УДК 004.056

И.А. Огнев

Вопросы математической интерпретации процесса аудита информационной безопасности с применением сетей Петри

Сформирована математическая модель процесса аудита информационной безопасности, которая основана на применении временных сетей Петри для описания состояний процесса аудита информационной безопасности и изменений состояний процесса аудита. Описаны изменения состояний процесса аудита информационной безопасности, которые заключаются в выявлении свидетельств аудита, анализе свидетельств аудита и выявлении нарушений в реализации мер по защите информации, анализе нарушений в реализации мер по защите информации и выработке замечаний, которые должны быть сформированы как основной результат процесса аудита информационной безопасности. Разработаны эталонные показатели сети Петри по составу компонентов и связям между ними для применения в процессе оценки полноты и правильности структуры реальных процессов аудита информационной безопасности. Сформированная математическая модель как часть процесса оценки эффективности процесса аудита информационной безопасности призвана в первую очередь отвечать на вопрос достаточности компонентов аудита в исследуемой организации. Помимо этого, сформированная математическая модель процесса аудита информационной безопасности является основой для имитационного моделирования процесса аудита в целях реализации оценки вероятности достижения целей аудита за заданный промежуток времени проведения аудита и определенный набор обнаруженных свидетельств аудита.

Ключевые слова: графы, аудит, аудит информационной безопасности, сеть Петри, доверие, оценка доверия, информационная безопасность, кибербезопасность.

DOI: 10.21293/1818-0442-2024-27-2-15-20

Формирование устойчивой системы обеспечения информационной безопасности основано на ряде процессов, которые применяются в системах контроля информационной безопасности [1, 2]:

1. Контроль внедрения мер защиты информации и регламентов по их внедрению.

2. Контроль за полнотой реализации мер защиты информации и правильностью их исполнения согласно требованиям регуляторов, внутренних нормативно-правовых актов или договорных обязательств по защите информации.

Контроль реализованных мер по защите информации на сегодняшний день реализован в виде процессов аудита различной направленности [3, 4]:

1. Нормативный – аудит на соответствие требованиям регуляторов или договорным обязательствам.

2. Экспертный (compliance) – аудит на соответствие лучшим практикам (стандартам) в области информационной безопасности.

3. Технический (оценка защищенности, penetration test) – аудит с применением различных средств анализа защищенности и специализированных программных комплексов и утилит, направленный на практическую реализацию недопустимых событий в информационной системе организации заказчика.

В рамках информационного обмена встает вопрос достаточности принятых мер по защите информации контрагента для нейтрализации угроз безопасности информации типа supply chain [5] (атаки на цепочки поставок) или нейтрализации угроз, связанных с компьютерными атаками со стороны доверенных контрагентов, которые субъект информационного обмена не принял во внимание. Данный вопрос важен для уверенности в том, что раскрытие своей информационной системы для третьего лица не приведет к реализации недопустимых рисков или рисков, связанных с информационным обменом и неучтенных при построении системы защиты информации.

Для реализации возможности подтверждения факта добросовестного и эффективного подхода к реализации системы защиты информации и контроля системы защиты информации создается методика оценки доверия к аудиту информационной безопасности, которая включает в себя две основные оценки – зрелости и эффективности процесса аудита. В рамках данной статьи будут рассмотрены вопросы оценки эффективности процесса аудита информационной безопасности.

Создаваемая методика оценки доверия к аудиту информационной безопасности является частью технологии оценки уровня доверия к субъекту информационного обмена [6]. Технология оценки уровня доверия включается в себя оценку ряда процессов информационной безопасности, одним из которых является аудит информационной безопасности.

Для оценки эффективности процесса аудита информационной безопасности предлагается анализ двух составляющих процесса аудита:

1. Анализ достаточности состава компонентов процесса аудита.

2. Анализ вероятности достижения поставленных целей аудита в условиях ограничений по времени и ресурсам.

