала связи до i-й площадки, $L_2 = \{l_{2j}\}$ – множеством площадок РАИС с компонентами единой подсистемы хранения данных, а также введя условие, определяющее возможность централизации подсистемы хранения данных (1).

$$(S + 58) \cdot E \cdot 8 \cdot 9{,}54 \cdot 10^{-7} \le B_i. \quad (1)$$

Под методом будем понимать отображение $M_1 : L_1 \longrightarrow L_2$.

Без единой подсистемы хранения данных невозможно реализовать data-driven вариант реагирования на инциденты ИБ в РАИС.

M_2: метод предоставления мандата на выполнение действий по локализации инцидентов ИБ, который, в отличие от известных, учитывает вариативность и взаимосвязи различных критериев предоставления мандата, релевантных для конкретной РАИС (на основе работы автора [17]).

Обозначив $Cr_1 = \{c_q\}$ – множеством возможных мандатов, $A = \{a_{p,k}\}$ – матрицей влияния критерия на предоставление мандата, $X = \{x_k\}$ – вектором целочисленных переменных, отражающих соблюдение k-го критерия предоставления мандата, $Cr_2 = \{c_w\}$ – множеством предоставленных мандатов; под методом будем понимать отображение $M_2 : Cr_1 \longrightarrow Cr_2$.

Оператор предоставления мандата для локализации инцидентов ИБ будет иметь вид (2).

$$F_{cr}(Cr_1,A,X) = \begin{cases} 1, & \text{мандат для локализации предоставляется;} \\ 0, & \text{мандат для локализации не предоставляется.} \end{cases}. \quad (2)$$

Без предоставления мандатов невозможно сократить вовлечение сил ГРИИБ и время, затрачиваемое группой на локализацию инцидентов ИБ.

M_3: метод обработки данных мониторинга ИБ и инцидентов ИБ, который, в отличие от известных, базируется на концептуальной датацентричной модели (рис. 1) и нацелен на подтверждение инцидента ИБ и принятие решения о необходимости (отсутствии необходимости) его локализации, а также предусматривает проведение обязательной проверки выполнения действия по локализации.

Обозначив $V_1 = \{v_{1t}\}$ – множеством обнаруженных инцидентов ИБ, $C = \{c_y\}$ – множеством мер по локализации, $V_2 = \{v_{1o}\}$ – множеством локализованных инцидентов ИБ; под методом будем понимать отображение $M_3 : V_1 \longrightarrow V_2$.

Оператор локализации инцидента ИБ v_{1t} будет иметь вид (3).

$$F_r(V_1,C,Cr_2) = \begin{cases} 1, & \text{если инцидент ИБ } v_{1t} \text{ локализован;} \\ 0, & \text{если инцидент ИБ } v_{1t} \text{ не локализован.} \end{cases}. \quad (3)$$

Выводы

По результатам проведенного исследования автором:

1. Предложены концептуальная модель и единая методология реагирования на инциденты ИБ, которые, в отличие от известных, учитывают особенности построения и обслуживания РАИС, акцентируются на активном противодействии атакующему и базируются на принципе датацентричности, что позволяет сократить время и силы, затрачиваемые ГРИИБ на локализацию инцидентов ИБ, т. е. повысить эффективность деятельности указанных групп.

2. Сформулированы три метода M_1, M_2 и M_3 в рамках предложенной методологии, в т. ч. M_3: метод обработки данных мониторинга ИБ и инцидентов ИБ, который, в отличие от известных, нацелен на подтверждение инцидента ИБ и принятие решения о необходимости (отсутствии необходимости) его локализации, а также предусматривает проведение обязательной проверки выполнения действия по локализации, что позволяет на каждом этапе реализации предложенной методологии вносить положительный вклад в сокращение времени

и сил, затрачиваемых ГРИИБ на локализацию инцидентов ИБ, а также удостовериться в реализации действий по локализации.

