ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004.056.5

DOI: 10.21822/2073-6185-2025-52-2-74-80 Оригинальная статья/ Original article

Сервис управления и анализа инцидентов информационной безопасности

О.Ю. Башарина, Е.В. Буценко, А.С. Еремеев
Уральский государственный экономический университет,
620144, г. Екатеринбург, ул.8 Марта, 62, Россия

Резюме. Цель. В работе рассмотрены вопросы проектирования и разработки сервиса для автоматизации процессов управления и анализа инцидентами информационной безопасности для металлургического предприятия; обследованы и описаны основные этапы и действия управления инцидентами на данном предприятии. **Метод.** Программный сервис, позволяющий автоматизировать процессы мониторинга, оценки и анализа нежелательных и неожиданных событий информационной безопасности, разработан в среде Visual Studio Code на высокоуровневом языке программирования Python. Для расширения функционала созданного программного приложения использовались дополнительные фреймворки и необходимые библиотеки. Хранение информации об инцидентах компании организовано в созданной базе данных. **Результат.** Описан алгоритм разработки программного сервиса, представлены примеры экранных форм данного приложения. Функционал сервиса позволяет получать различную аналитику: общий и детальный анализ произошедших инцидентов по типам, способам обнаружения, временны́м затратам на решение инцидента, уровню критичности, статусу, способу обнаружения, быстроте реагирования, причиненным последствиям. **Вывод.** Апробация программного сервиса в отделе информационной безопасности показала эффективное обнаружение новых атак и оперативную защиту информационных систем и автоматизированного оборудования предприятия. Анализ инцидентов направлен также на выявление проблемных участков в работе служб информационной безопасности компании, устранение которых позволит гораздо быстрее обнаруживать нежелательные события и минимизировать повторное появление инцидентов и их последствия.

Ключевые слова: программная система, информационная безопасность, инцидент, угроза, распознавание, анализ, управление, реагирование

Для цитирования: О.Ю. Башарина, Е.В. Буценко, А.С. Еремеев. Сервис управления и анализа инцидентов информационной безопасности. Вестник Дагестанского государственного технического университета. Технические науки. 2025; 52(2):74-80. DOI:10.21822/2073-6185-2025-52-2-74-80

Information security incident management and analysis service

O.Yu. Basharina, E.V. Butsenko, A.S. Eremeev
Ural State University of Economics,
62 8 Marta St., Yekaterinburg 620144, Russia

Abstract. Objective. The paper considers the issues of designing and developing a service for automating the management and analysis of information security incidents for a metallurgical enterprise. The main stages and actions of incident management at the enterprise are examined and described. **Methods.** A software service that allows you to automate the processes of monitoring, evaluating and analyzing undesirable and unexpected information security events has been developed in the Visual Studio Code environment in the high-level Python programming language. To expand the functionality of the created software application, additional frameworks and the necessary libraries were used. The storage of information about the company's incidents is organized in the created database. **Result.** The article describes the algorithm for developing a software service, and provides examples of screen forms of this application. The functionality of the service

allows you to receive various analytics: a general and detailed analysis of incidents by type, detection methods, time spent on solving the incident, the level of criticality, status, method of detection, speed of response, and the consequences caused. **Conclusion.** Testing of the software service demonstrated effective detection of new attacks and prompt protection of information systems and automated equipment of the enterprise. Incident analysis is aimed at identifying problem areas in the work of information security services, the elimination of which will allow for faster detection of unwanted events and minimization of the recurrence of incidents and their consequences.