Для реализации оценки эффективности процесса аудита информационной безопасности предлагается использование сетей Петри для визуализации процесса аудита в целях анализа достаточности состава компонентов процесса аудита, а также в целях построения имитационных моделей процесса аудита информационной безопасности для анализа вероятности достижения целей аудита.

Применение сетей Петри распространено для формирования имитационных моделей различных процессов управления или контроля, например процессов обслуживания и ремонта сложных технических систем [7], а также широко применяется для проведения анализа производственных процессов, например организационных процессов производства или процессов сборочного производства [8, 9]. Поэтому было принято решение применить сети Петри в области информационной безопасности для исследования процессов аудита информационной безопасности.

Целью настоящего исследования является формирование математического аппарата сетей Петри для визуализации процесса аудита информационной безопасности.

Для достижения цели были решены задачи математического описания процесса аудита информационной безопасности, описания сети Петри процесса аудита информационной безопасности, а также описание эталонных значений графа в сети Петри процесса аудита.

Описание процесса аудита информационной безопасности

Основная цель процесса аудита информационной безопасности – исследование системы защиты информации целевой организации и выявление несоответствий реализованных мер по защите информации требованиям по обеспечению безопасности информации [10].

Соответственно, в качестве выходных данных процесса аудита информационной безопасности должен появиться набор замечаний Z:

$$Z = \{z\}. \quad (1)$$

В процессе проведения аудита информационной безопасности экспертная комиссия анализирует ряд свидетельств аудита C, связанных с каждой мерой защиты информации:

$$C = \{c\}. \quad (2)$$

Замечания выявляются на основе анализа свидетельств аудита путем выявления нарушений в реализации мер по защите информации N:

$$N = \{n\}. \quad (3)$$

$$z = \begin{cases} 0, \exists c \wedge \nexists n; \\ 1. \end{cases} \quad (4)$$

Если существует свидетельство аудита и не существует нарушений, то считаем, что замечаний нет ($z = 0$). Во всех остальных случаях считаем, что замечание существует ($z = 1$) и должно быть включено в итоговый отчет по аудиту.

Для реализации сбора и анализа свидетельств аудита необходимо выполнить ряд действий, из которых состоит процесс аудита информационной безопасности (рис. 1).

1. Этап подготовки [11; 12]:

a) формирование команды аудита;

b) предварительное обследование объекта;

c) формирование программы аудита.