Применение результатов настоящего исследования дает положительный эффект в области технических наук: научная специальность «Методы и системы защиты информации, ИБ», а также могут быть применимы в смежной научной специальности: «ИИ и машинное обучение», при рассмотрении проблем и задач применения ИИ в обнаружении и реагировании на инциденты ИБ[18].

Практическое применение предложенной методологии позволит внести значительный положительный вклад в развитие ГРИИБ, в т. ч. центров ГосСОПКА и CERT CC.

Предложенная методология в 2023–2025 гг. проходит апробацию в рамках выполнения работ в интересах организаций-владельцев РАИС федерального масштаба, а также ведущих организаций-лицензиатов ФСТЭК России, оказывающих услуги по мониторингу ИБ средств и систем информатизации[19] на территории всей страны.

Развитием данной data-driven методологии является переход к AI-driven методологии, которую отдельные лидеры ИТ/ИБ-отрасли уже начали демонстрировать (например, корпорация Microsoft в 2023 году запустила ИИ-помощника для групп мониторинга ИБ и реагирования – Security Copilot[20]). Стоит отметить, что уже есть успешные отдельные примеры автоматизации процедур условного реагирования на инциденты ИБ, в части установки обновлений для программного обеспечения [20, 21], в т. ч. появилось понятие – Vulnerability Management Detection and Response (VMDR)[21].

18 Are AI-powered SOCs the future of cybersecurity?: https://www.tahawultech.com/insight/are-ai-powered-socs-the-future-of-cybersecurity/. The rise of autonomous SOCs: embracing AI-powered security operations for the ever-evolving threat landscape: https://global.ptsecurity.com/analytics/autonomous-socs-ai-powered-security-operations-for-evolving-threat-landscape

19 Положение о лицензировании деятельности по технической защите конфиденциальной информации, утв. постановлением Правительства Российской Федерации от 03.02.2012 г. N 79.

20 What is Microsoft Security Copilot?: https://learn.microsoft.com/en-us/security-copilot/microsoft-security-copilot

21 VMDR: Inside vulnerability management, detection and response: https://www.techtarget.com/searchsecurity/feature/VMDR-Inside-vulnerability-management-detection-and-response