Keywords: software system, information security, incident, threat, recognition, analysis, management, response

For citation: O.Yu. Basharina, E.V. Butsenko, A.S. Eremeev. Information security incident management and analysis service. Herald of Daghestan State Technical University. Technical Sciences. 2025;52(2):74-80. (In Russ.) DOI:10.21822/2073-6185-2025-52-2-74-80

Введение. В современном мире с развитием IT-технологий обеспечение информационной безопасности (ИБ) является неотъемлемой частью построения бизнес-процессов предприятий. Рост объемов данных, расширение сетей и увеличение числа подключенных устройств создают различные уязвимости и возможности для кибератак. Каждая организация, независимо от её размера и сферы деятельности, сталкивается с угрозой утечки конфиденциальной информации, которая может повлечь за собой финансовые, имиджевые потери и прочие негативные последствия [1, 2, 3]. Одной из основных задач обеспечения ИБ является работа специалистов с инцидентами. Поэтому разработка сервиса анализа инцидентов с целью повышения эффективности этой работы приобретает особую важность для каждого предприятия. С помощью данного сервиса можно проанализировать произошедшие инциденты для снижения ущерба от возникновения таких нежелательных событий и предотвращения их появления в будущем.

Инцидент информационной безопасности – событие, являющееся следствием одного или нескольких нежелательных или неожиданных событий информационной безопасности, имеющих значительную вероятность компрометации бизнес-операции и создания угрозы информационной безопасности [4]. Инциденты ИБ могут обнаруживаться системами безопасности, например, различными мониторинговыми инструментами. Другим способом выявления может быть аудит ИБ, например, различные проверки системы на соответствие стандартам безопасности. Также об инциденте могут сообщить сотрудники организации, обнаружив его в своей рабочей среде. Инциденты ИБ могут негативно влиять на деятельность предприятия. Для поддержания высокого уровня информационной безопасности необходимо иметь возможность управлять инцидентами.

Управление инцидентами ИБ – это специализированная форма управления инцидентами, основной целью которой является разработка хорошо понятного и предсказуемого реагирования на опасные события и компьютерные вторжения [5, 6]. Для эффективного менеджмента инцидентов ИБ важно применять соответствующие процедуры на всех этапах [7, 8]: обнаружение инцидентов; оценка инцидентов; реагирование на инциденты; активизация защитных мер для предотвращения инцидентов. Регулярные проверки и тестирование процессов информационной системы помогут выявить потенциальные угрозы инцидентов и обеспечить информационную безопасность сети. Такой подход применим к системам и сетям, которые организация использует для управления и мониторинга своей информации, информационных процессов и информационных технологий [9].

Постановка задачи. Цель работы заключается в проектировании и разработке сервиса для автоматизации процессов управления и анализа инцидентов информационной безопасности в металлургической компании. Для достижения поставленной цели необходимо рассмотреть и проанализировать существующие информационные процессы и события, происходящие в информационных системах, с целью увеличения детализации и четкости совершаемых процедур. Кроме того, необходимо рассмотреть показатели эффективности

для управления инцидентами информационной безопасности для совершенствования процессов управления, а также анализ фреймворков и библиотек языка программирования, выбор наиболее подходящих из них. Выше перечисленное позволит в дальнейшем разработать программное приложение, с помощью которого можно отслеживать и анализировать инциденты информационной безопасности предприятия.

Методы исследования. На исследуемом металлургическом предприятии события ИБ могут поступать из различных источников: антивирус Kaspersky endpoint security; межсетевой экран Usergate NGFW; система защиты информации Dallas lock; стандартные средства MS Windows для администрирования. Администраторы информационных систем и систем защиты информации, а также ответственные за информационную безопасность предприятия лица отслеживают и анализируют все события, происходящие в системах. Управление инцидентами на данном предприятии включает в себя следующие процедуры:

1. *Обнаружение инцидента.* Все события, полученные от указанных источников, а также любые другие подозрительные активности обнаруживаются и регистрируются сотрудниками отдела ИБ.

2. *Анализ инцидента.* После обнаружения инцидента специалисты предприятия классифицируют его по типу и уровню критичности. По типу инциденты подразделяются: вредоносное программное обеспечение / уязвимости; несанкционированный доступ; социальная инженерия; отказ в обслуживании (DoS); нарушение внутренних политик/регламентов; утечка / потеря защищаемых данных. Уровень угрозы инцидента может быть критический или некритический.

