www.volsu.ru

CC BY

DOI: https://doi.org/10.15688/NBIT.jvolsu.2025.4.2

УДК 004.5:004.056
ББК 32.971.352

ФУНКЦИОНАЛЬНОЕ МОДЕЛИРОВАНИЕ ПРОЦЕССА ВЫЯВЛЕНИЯ АНОМАЛИЙ ПОВЕДЕНИЯ ПОЛЬЗОВАТЕЛЕЙ В КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Светлана Александровна Елизарова

Студент,
Волгоградский государственный университет
bit-211_114288@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Алексей Александрович Бабенко

Кандидат педагогических наук, доцент кафедры компьютерной безопасности,
Волгоградский государственный университет
babenko.aleksey@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. Построена функциональная модель процесса выявления аномалий поведения пользователей в корпоративных информационных системах. Определены и формализованы взаимосвязи между элементами процесса: входами, управлениями, механизмами и выходами. Выделены основные функциональные блоки модели. Детализирован блок выявления аномалий на подпроцессы анализа журналов событий, программного обеспечения, устройств и событий безопасности.

Ключевые слова: функциональное моделирование, IDEF0, анализ поведения пользователей, аномальное поведение, корпоративные информационные системы, внутренние угрозы, информационная безопасность.

Современные корпоративные информационные системы характеризуются высокой сложностью и распределенностью, что создает значительные сложности для обеспечения их безопасности [2; 5; 8]. Согласно статистике InfoWatch, долю утечек конфиденциальной информации, вызванных умышленными действиями внутреннего нарушителя, составляет 18,5 % [7]. Традиционные системы безопасности, ориентированные на внешние угрозы, часто оказываются неэффективными для современного обнаружения аномальной активности легитимных пользователей.

В этом контексте анализ поведения пользователей (User Behavior Analytics – UBA) становится критически важным компонентом комплексной системы защиты информации. Однако проектирование таких систем требует четкого понимания и формализации процесса выявления аномалий, что обусловливает актуальность применения методов функционального моделирования.

Методология IDEF0 (Integration Definition for Function Modeling) является международным стандартом функционального моделирования и широко используется для описания бизнес-процессов и организационных

© Елизарова С.А., Бабенко А.А., 2025

систем [9]. Ее применение для формализации процесса анализа поведения пользователей позволяет:

1) системно представить процесс выявления аномалий;

2) установить четкие взаимосвязи между компонентами системы;

3) идентифицировать требования к данным и ресурсам;

4) обеспечить основу для последующей разработки программного обеспечения.

Целью исследования является разработка функциональной модели процесса выявления аномалий поведения пользователей в корпоративных информационных системах с использованием методологии IDEF0.

Для достижения цели необходимо решить следующие задачи:

1. Определить контекст процесса выявления аномалий поведения пользователей.

2. Разработать декомпозицию процесса на функциональные блоки.

3. Установить состав и характеристики входных данных, управляющих воздействий, механизмов и результатов процесса.

4. Провести верификацию модели в ходе экспериментальных исследований.

Проблема противодействия внутренним угрозам активно исследуется в области информационной безопасности. Существуют различные подходы к анализу поведения пользователей, включая методы машинного обучения и статистического анализа [1; 3]. Однако многие из существующих решений фокусируются на алгоритмической составляющей, не уделяя достаточного внимания формализации и структурированию самого процесса детектирования аномалий как комплекса взаимосвязанных действий.

Методология IDEF0, в свою очередь, широко применяется для моделирования бизнес-процессов в различных предметных областях [4; 6], но ее использование для описания процессов в области UBA освещено в научной литературе недостаточно. Это определяет научную новизну представленного исследования, которая заключается в системном представлении процесса выявления аномалий поведения пользователей корпоративных информационных систем в виде иерархической функциональной модели, устанавливающей строгие взаимосвязи между всеми компонентами процесса.

Исследование проводилось с использованием методологии IDEF0, которая предусматривает построение иерархии функциональных моделей, начиная с контекстной диаграммы общего уровня (A0) с последующей детализацией на декомпозиционных диаграммах.