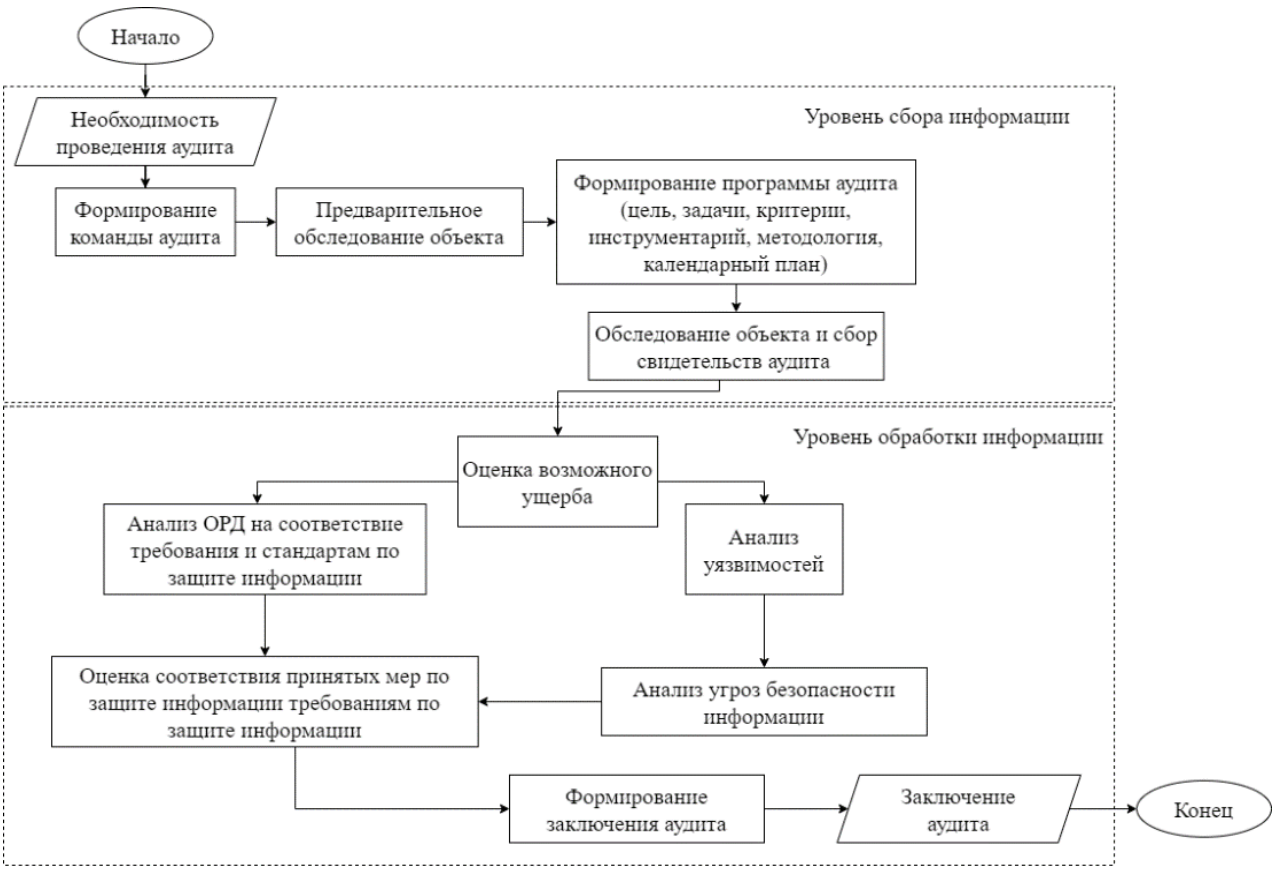

Рис. 1. Порядок действий при проведении аудита информационной безопасности

2. Этап проведения аудита [11, 12]:

a) сбор свидетельств аудита [13];

b) оценка возможного ущерба [14];

c) анализ уязвимостей [13, 15];

d) анализ угроз [13, 15];

e) анализ ОРД на соответствие требованиям и стандартам по защите информации [10];

f) анализ мер по защите информации на соответствие требованиям по защите информации [10, 16];

3. Этап отчетности [11, 12]:

a) формирование отчета аудита [17, 18].

Каждый из вышеперечисленных этапов является компонентой процесса аудита информационной безопасности. Соответственно процесс аудита можно описать как совокупность компонент K:

$$K = \{k\}. \quad (5)$$

Приведенный алгоритм процесса аудита информационной безопасности (рис. 1) является идеальным (эталонным), так как базируется на ГОСТах [11, 12], регламентирующих процесс аудита, а также на научных исследованиях, использующих приведенный алгоритм. Процессы аудита информационной безопасности в реальной жизни могут отличаться от приведенного эталонного, т.е. они могут быть неидеальными (неэталонными).

Таким образом, сформировав эталонный алгоритм проведения процесса аудита информационной безопасности, можно построить эталонную сеть Петри процесса аудита информационной безопасности, которая будет являться источником эталонных показателей для оценки достаточности состава компонентов процесса аудита. Также эталонная сеть Петри позволит построить эталонную имитационную модель процесса аудита информационной безопасности, которая будет применяться для оценки эффективности процесса аудита информационной безопасности.

Формирование сети Петри процесса аудита информационной безопасности

Основные характеристики процесса аудита информационной безопасности, на которые предстоит обратить внимание в процессе оценки эффективности:

1. Структурная полнота процесса аудита информационной безопасности – наличие всех компонентов процесса аудита.

2. Требуемое время для выполнения операций в каждом компоненте процесса аудита.

3. Количество выявленных свидетельств доверия.

4. Количество выявленных замечаний в результате процесса аудита.