3. *Реагирование на инцидент*. Некритические инциденты, как правило, решаются быстро. Например, в случае обнаружения антивирусом Kaspersky Endpoint Security на компьютере сотрудника вредоносного программного обеспечения, реагированием может быть следование рекомендациям антивируса. Если инцидент является критическим, то перед его ликвидацией необходимо локализовать затронутые информационные системы и/или персональные компьютеры. Локализация может включать: отключение от компьютерной сети предприятия задетых инцидентом систем и оборудования; остановку различных процессов или служб операционной системы; разграничение прав пользователей. Для ликвидации критического инцидента специалисты ИБ действуют в зависимости от нанесенного урона автоматизированному оборудованию. Например, в случае DoS атаки может быть перенастроена работа межсетевого экрана для фильтрации различных запросов.

4. *Восстановление данных*. В случае, если были задеты какие-либо данные, сотрудники руководствуются инструкциями внутреннего документа предприятия «Политика резервного копирования и восстановления данных». Для восстановления данных используется система Symantec Netbackup.

5. *Расследование инцидента и оценка последствий*. На этапе расследования проводится более глубокое изучение события с целью выявления его причин и механизмов распространения: анализ логов, детальное изучение атаки, исследование уязвимостей в системе, определение возможных участников или источников атаки. Последствия инцидента для предприятия могут отсутствовать, быть незначительными или значительными. По мнению специалистов ИБ, на исследуемом предприятии чаще всего фиксируются инциденты без последствий. Это может означать, что система защиты информации предприятия могла в автоматическом режиме устранить нежелательное событие. Инцидент может привести к минимальным нарушениям в работе ИС и автоматизированного оборудования предприятия, которые не оказали существенного влияния на основные бизнес-процессы, т.е. инцидент имел незначительные последствия для предприятия. Например, небольшая DoS атака не привела к серьезному сбою в оборудовании, либо незначительный объем потерянных данных был быстро восстановлен из резервных копий. Последствия инцидента считаются значительными, если он вызвал серьезные сбои в работе предприятия, привел к крупным

финансовым и/или репутационным потерям. Это может быть полное отключение производственных линий или большая утечка персональных данных.

Эффективность управления инцидентами ИБ оценивается количественными показателями, такими как [10]: общее число инцидентов; среднее фактическое время, затраченное на разрешение инцидента; число и доля инцидентов, обработанных в рамках согласованного времени реакции; средние затраты на полную обработку инцидента; доля инцидентов, закрытых без обращения к специализированным группам поддержки; число и доля инцидентов, разрешенных удаленно. Повышение эффективности процессов управления и анализа инцидентами требует специального программного обеспечения для автоматизации этих процессов и поддержки принятия решений по работе с инцидентами [11, 12]. Сервис анализа инцидентов – это приложение, обеспечивающее удобный доступ к произошедшим инцидентам ИБ и их аналитике. Данный сервис должен иметь функционал добавления, редактирования и удаления инцидентов, а также предоставлять пользователю различные аналитические и статистические данные и визуализировать их с помощью графиков и диаграмм [13-14]. Разработанный сервис позволит предприятию решать инциденты быстрее и снизить риск их появления в будущем. Для разработки сервиса были выбраны язык программирования Python и среда разработки Visual Studio Code.

Для расширения функционала созданного приложения использовались дополнительные фреймворки: tkinter – создание графического интерфейса приложения; PIL – загрузка и обработка изображений с целью дальнейшего размещения в окнах приложения; sqlite3– создание базы данных SQL для хранения информации об инцидентах; datetime – отображение даты и времени инцидентов; ttkthemes –изменение дизайна интерфейса, построенного на tkninter; matplotlib –построение различных графиков и диаграмм, анализирующих инциденты.

Обсуждение результатов. Алгоритм разработки сервиса для анализа инцидентов информационной безопасности состоит из следующих шагов:

Шаг 1. Загрузка фреймворков *tkinter*, *sqlite3*, *matplotlib* и сторонней темы библиотеки графического интерфейса *tkinter* для создания современного дизайна приложения.