Контекстная диаграмма процесса выявления аномалий поведения пользователей представлена на рисунке 1. Модель идентифицирована как «Выявление аномалий поведения пользователей в корпоративных информационных системах». На вход процесса подаются данные о пользовательской активности, управляющими воздействиями являются нормативно-правовые документы и политики безопасности, механизмами – программно-аппаратный комплекс и персонал, а выходом – отчеты об аномалиях и скорректированные политики.

В результате декомпозиции контекстной диаграммы была разработана диаграмма первого уровня (см. рис. 2), включающая четыре функциональных блока:

– блок «Обработка полученных данных» осуществляет прием и первичную обработку

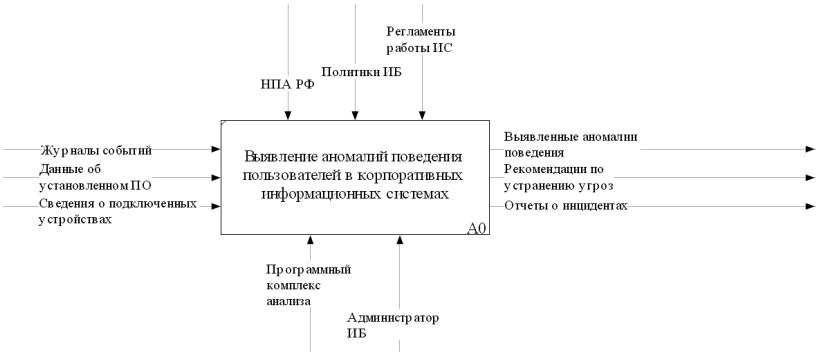


Рис. 1. Контекстная диаграмма процесса выявления аномалий

данных с клиентских рабочих станций, включает операции подключения к источникам данных, передачи данных на сервер анализа и проверки целостности полученной информации;

– блок «Корректировка данных» выполняет сбор и формирование эталонных значений поведения пользователей, осуществляет создание базовых профилей нормального поведения, установление допустимых диапазонов параметров и формирование белых списков ПО и устройств;

– блок «Настройка политики безопасности» обеспечивает конфигурирование критериев детектирования аномалий, включает определение пороговых значений для различных типов событий, настройку правил корреляции событий и установку параметров чувствительности обнаружения;

– блок «Выявление аномалий» реализует непосредственно процесс анализа и детектирования отклонений.

Между функциональными блоками установлены следующие потоки данных:

1) A1 – A2, A4: обработанные данные пользовательской активности передаются как для формирования эталонов, так и для непосредственного анализа аномалий;

2) A2 – A3: результаты корректировки данных (эталонные модели поведения и скорректированные параметры мониторинга) используются для настройки политик безопасности;

3) A3 – A4: настроенные критерии детектирования и параметры политик направляются в блок детектирования аномалий для проведения анализа.

Такая организация потоков обеспечивает последовательную обработку информации и возможность адаптации системы к изменяющимся условиям работы корпоративной информационной системы.

Для верификации разработанной функциональной модели был реализован программный комплекс, архитектура которого соответствует установленным в модели функциональным блокам и потокам данных.

Экспериментальные исследования включали серию тестовых сценариев, имитирующих различные типы аномального поведения:

1. Неудачные попытки входа в систему – зафиксировано 2 попытки неудачного входа, сформирован подробный отчет об ошибках.

2. Несанкционированное изменение прав пользователя – обнаружено изменение прав учетной записи User2 на «Администратор», сформирован и отправлен отчет на серверную составляющую.

Результаты экспериментов подтвердили корректность организации потоков данных между функциональными блоками и практическую применимость разработанной модели для построения систем анализа поведения пользователей.

Разработанная функциональная модель процесса выявления аномалий поведения пользователей в корпоративных информационных системах представляет собой системное описание данного процесса с установлением четких взаимосвязей между его компонентами и организацией потоков данных.