На основе указанных характеристик необходимо ответить на два основных вопроса, касающихся эффективности процесса аудита информационной безопасности:

1. Содержится ли в процессе аудита полный набор компонент аудита?

2. Какова вероятность достижения целей аудита за выделенный промежуток времени и за определенное количество обнаруженных свидетельств аудита?

Соответственно, каждый компонент свидетельствует об определенном состоянии процесса аудита. Также каждый компонент аудита характеризуется определенными временными затратами на выполнение внутренних операций.

Таким образом, процесс аудита можно описать графом (временной сетью Петри) G [7–9]:

$$G = \langle K, S_k, T_k \rangle, \quad (6)$$

где K – набор компонент процесса аудита, S_k – набор отношений между компонентами аудита, T_k – время, на протяжении которого процесс находится на компоненте:

$$T_k = \{t_k\}. \quad (7)$$

Компоненты процесса аудита, относящиеся к этапу выполнения процесса аудита, можно описать кортежем (последовательностью)

$$k = \langle c, n, t_k \rangle. \quad (8)$$

А компоненты процесса аудита, относящиеся к этапу отчетности, можно описать кортежем

$$k = \langle z, t_k \rangle. \quad (9)$$

Компоненты этапа подготовки описываются кортежем

$$k = \langle t_k \rangle. \quad (10)$$

Схематично сеть Петри на основе эталонного процесса аудита информационной безопасности (см. рис. 1) будет выглядеть как представлено на рис. 2. Примем данную сеть Петри за эталонную, так как она имеет полный набор компонент и правильный набор связей между компонентами.

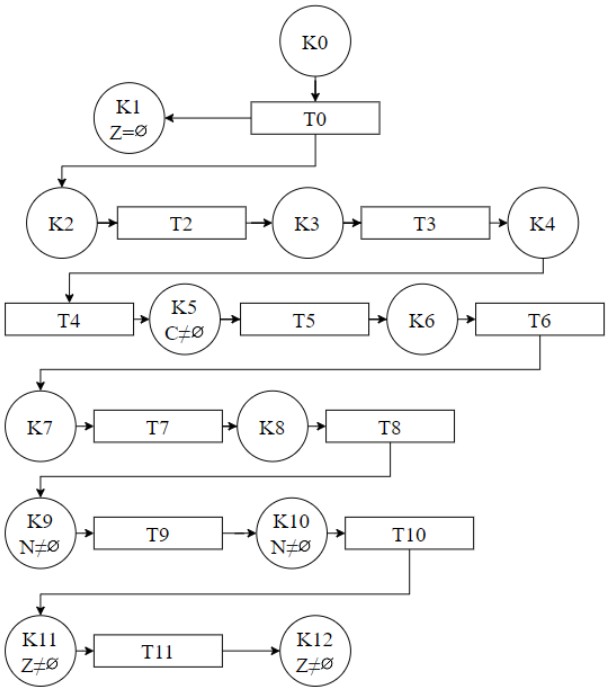

Рис. 2. Эталонная сеть Петри процесса аудита информационной безопасности

Сформированная эталонная сеть Петри позволяет решать часть задач в рамках методики оценки

эффективности процесса аудита информационной безопасности:

1. Оценить полноту компонентов процесса аудита изучаемой организации и правильность связей между ними.

2. Построить имитационную модель процесса аудита информационной безопасности для оценки вероятности достижения целей аудита в полной мере.

Эталонные значения сети Петри процесса аудита информационной безопасности

Опираясь на основной базовый стандарт по проведению процедур аудита информационной безопасности – ISO 19011:2018 [11], была построена сеть Петри (см. рис. 2). Принимая данную сеть Петри аудита информационной безопасности за эталонную, сформируем перечень обязательных эталонных компонентов и их связей.

$$K_{эт} = \{k_0 \ldots k_{12}\}, \quad (11)$$

где $K_{эт}$ – эталонные компоненты процесса аудита:

– k_0 – инициация процесса аудита;
– k_1 – отсутствие необходимости в аудите процесса аудита;
– k_2 – создание программы аудита;
– k_3 – предварительное обследование объекта;
– k_4 – формирование программы аудита;
– k_5 – сбор свидетельств аудита;
– k_6 – оценка возможного ущерба;
– k_7 – анализ уязвимостей;
– k_8 – анализ угроз безопасности информации;
– k_9 – анализ ОРД в процессе аудита;
– k_{10} – анализ мер по защите информации;
– k_{11} – формирование замечаний по результатам анализа мер по защите информации и ОРД;
– k_{12} – формирование отчета о проведении аудита.