Шаг 2. Создание и подключение базы данных SQL с помощью функции *create and update database ()* с использованием фреймворка *sqlite3*. Проверка корректности значений базы данных и вызов созданной функции.

Шаг 3. Создание классов *IncidentWindow*, *IncidentDetailWindow*, *MainWindow,* отражающих соответственно окна для добавления и редактирования инцидентов, для просмотра подробной информации об инциденте, главное окно для управления инцидентами и отражения аналитики.

Шаг 4. Создание функций *general_analysis, detailed_analysis* и *response_analysis* для формирования аналитических графиков и диаграмм на основе данных об инцидентах, загружаемых из базы данных SQL.

Шаг 5. Создание функций для реализации пользовательского интерфейса при обработке и анализе инцидентов: *toggle_view, hide_all, add_incident*, *edit_incident*, *delete_incident show_selected_incident_details, on_tree_select*.

Шаг 6. Создание процедуры открытия главного окна, т.е. класса *MainWindow*, и зацикливание данного класса.

Основной функционал приложения сосредоточен в главном окне, где пользователь выбирает требуемую аналитику: общий анализ инцидентов, детальный анализ инцидентов или анализ реагирования на инциденты и их последствия. Общая аналитика показывает суммарное число зафиксированных инцидентов, частоту их возникновения по месяцам и времени суток, распределение по статусам «в работе» и «закрыт». Графики визуально помогают оценить сколько инцидентов еще не завершено, какое количество инцидентов произошло по месяцам года, а также в какое время суток инциденты происходили чаще всего (рис.1).

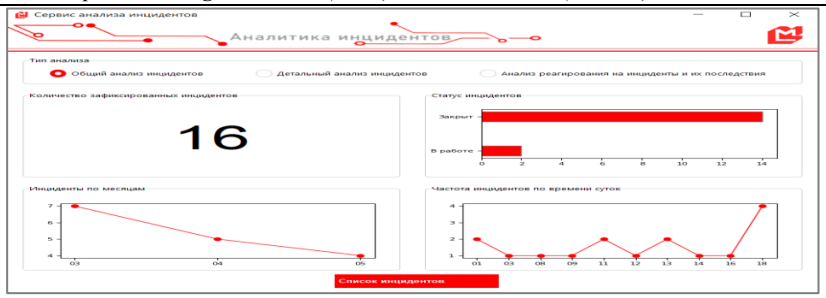

Рис. 1 - Главное окно программного сервиса анализа инцидентов
Fig. 1 - The main window of the incident analysis software service

Кнопка «Список инцидентов» на главном окне открывает другой раздел приложения с таблицей инцидентов ИБ за определенный временной период и командами управления: «Добавить инцидент», «Редактировать инцидент» и «Удалить инцидент». На рис. 2 представлено окно редактирования инцидента.

Рис. 2 - Окно редактирования инцидента
Fig. 2 - Incident editing window

Детальный анализ инцидентов отражает статистику по средствам обнаружения инцидентов, распределение их по степени критичности и по типам (рис.3). На вкладке «Анализ реагирования на инциденты и их последствия», размещены диаграммы «Распределение времени на решение инцидентов», «Количество инцидентов с различными последствиями», а также точечная диаграмма соотношения времени решения инцидента и его последствий.

Рис. 3 - Детальный анализ инцидентов
Fig. 3 - Detailed analysis of incidents

Такая визуализация может помочь в анализе временных затрат на обработку инцидентов и их последствий, а также оценить взаимосвязь уровня последствий инцидентов со временем их устранения.

Вывод. В условиях стремительного развития информационно-коммуникационных технологий информационная безопасность является одной из самых важных составляющих в построении бизнес-процессов. Растущие кибератаки представляют серьезную угрозу для организаций, а инциденты информационной безопасности происходят все чаще. Управление инцидентами информационной безопасности позволяет предприятиям эффективно обнаруживать новые атаки и защищать системы от потенциальных угроз. Анализ произошедших нежелательных и неожиданных событий позволяет повысить уровень эффективности систем управления информационной безопасностью предприятий.