Основные научные и практические результаты работы:

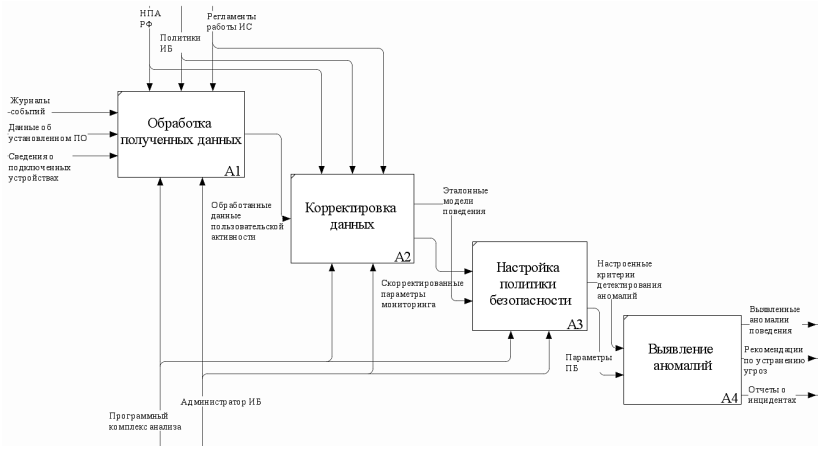


Рис. 2. Декомпозиция контекстной диаграммы процесса выявления аномалий

1. Построена контекстная диаграмма процесса выявления аномалий и выполнена ее декомпозиция на четыре функциональных блока.

2. Установлены и формализованы потоки данных между функциональными блоками, обеспечивающие последовательную обработку информации.

3. Осуществлена экспериментальная верификация модели, подтвердившая корректность организации потоков данных и практическую применимость модели.

Разработанная модель может служить основой для проектирования корпоративных систем безопасности, ориентированных на противодействие внутренним угрозам, а также для дальнейших исследований в области анализа поведения пользователей.

СПИСОК ЛИТЕРАТУРЫ

1. Гостев, И. М. Алгоритмы обнаружения аномалий в поведении пользователей на основе анализа временных рядов / И. М. Гостев // Известия ЮФУ. Технические науки. – 2022. – Т. 65, № 4. – С. 112–125.

2. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности : ГОСТ Р ИСО/МЭК 27001-2022. – Введ. 2023-01-01. – М. : Стандартинформ, 2022. – 40 с.

3. Леонова, Е. А. Современные подходы к анализу поведения пользователей в корпоративных информационных системах / Е. А. Леонова // Безопасность информационных технологий. – 2023. – Т. 30, № 2. – С. 45–56.

4. Марков, А. С. Функциональное моделирование бизнес-процессов с использованием методологии IDEF0 / А. С. Марков, Д. М. Цыганов // Информационные технологии. – 2020. – Т. 26, № 4. – С. 245–252.

5. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» // Бюллетень нормативных актов федеральных органов исполнительной власти. – 2013. – № 35.

6. Смирнов, А. В. Применение стандарта IDEF0 для проектирования информационных систем управления предприятием / А. В. Смирнов // Проблемы управления. – 2021. – № 3. – С. 56–64.

7. Утечки информации в мире и России за первое полугодие 2024 года // InfoWatch. – URL: https://www.infowatch.ru/sites/default/files/analytics/files/utechki-informatsii-v-mire-i-rossii-za-pervoye-polugodiye-dve-tysyachi-dvadtsat-chetvertogo-goda.pdf

8. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ред. от 24.02.2024) // Собрание законодательства РФ. – 2006. – № 31, ч. 1. – Ст. 3448.

9. Kim, J. A comprehensive approach to insider threat detection using user behavior analytics / J. Kim, S. Park // Computers & Security. – 2022. – Vol. 118. – P. 102742. – DOI: 10.1016/j.cose.2022.102742

REFERENCES

1. Gostev I.M. Algoritmy obnaruzheniya anomaliy v povedenii polzovateley na osnove analiza vremennyh ryadov [Algorithms for Detecting Anomalies in User Behavior Based on Time Series Analysis]. *Izvestiya YuFU. Tekhnicheskiye nauki* [Izvestiya SFedU. Engineering Sciences], 2022, vol. 65, no. 4, pp. 112-125.

2. Informatsionnaya tehnologiya. Metody i sredstva obespecheniya bezopasnosti. Sistemy menedzhmenta informatsionnoy bezopasnosti: GOST R ISO/MEC 27001-2022 [Information Technology. Security Techniques. Information Security Management Systems. GOST R ISO/IEC 27001-2022]. Moscow, Standartinform Publ., 2022. 40 p.

3. Leonova E.A. Sovremennye podhody k analizu povedeniya polzovatelei v korporativnyh informatsionnyh sistemah [Modern Approaches to User Behavior Analysis in Corporate Information Systems]. *Bezopasnost informatsionnyh tekhnologiy* [Information Technology Security], 2023, vol. 30, no. 2, pp. 45-56.