Аналогично перечню эталонных компонент аудита сформированный эталонный набор связей между компонентами аудита S_k будет выглядеть следующим образом:

$$S_k \subseteq s_0 = \{k_0, k_1\}, s_1 = \{k_0, k_2\}, \ldots s_{11} = \{k_{11}, k_{12}\}. \quad (12)$$

Здесь связь s_0 обозначает связь между компонентами k_0 и k_1, связь s_1 – связь между компонентами k_0 и k_2, а связи $s_2 \ldots s_{11}$ аналогичны по смыслу связи s_0. Таким образом, получаются преимущественно последовательные связи между компонентами аудита практически без ветвлений и циклов.

Далее оценку достаточности структуры реального процесса аудита информационной безопасности можно проводить путем сравнения графов процесса аудита изучаемой организации и эталонного графа аудита.

Пример имитационной модели процесса аудита информационной безопасности

Согласно рис. 2, была сформирована имитационная модель процесса аудита информационной безопасности в виде системы массового обслуживания (рис. 3). Модель была построена с помощью среды имитационного моделирования AnyLogic.

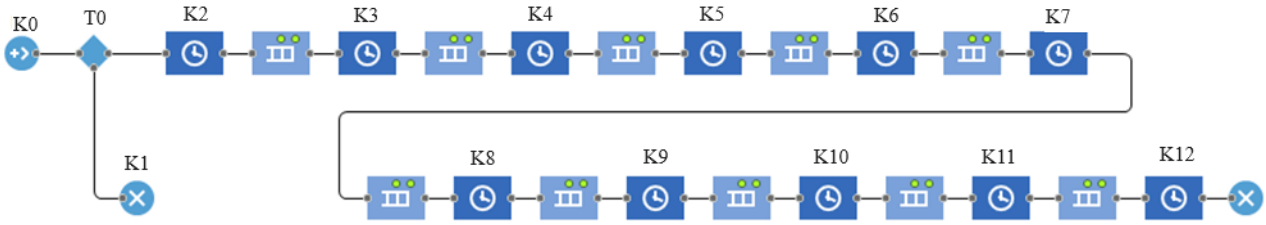

Рис. 3. Пример имитационной модели процесса аудита информационной безопасности

Для постановки экспериментов по оценке эффективности процесса аудита информационной безопасности необходимо использовать конкретные данные по временным затратам, количеству свидетельств аудита и замечаний на каждый компонент аудита ((8)–(10)).

При этом использование инструмента имитационного моделирования позволяет довольно быстро реализовывать эксперименты. Например, при условии, что аудит информационной безопасности должен занять 20 рабочих дней [19] (суммарное время для компонент $k_5 – k_{12}$), время одного прогона модели занимает 1,85 с при использовании максимального виртуального времени.

Заключение

В рамках настоящего исследования была сформирована математическая модель процесса аудита информационной безопасности в виде графа. Математическая модель основана на временных сетях Петри. Построена эталонная сеть Петри на базе стандарта ISO 19011:2018, основанных на нем других ГОСТах и научных публикациях. Также выделены эталонные компоненты и связи компонентов процесса аудита информационной безопасности.

Построенная сеть Петри процесса аудита информационной безопасности позволяет решить одну из двух задач оценки эффективности процесса аудита информационной безопасности – оценка полноты и правильности состава компонент процесса аудита информационной безопасности и связей между этими компонентами. Вторая задача оценки эффективности процесса аудита информационной безопасности – оценка вероятности реализации целей аудита за отведенный промежуток времени и количество свидетельств аудита. Данная задача будет решаться инструментами имитационного моделирования, которые в основе своей будут использовать выведенную математическую модель процесса аудита информационной безопасности.