Разработанный сервис способен улучшить управление инцидентами информационной безопасности на предприятии, а также дает возможность проанализировать уже произошедшие инциденты и, как следствие, минимизировать их последствия. Используя данную программную разработку, предприятие может повысить эффективность деятельности в области информационной безопасности.

Библиографический список:

1. Bandari V. Enterprise data security measures: a comparative review of effectiveness and risks across different industries and organization types. *International Journal of Business Intelligence and Big Data Analytics.* 2023; 6(1):1-11.
2. Patterson C.M., Nurse J.R.C., Franqueira V.N.L. Learning from cyber security incidents: A systematic review and future research agenda // Computers & Security. – 2023. – Т. 132. – С. 103309.
3. Alarcon J.C.M. Information security: A comprehensive approach to risk management in the digital world //SCT Proceedings in Interdisciplinary Insights and Innovations. – 2023. – Т. 1. – С. 84-84.
4. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. ГОСТ Р ИСО/МЭК ТО 18044-2007. Москва: Стандартинформ, 2009. URL:https://rosgosts.ru/file/gost/01/040/gost_r_iso! mek_to_18044-2007.pdf (20.05.2024).
5. Олейникова А.А., Золотарев В.В. Концепция управления информационной безопасностью на основе цикла непрерывного детектирования и реагирования на инциденты безопасности информации // Известия ЮФУ. Технические науки. 2023. № 5(235). С. 66-81. DOI: 10.18522/2311-3103-2023-5-66-81.
6. Трофимов Д.О., Шепелев М.С., Резниченко С.А. Организация реагирования на инциденты информационной безопасности // Вестник Дагестанского государственного технического университета. Технические науки. 2023. №4(50). С. 148-157. DOI: 10.21822/2073-6185-2023-50-4-148-157.
7. 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.
8. Солдатов Е.Ю., Селифанов В.В., Кувшинов М.А. Разработка системы контроля инцидентов информационной безопасности // Безопасность цифровых технологий. 2023. № 3(110). С. 54-66. DOI: 10.17212/2782-2230-2023-3-54-66.
9. Ehis A. T. Optimization of security information and event management (SIEM) infrastructures, and events correlation/regression analysis for optimal cyber security posture. Archives of Advanced Engineering Science. – 2023. – С. 1-10.
10. Рытов М.Ю., Голембиовская О.М., Кондрашова Е.В. Порядок оценки уровня эффективности системы непрерывного противодействия инцидентам информационной безопасности на объекте // Информация и безопасность. 2024. Т. 27. № 1. С. 135-142. DOI: 10.36622/1682-7813.2024.27.1.011.
11. Mouratidis H., Islam S., Santos-Olmo A., Sanchez L.E, Ismail M.U. Modelling language for cyber security incident handling for critical infrastructures.*Computers & Security*. 2023;128:103139. DOI: 10.1016/j.cose.2023.103139
12. Naseer H., Desouza K.C., Maynard S.B., Ahmad A. Enabling cybersecurity incident response agility through dynamic capabilities: the role of real-time analytics // European Journal of Information Systems. 2024. V. 33. No. 2. P. 200-220. DOI:10.1080/0960085X.2023.2257168.
13. Walter M., Heinrich R., Reussner R. Architecture-based attack path analysis for identifying potential security incidents. *European Conference on Software Architecture. Cham: Springer Nature Switzerland*. 2023; 37-53.
14. Kyriazoglou J. Improving Security Incident and Data Breach Responses // Information Security Incident and Data Breach Management: A Step-by-Step Approach. – Berkeley, CA : Apress, 2024. – С. 67-73.