Литература

1. Braione P., Briola D., De Angelis G., Gallo F., Poggi F., Quattrocchi G. About the special issue on: «Distributed Complex Systems: Governance, Engineering, and Maintenance» // Journal of Software: Evolution and Process. 2022. Т. 34. № 10. DOI: https://doi.org/10.1002/smr.2459.
2. Созонтов А. В. Распределенные информационные системы: особенности применения и построения // Актуальные исследования. 2023. № 37-1 (167). С. 69–74.
3. Панделов Т. С., Янаева М. В. Территориально-распределенные информационные системы // Молодой исследователь Дона. 2022. № 6 (39). С. 59–62.
4. Кузнецов А. В. Особенности реагирования на инциденты в пространственно-распределенных автоматизированных информационных системах // Инженерный вестник Дона: сетевое издание. 2025. № 5-25. URL: http://www.ivdon.ru/ru/magazine/archive/n5y2025/10046 (дата обращения 12.05.2025).
5. Зайчиков Н. План действий ИТ-службы в эпоху замещения // Системный администратор. 2022. № 5 (234). С. 20–23.
6. Хохлов А. Ю., Асанов С. А. Использование технологической платформы «1С: Предприятие» для автоматизации учёта и уведомления ГосСОПКА об инцидентах информационной безопасности объектов критической информационной инфраструктуры // В сборнике: Россия молодая. Сборник материалов XVI всероссийской, научно-практической конференции молодых ученых с международным участием. Кемерово, 2024. С. 31691.1–31691.8.
7. Репецкий С. О., Репецкая Н. В. Обработка заявок в IT Service Desk // StudNet: сетевой журнал. 2021. Т. 4. № 5. URL: https://stud.net.ru/obrabotka-zayavok-v-it-service-desk/ (дата обращения 12.05.2025).
8. Кузнецов А. В. Эволюция реагирования на инциденты информационной безопасности // Защита информации. Инсайд. 2024. № 5(119). С. 14–20.
9. Кузнецов А. В. Конвейер данных для автоматической локализации компьютерных инцидентов // Вторая Всероссийская научно-техническая конференция «Кибернетика и информационная безопасность «КИБ-2024». Сборник научных трудов. 22-23 октября 2024 г., Москва. М.: НИЯУ МИФИ. 2024. С. 120-121.
10. Зеневич А. М., Пунчик З. В. Датацентричность как тренд развития корпоративных информационных систем // В сборнике: Эколого-экономические и технологические аспекты устойчивого развития Республики Беларусь и Российской Федерации. сборник статей III Международной научно-технической конференции: в 3 т. Минск, 2021. С. 179–182.
11. Гладилина И. П., Сергеева С. А., Синицына Е. В. Цифровая этика и этика данных как основа рациональной деятельности экономических субъектов в условиях цифровой трансформации // Экономические системы. 2024. Т. 17. № 4. С. 28–38. DOI: 10.29030/2309-2076-2024-17-4-28-38.
12. Расширенная модель зрелости SOC компании Cybereason / И. С. Листратов, Н. Г. Милославская, И. С. Сирбай, Б. А. Рейносо // Безопасность информационных технологий. 2025. Т. 32. № 1. С. 68–84. DOI: 10.26583/bit.2025.1.04.
13. Месенгисер Я. Я., Малахов М. А., Милославская Н. Г. Центры управления сетевой безопасностью как силы ГосСОПКА // Безопасность информационных технологий. 2022. Т. 29. № 1. С. 94–107. DOI: http://dx.doi.org/10.26583/bit.2022.1.09.
14. Методика обнаружения аномалий и кибератак на основе интеграции методов фрактального анализа и машинного обучения / И. В. Котенко, И. Б. Саенко, О. С. Лаута, А. М. Крибель // Информатика и автоматизация. 2022. Т. 21. № 6. С. 1328–1358. DOI: https://doi.org/10.15622/ia.21.6.9.

15. 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.
16. Андрушкевич Д. В., Андрушкевич С. С., Крюков Р. О. Метод реагирования на целевые атаки, основанный на отображении событий информационной безопасности с применением индикационных сигнатур // Проблемы информационной безопасности. Компьютерные системы. 2023. № 4(57). С. 48–60.
17. Кузнецов А. В. Анализ критериев предоставления мандата на локализацию инцидента информационной безопасности // Инженерный вестник Дона: сетевое издание. 2025. № 3-25. URL: http://www.ivdon.ru/ru/magazine/archive/n3y2025/9919 (дата обращения 12.05.2025).
18. Смирнов С. И. Методика расследования киберинцидента, основанная на интеллектуальном анализе событий безопасности домена // Защита информации. Инсайд. 2022. № 4(106). С. 60–69.
19. Кузнецов А. В. Организация раздельного хранения данных о событиях безопасности // Вопросы кибербезопасности. 2024. № 2(60). С. 22–28. DOI: 10.21681/2311-3456-2024-2-22-28.
20. Yu Nong, Haoran Yang. Automated Software Vulnerability Patching using Large Language Models. August, 2024. URL: https://arxiv.org/html/2408.13597v1 (дата обращения 12.05.2025). DOI:10.48550/arXiv.2408.13597.
21. Minjae Seo, Wonwoo Choi, Myoungsung You, Seungwon Shin. AutoPatch: Multi-Agent Framework for Patching Real-World CVE Vulnerabilities. May 2025. URL: https://arxiv.org/abs/2505.04195 (дата обращения 12.05.2025). DOI: 10.48550/arXiv.2505.04195.