Данная работа выполнена при финансовой поддержке Фонда поддержки проектов Национальной технологической инициативы (НТИ) в рамках реализации Программы Центра компетенций НТИ «Технологии доверенного взаимодействия» (договор от 14 декабря 2021 г. № 70-2021-00246).

Литература

1. Al-Fatlawi Q.A. Accounting Information Security and IT Governance Under COBIT 5 Framework: A Case Study / Q.A. Al-Fatlawi, D.S. Al Farttoosi, A.H. Almagtome // Webology. – 2021. – Vol. 18, No. Special Iss. 02. – P. 294–310.

2. Defining organisational information security culture—Perspectives from academia and industry / A. Da Veiga, L.V. Astakhova, A. Botha, M. Herselman // Computers & Security. – 2020. – Vol. 92. – P. 101713.

3. Макаренко С.И. Аудит информационной безопасности: основные этапы, концептуальные основы, классификация мероприятий // Системы управления, связи и безопасности. – 2018. – № 1. – С. 1–29.

4. Create your own MUSE: A method for updating security level evaluation instruments / M. Seeba, A.-A.O. Affia, S. Mäses, R. Matulevičius // Computer Standards & Interfaces. – 2024. – No. 87. – P. 103776.

5. Parker S. Cybersecurity in process control, operations, and supply chain / S. Parker, Z. Wu, P.D. Christofides // Computers & Chemical Engineering. – 2023. – No. 171. – P. 108169.

6. Технологии доверенного взаимодействия в экосистеме Национальной технологической инициативы / А.А. Шелупанов, Д.С. Брагин, А.А. Конев, Р.А. Пермяков // Современное образование: интеграция образования, науки, бизнеса и власти. – Томск: ТУСУР, 2022. – С. 15–20.

7. Орлов С.П. Имитационные модели на сетях Петри для анализа процессов обслуживания и ремонта сложных технических систем / С.П. Орлов, С.В. Сусарев // Вестник Самар. гос. тех. ун-та. Сер.: Технические науки. – 2023. – Т. 30, № 4. – С. 49–75.

8. Наумов В.Н. Анализ применимости процессного подхода, основанного на графовой аналитике, к исследованию организационных систем / В.Н. Наумов, М.В. Буйневич, А.Д. Стрелец // Вестник Санкт-Петерб. ун-та ГПС МЧС России. – 2022. – № 3. – С. 89–101.

9. Сочнев А.Н. Оптимизация сборочного производства на основе имитации сетей Петри // Вестник МГТУ им. Н.Э. Баумана. Сер.: Приборостроение. – 2021. – Т. 135, № 2. – С. 133–146.

10. Ситская А.В. Вопросы аудита информационной безопасности / А.В. Ситская, В.В. Селифанов, П.А. Звягинцева // Безопасность цифровых технологий. – 2023. – Т. 110, № 3. – С. 67–82.

11. ISO 19011:2018 – Guidelines for auditing management systems [Электронный ресурс]. – Режим доступа: https://pqm-online.com/assets/files/pubs/translations/std/iso-19011-2018-(rus).pdf, свободный (дата обращения: 20.05.2024).

12. ГОСТ Р ИСО/МЭК 27007–2014. Информационная технология (ИТ). Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности [Электронный ресурс]. – Режим доступа: https://internet-law.ru/gosts/gost/57828/, свободный (дата обращения: 19.05.2024).

13. Senkiv D.A. Audit as a Means of Ensuring Information Security of Web Applications and Used Computer Systems // American Scientific Journal. – 2020. – Vol. 40, No. 2. – P. 54–57.

14. Методический документ «Методика оценки угроз безопасности информации» (утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г.) [Электронный ресурс]. – Режим доступа: https://www.garant.ru/products/ipo/prime/doc/400325044/, свободный (дата обращения: 20.05.2024).