References:

1. Bandari V. Enterprise data security measures: a comparative review of effectiveness and risks across different industries and organization types. *International Journal of Business Intelligence and Big Data Analytics.* 2023; 6(1):1-11.
2. Patterson C.M., Nurse J.R.C., Franqueira V.N.L. Learning from cyber security incidents: A systematic review and future research agenda. *Computers & Security*. 2023;132:103309.
3. Alarcon J.C.M. Information security: A comprehensive approach to risk management in the digital world. *SCT Proceedings in Interdisciplinary Insights and Innovations*. 2023;1:84-84.
4. Information technology. Methods and means of ensuring security. Information security incident management. GOST R ISO/IEC TO 18044-2007. Moscow: Standartinform, 2009. URL: https://rosgosts.ru/file/gost/01/040/gost_r_iso ! mek_to_18044-2007.pdf (accessed: 05/20/2024). (In Russ)
5. Oleinikova A.A., Zolotarev V.V. The concept of information security management based on a cycle of continuous detection and response to information security incidents. *Izvestiya SFU. Technical sciences*. 2023; 5(235):66-81. DOI: 10.18522/2311-3103-2023-5-66-81. (In Russ)

6. Trofimov D.O., Shepelev M.S., Reznichenko S.A. Organization of response to information security incidents. *Herald of the Daghestan State Technical University. Technical Sciences*. 2023;4(50):148-157. DOI: 10.21822/2073-6185-2023-50-4-148-157. (In Russ)
7. Basharina O.Yu., Butsenko E.V., Pokhomchikova E.O., Shilnikova I.S. Technology of corporate protection of personal data and confidential information. *Modern high-tech technologies*. 2024; 2:8-14. DOI: 10.17513/snt.39924. (In Russ)
8. Soldatov E.Yu., Selifanov V.V., Kuvshinov M.A. Development of an information security incident control system. *Security of digital technologies*. 2023;3(110):54-66. DOI:10.17212/2782-2230-2023-3-54-66.
9. Ehis A. T. Optimization of security information and event management (SIEM) infrastructures, and events correlation/regression analysis for optimal cyber security posture.*Archives of Advanced Engineering Science*. 2023;1-10.
10. Rytov M. Yu., Golembiovskaya O.M., Kondrashova E.V. The procedure for assessing the level of effectiveness of the system of continuous counteraction to information security incidents at the facility. *Information and Security.* 2024;27(1):135-142. DOI: 10.36622/1682-7813.2024.27.1.011. (In Russ)
11. Mouratidis H., Islam S., Santos-Olmo A., Sanchez L.E, Ismail M.U. Modelling language for cyber security incident handling for critical infrastructures.*Computers & Security*. 2023;128:103139. DOI: 10.1016/j.cose.2023.103139.
12. Naseer H., Desouza K.C., Maynard S.B., Ahmad A. Enabling cybersecurity incident response agility through dynamic capabilities: the role of real-time analytics. *European Journal of Information Systems.* 2024;33(2): 200-220. DOI:10.1080/0960085X.2023.2257168.
13. Walter M., Heinrich R., Reussner R. Architecture-based attack path analysis for identifying potential security incidents. *European Conference on Software Architecture. Cham: Springer Nature Switzerland*. 2023; 37-53.
14. Kyriazoglou J. Improving Security Incident and Data Breach Responses. *Information Security Incident and Data Breach Management: A Step-by-Step Approach. – Berkeley, CA : Apress*, 2024; 67-73.

Сведения об авторах:

Ольга Юрьевна Башарина, кандидат технических наук, доцент кафедры бизнес-информатики; basharinaolga@mail.ru

Елена Владимировна Буценко, кандидат экономических наук, доцент кафедры бизнес-информатики; evl@usue.ru

Артем Сергеевич Еремеев, студент, artemdog77@gmail.com

Information about authors:

Olga Yu. Basharina, Dr. Sci. (Eng.), Assoc. Prof.; basharinaolga@mail.ru

Elena V. Butsenko, Dr. Sci. (Econ.), Assoc. Prof.; evl@usue.ru

Artem S. Eremeev, Student; artemdog77@gmail.com

Конфликт интересов/Conflict of interest.

Авторы заявляют об отсутствии конфликта интересов/The authors declare no conflict of interest.

Поступила в редакцию/Received 19.12.2024.

Одобрена после рецензирования/ Reviced 16.02.2025.

Принята в печать/Accepted for publication 20.05.2025.