THE METHODOLOGY OF INFORMATION SECURITY INCIDENTS RESPONSE WITHIN DISTRIBUTED AUTOMATED INFORMATION SYSTEMS

Kuznetsov A. V.[22]

Keywords: *managed detection and response, incident response team, incident localization (containment), data-centricity, data, data source, method.*

Purpose of the study: *to develop the unified methodology to reduce the time and effort spent by an information security incident response team to localize (contain) information security incidents occurring in distributed automated information systems.*

Methods of research: *analysis and synthesis of existing publicly available materials and advances, including patented ones, related to information security incident response and data analysis, as well as modeling.*

Result(s): *1. The conceptual model and unified methodology of information security incident response are proposed, which, unlike the known ones, take into account the specifics of construction and maintenance of distributed automated information systems, focus on active counteraction to the attacker and are based on the principle of data-centricity, which reduces the time and effort spent by an information security incident response team to localize information security incidents, i.e., increase the efficiency of the activity of an information security incident response team. 2. Three methods within the proposed methodology are formulated, including the method of organizing the unified subsystem for storing information security monitoring data and information security incident data, the method of providing a mandate to perform an action to localize an information security incident, and the method of processing information security monitoring data and information security incident data. The latter method, unlike the known ones, is aimed at confirming the information security incident and making a decision on the need (lack of need) for its localization, and also provides for mandatory verification of the localization action, which allows at each stage of implementation of the proposed methodology to make a positive contribution to reducing the time and effort spent by an information security incident response team to localize information security incidents, as well as ascertain that actions to localize information security incidents were implemented.*

Scientific novelty: *The conceptual model of response to information security incidents is based on a continuous process of data processing (data pipeline) from four different types of data sources, taking into account the attribute composition of data relevant to a particular distributed automated information system. The information security incident response methodology focuses on active counteraction to the attacker, is based on the principle of data-centricity, and provides for mandatory verification that actions to localize information security incidents were implemented.*

References

1. Braione P., Briola D., De Angelis G., Gallo F., Poggi F., Quattrocchi G. About the special issue on: «Distributed Complex Systems: Governance, Engineering, and Maintenance» // Journal of Software: Evolution and Process. 2022. Т. 34. № 10. DOI: https://doi.org/10.1002/smr.2459.

22 Aleksandr V. Kuznetsov, Ph.D. (in Tech.), CISM, CISSP, RTK IS LLC, Financial University under the Government of the Russian Federation, Moscow. E-mail: 1283_my@mail.ru.