15. Kitsios F. The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector / F. Kitsios, E. Chatzidimitriou, M. Kamariotou // Sustainability. – 2023. – No. 15. – P. 5828.

16. Денисенко В.В. Аудит информационной безопасности организаций: методы и преимущества / В.В. Денисенко, А.М. Гончаров, И.П. Маслов // Наукосфера. – 2023. – № 11–2. – С. 135–140.

17. Information security audit for a manufacturing company / S.V. Shirokova, O.V. Rostova, M.V. Bolsunovskaya, L.A. Dmitrieva, T.O. Almataev // Information and control systems. – 2023. – Vol. 122, No. 1. – P. 41–50.

18. Сиротский А.А. Формализованная модель аудита информационной безопасности организации на предмет соответствия требованиям стандартов / А.А. Сиротский, С.А. Резниченко // Безопасность информационных технологий. – 2021. – Т. 28, № 3. – С. 103–117.

19. Постановление Правительства РФ от 17 февраля 2018 г. № 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» [Электронный ресурс]. – Режим доступа: https://base.garant.ru/71883452/, свободный (дата обращения: 21.05.2024)

Огнев Игорь Александрович
Аспирант, ассистент каф. защиты информации (ЗИ)
Новосибирского государственного технического ун-та (НГТУ)
К. Маркса пр-т, 20, г. Новосибирск, Россия, 630073
ORCID: 0000-0003-3884-7170
Тел.: +7-999-465-77-31
Эл. почта: i.ognev.2016@corp.nstu.ru

Ognev I.A.

Issues of mathematical interpretation of the information security audit process using Petri nets

This article presents the way to compose a mathematical model of the information security audit process. The model is based on the use of temporary Petri nets to describe the states of the information security audit process and the changes in the states of the audit process. The changes in the state of the information security audit process are described, that consist in identifying audit evidence, analyzing audit evidence and identifying violations in the implementation of information security measures, analyzing violations in the implementation of information security measures and developing comments that should be formed as the main result of the information security audit process. The reference indicators of the Petri net on the composition of components and connections between them have been developed to assess the completeness and correctness of the structure of real information security audit processes. The mathematical model obtained when assessing the efficiency of the information security audit process is primarily designed to answer the question of the sufficiency of audit components in the

organization under study. In addition, the obtained mathematical model of the information security audit process represents the basis for simulation modeling of the audit process in order to assess the probability of achieving audit goals for a given period of audit time and a certain set of detected audit evidence.
Keywords: graphs, audit, information security audit, Petri net, trust, trust assessment, information security, cybersecurity.
DOI: 10.21293/1818-0442-2024-27-2-15-20

References

1. Al-Fatlawi Q.A., Al Farttoosi D.S., Almagtome A.H. Accounting Information Security and IT Governance Under COBIT 5 Framework: A Case Study. *Webology*, 2021, vol. 18, no. Special Iss. 2, pp. 294–310.

2. Da Veiga A., Astakhova L.V., Botha A., Herselman M. Defining organisational information security culture-Perspectives from academia and industry. *Computers & Security*, 2020, vol. 92, p. 101713.

3. Makarenko S.I. [Information security audit: main stages, conceptual framework, classification of activities]. *Control, Communication and Security Systems*, 2018, no. 1, pp. 1–29 (in Russ.)

4. Seeba M., Affia A.O., Mäses S., Matulevičius R. Create your own MUSE: A method for updating security level evaluation instruments. *Computer Standards & Interfaces*, 2024, no. 87, p. 103776.

5. Parker S., Wu Z., Christofides P.D. Cybersecurity in process control, operations, and supply chain. *Computers & Chemical Engineering*, 2023, no. 171, p. 108169.

6. Shelupanov A.A., Bragin D.S., Konev A.A., Per-myakov R.A. [Technologies of trusted interaction in the ecosystem of the National Technology Initiative]. *Sovremennoe obrazovanie: integratsiya obrazovaniya, nauki, biznesa i vlasti* [Modern education: integration of education, science, business and government]. Tomsk, 2022, pp. 15–20 (in Russ.)