4. Markov A.S., Tsyganov D.M. Funktsionalnoye modelirovaniye biznes-protsessov s ispolzovaniem metodologii IDEF0 [Functional Modeling of Business Processes Using the IDEF0 Methodology]. *Informatsionnye tehnologii* [Information Technologies], 2020, vol. 26, no. 4, pp. 245-252.

5. Prikaz FSTEK Rossii ot 11.02.2013 № 17 «Ob utverzhdenii Trebovaniy o zashchite informatsii, ne sostavlyayushchey gosudarstvennuyu tainu, soderzhashcheysya v gosudarstvennyh informatsionnyh sistemakh» [Order of the FSTEC of Russia No. 17 of February 11, 2013 "On Approval of the Requirements for the Protection of Information Not Constituting a State Secret Contained in State Information Systems"]. *Byulleten normativnyh aktov federalnyh organov ispolnitelnoy vlasti* [Bulletin of Regulatory Acts of Federal Executive Bodies], 2013, no. 35.

6. Smirnov A.V. Primeneniye standarta IDEF0 dlya proektirovaniya informatsionnyh sistem upravleniya predpriyatiyem [Application of the IDEF0 Standard for Designing Enterprise Management Information Systems]. *Problemy upravleniya* [Control Sciences], 2021, no. 3, pp. 56-64.

7. Utechki informatsii v mire i Rossii za pervoe polugodie 2024 goda [Information Leaks in the World and Russia for the First Half of 2024]. *InfoWatch.* URL: https://www.infowatch.ru/sites/default/files/analytics/files/utechki-informatsii-v-mire-i-rossii-za-pervoye-polugodiye-dve-tysyachi-dvadtsat-chetvertogo-goda.pdf

8. Federalny zakon ot 27.07.2006 № 149-FZ «Ob informatsii, informatsionnyh tekhnologiyah i o zashchite informatsii» (red. ot 24.02.2024) [Federal Law No. 149-FZ of July 27, 2006 "On Information, Information Technologies and Information Protection" (As Amended on February 24, 2024)]. *Sobraniye zakonodatelstva RF* [Collection of Legislation of the Russian Federation], 2006, no. 31, pt. 1, art. 3448.

9. Kim J., Park S. A Comprehensive Approach to Insider Threat Detection Using User Behavior Analytics. *Computers & Security*, 2022, vol. 118, p. 102742. DOI: 10.1016/j.cose.2022.102742

FUNCTIONAL MODELING OF THE PROCESS OF DETECTING USER BEHAVIOR ANOMALIES IN CORPORATE INFORMATION SYSTEMS

Svetlana A. Elizarova

Student,
Volgograd State University
bit-211_114288@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Aleksey A. Babenko

Candidate of Sciences (Pedagogy), Associate Professor, Department of Computer Security,
Volgograd State University
babenko.aleksey@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Abstract. This study addresses the growing challenge of internal threats within complex corporate information systems by developing a functional model for detecting user behavior anomalies. Traditional security measures often prove insufficient against insider risks, necessitating structured approaches like User Behavior Analytics (UBA). The research employs the IDEF0 methodology to systematically formalize the detection process, establishing clear relationships between its core components: inputs (user activity data), controls (security policies), mechanisms (software/hardware and personnel), and outputs (anomaly reports and updated policies). The constructed model is hierarchically decomposed, starting from a contextual diagram (A0) and detailing into four primary functional blocks: Data Processing, Data Adjustment (creating behavioral baselines), Security Policy Configuration, and Anomaly Detection. Data flows between these blocks are formally defined, ensuring sequential information processing and system adaptability. The anomaly detection block is further detailed into sub-processes analyzing event logs, software, devices, and security events. The model's practical validity was verified through a prototype implementation and experimental testing using scenarios simulating unauthorized access attempts and privilege changes. Results confirmed the correctness of the designed data flows and the model's applicability for building real-world user behavior analysis systems. The developed functional model provides a structured foundation for designing corporate security systems against internal threats and for further research in user behavior analytics.

Key words: functional modeling, IDEF0, user behavior analysis, anomalous behavior, corporate information systems, internal threats, information security.