2. Sozontov, A. V. Raspredelennye informacionnye sistemy: osobennosti primeneniya i postroeniya // Aktual'nye issledovaniya. 2023. № 37-1 (167). pp. 69–74.
3. Pandelov, T. S., Yanaeva, M. V. Geographically distributed information systems // Young Researcher of Don. 2022. № 6(39). pp. 59–62.
4. Kuznetsov, A. V. Osobennosti reagirovaniya na incidenty v prostranstvenno-raspredelennyx avtomatizirovannyx informacionnyx sistemax // Inzhenernyj vestnik Dona. 2025. № 5-25. URL: ivdon.ru/ru/magazine/archive/n3y2025/9919 (accessed 12.05.2025).
5. Zajchikov, N. Plan dejstvij IT-sluzhby v epoxu zameshheniya // Sistemnyj administrator. 2022. № 5 (234). pp. 20–23.
6. Hohlov, A. Yu., Asanov. S. A. Ispol'zovanie texnologicheskoj platformy «1S: Predpriyatie» dlya avtomatizacii uchyota i uvedomleniya GosSOPKA ob incidentax informacionnoj bezopasnosti ob''ektov kriticheskoj informacionnoj infrastruktury // V sbornike: Rossiya molodaya. Sbornik materialov XVI vserossijskoj, nauchno-prakticheskoj konferencii molodyx uchenyx s mezhdunarodnym uchastiem. Kemerovo, 2024. pp. 31691.1–31691.8.
7. Repeckij, S. O., Repeckaya, N. V. Obrabotka zayavok v IT Service Desk // StudNet. 2021. T. 4. № 5. URL: https://stud.net.ru/obrabotka-zayavok-v-it-service-desk/ (accessed 12.05.2025).
8. Kuznetsov, A. V. The Evolution of Information Security Incident Response // Zaŝita informacii. Inside. 2024. № 5 (119). pp. 14–20.
9. Kuznetsov, A. V. Konvejer dannyx dlya avtomaticheskoj lokalizacii komp'yuternyx incidentov // Vtoraya Vserossijskaya nauchno-texnicheskaya konferenciya «Kibernetika i informacionnaya bezopasnost' «KIB-2024». Sbornik nauchnyx trudov. 22-23 oktyabrya 2024 g., Moskva. M.: NRNU MEPhI. 2024. Pp. 120-121.
10. Zenevich, A. M., Punchik, Z. V. Datacentrichnost' kak trend razvitiya korporativnyx informacionnyx sistem // V sbornike: Ekologo-ekonomicheskie i texnologicheskie aspekty ustojchivogo razvitiya Respubliki Belarus' i Rossijskoj Federacii. sbornik statej III Mezhdunarodnoj nauchno-texnicheskoj konferencii: v 3 t.. Minsk, 2021. pp. 179–182.
11. Gladilina, I. P., Sergeeva, S. A., Sinitsyna, E. V. Digital ethics and data ethics as the basis for the rational activities of economic entities in the context of digital transformation // Economic Systems. 2024. T. 17. № 4. pp. 28–38. DOI: 10.29030/2309-2076-2024-17-4-28-38.
12. Extended Cybereason's SOC maturity model / Listratov, I. S., Miloslavskaya, N. G., Sirbay, I. S., Reinoso, B. A. // IT Security. 2025. T. 32. № 1. pp. 68–84. DOI: 10.26583/bit.2025.1.04.
13. Mesengiser, Y. Y., Malakhov, M. A., Miloslavskaya, N. G. Network Security Centers as the GosSOPKA Forses // IT Security. 2022. T. 29. № 1. pp. 94–107. DOI: http://dx.doi.org/10.26583/bit.2022.1.09.
14. Anomaly and cyber-attack detection technique based on the integration of fractal analysis and machine learning methods / Kotenko, I.V., Saenko, I. B., Lauta, O. S., Kriebel, A. M. // Informatics and Automation. 2022, T. 21, № 6. pp. 1328–1358. DOI: https://doi.org/10.15622/ia.21.6.9.
15. 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. № 2(48). Pp. 87–97. DOI: 10.21681/2311-3456-2022-2-87-97.
16. Andrushkevich, D. V., Andrushkevich, S. S., Kryukov, R. O. Metod reagirovaniya na celevye ataki, osnovannyj na otobrazhenii sobytij informacionnoj bezopasnosti s primeneniem indikacionnyx signatur // Information Security Problems. Computer Systems. 2023. № 4(57). pp. 48–60.
17. Kuznetsov, A. V. Analiz kriteriev predostavleniya mandata na lokalizaciyu incidenta informacionnoj bezopasnosti // Inzhenernyj vestnik Dona. 2025. № 3-25. URL: http://www.ivdon.ru/ru/magazine/archive/n3y2025/9919 (accessed 12.05.2025).
18. Smirno, S. I. Cyber incident investigation methodology based on intelligent analysis of domain security events // Zaŝita informacii. Inside. 2022. № 4(106). pp. 60–69.
19. Kuznetsov, A. V. The organization of separate security event data storage // Voprosy kiberbezopasnosti. 2024. № 2 (60). Pp. 22–28. DOI: 10.21681/2311-3456-2024-2-22-28.
20. Yu Nong, Haoran Yang. Automated Software Vulnerability Patching using Large Language Models. August 2024. URL: https://arxiv.org/html/2408.13597v1 (accessed 12.05.2025). DOI:10.48550/arXiv.2408.13597.
21. Minjae Seo, Wonwoo Choi, Myoungsung You, Seungwon Shin. AutoPatch: Multi-Agent Framework for Patching Real-World CVE Vulnerabilities. May 2025. URL: https://arxiv.org/abs/2505.04195 (accessed 12.05.2025). DOI: 10.48550/arXiv.2505.04195.