7. Orlov S.P., Susarev, S.V. [Simulation models on Petri nets for analyzing maintenance and repair processes of complex technical systems]. *Vestnik of Samara State Technical University. Technical Sciences Series*, 2023, no. 30, pp. 49–75 (in Russ.)

8. Naumov V. N., Buinevich M.V., Strelets A.D. [Analysis of the applicability of a process approach based on graph analytics to the study of organizational systems]. *Bulletin of St. Petersburg University State Fire Service EMERCOM of Russia*, 2022, no. 3, pp. 89–101 (in Russ.)

9. Sochnev A.N. [Optimization of assembly production based on Petri net simulation]. *Bulletin of MSTU im. N.E. Bauman. Instrumentation Series*, 2021, vol. 135, no. 2, pp. 133–146 (in Russ.)

10. Sitskaya A.V., Selifanov V.V., Zvyagintseva P.A. [Information security audit issues]. *Digital Technology Security*, 2023, vol. 110, no. 3, pp. 67–82 (in Russ.)

11. ISO 19011:2018 – *Guidelines for auditing management systems*. Available at: https://pqm-online.com/assets/files/pubs/translations/std/iso-19011-2018-(rus).pdf, free (Accessed: May 20, 2024)

12. GOST R ISO/MEK 27007–2014 *Informatsionnaya tekhnologiya (IT). Metody i sredstva obespecheniya bezopasnosti. Rukovodstva po auditu sistem menedzhmenta informatsionnoi bezopasnosti* [ISO/IEC 27007–2014 Information technology (IT). Methods and means of ensuring security. Guidelines for auditing information security management systems] (in Russ.) Available at: https://internet-law.ru/gosts/gost/57828/, free (Accessed: May 19, 2024)

13. Senkiv D.A. Audit as a Means of Ensuring Information Security of Web Applications and Used Computer Systems. *American Scientific Journal*, 2020, vol. 40, no. 2, pp. 54–57.

14. *Metodicheskii dokument «Metodika otsenki ugroz bezopasnosti informatsii» (utv. Federal'noi sluzhboi po tekhnicheskomu i eksportnomu kontrolyu 5 fevralya 2021 g.).* [Methodological document «Methodology for assessing threats to information security» (approved by the Federal Service for Technical and Export Control on February 5, 2021)] (in Russ.) Available at: https://www.garant.ru/products/ipo/prime/doc/400325044/, free (Accessed: May 20, 2024).

15. Kitsios F., Chatzidimitriou E., Kamariotou M. The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector. *Sustainability*, 2023, vol. 15, no. 7, p. 5828.

16. Denisenko V.V., Goncharov A.M., Maslov I.P. [Information Security Audit of Organizations: Methods and Benefits]. *Scienceosphere*, 2023, no. 11–2, pp. 135–140 (in Russ.)

17. Shirokova S.V., Rostova O.V., Bolsunovskaya M.V., Dmitrieva L.A., Almataev T.O. Information security audit for a manufacturing company. *Information and Control Systems*, 2023, vol. 122, no. 1, pp. 41–50.

18. Sirotskii A.A., Reznichenko S.A. [Formalized Model of Audit of Organization Information Security for Compliance with Standards Requirements]. *Information Technology Security*, 2021, vol. 28, no. 3, pp. 103–117 (in Russ.)

19. [Decree of the Government of the Russian Federation of February 17, 2018 № 162 «On approval of the Rules for the implementation of state control in the field of ensuring the security of significant objects of critical information infrastructure of the Russian Federation»] (in Russ.). Available at: https://base.garant.ru/71883452/, free (Accessed: May 21, 2024).

Igor A. Ognev
Postgraduate student, Assistant
Information Security Department (IS),
Novosibirsk State Technical University (NSTU)
20, K. Marks pr., Novosibirsk, Russia, 630073
ORCID: 0000-0003-3884-7170
Phone: +7-999-465-77-31
Email: i.ognev.2016@corp.nstu.ru