Д.А. Евдокимова, А.А. Микрюков

Российский экономический университет им. Г.В. Плеханова, Москва, Россия

УДК 51-7
DOI: http://dx.doi.org/10.21686/1818-4243-2024-4-33-42

Актуальные задачи выявления недопустимых событий на объектах критической информационной инфраструктуры

Целью исследования *является разработка подхода к выявлению и обработке недопустимых событий на объектах критической информационной инфраструктуры (КИИ) на основе концепции таксономии и категоризации. Подход направлен на решение задачи повышения эффективности идентификации, классификации и управления инцидентами информационной безопасности (ИБ). В статье рассматриваются актуальные задачи обеспечения требуемого уровня защищенности КИИ и минимизации негативных последствий от инцидентов информационной безопасности, являющихся следствием недопустимых событий, идентификация которых связана со сложностью их выявления, необходимостью обработки больших объемов данных, недостаточной оперативностью обнаружения событий ИБ, а также ограничениями технологического характера.*

Актуальность выявления и классификации недопустимых событий в области информационной безопасности, особенно для объектов КИИ обусловлена необходимостью своевременного выявления и реагирования на инциденты, которые могут привести к негативным последствиям. Понимание природы и характеристик таких событий позволяет эффективно обеспечить защиту систем и предотвратить существенный ущерб.

С целью повышения эффективности обеспечения результативной безопасности требуется выявлять класс недопустимых событий среди множества событий информационной безопасности с учетом признаков, которыми характеризуются недопустимые события.

Новизна предлагаемого подхода заключается в решении задачи выявления класса недопустимых событий информационной безопасности на основе методов таксономии, предусматривающих использование инструментов категоризации событий с использованием атрибутов недопустимых событий.

Материалы и методы исследования. *Для решения поставленной задачи использован подход к выявлению недопустимых событий на объектах КИИ, основанный на принципах таксономии событий информационной безопасности. Показано, что выявление недопустимых событий информационной безопасности напрямую связано с решением задачи поиска и анализа их атрибутов, которые представляют собой характеристики или параметры, используемые для описания и классификации инцидентов безопасности. На основе ключевых принципов таксономии разработана модель структуры множества недопустимых событий для определения признаков, которые могут положены в основу классификации недопустимых событий. Процесс выявления недопустимых событий информационной безопасности включает цепочку этапов: таксономию, категорирование и классификация, на каждом из которых реализуются соответствующие методы и инструменты.*

Результаты: *Проанализированы подходы к выявлению недопустимых событий на объектах КИИ. Рассмотрены проблемы, связанные с большим объемом данных, сложностью обработки событий, достаточно длительным временем их обнаружения и ограничениями технологических решений. Показано, что концепция таксономии и категоризации позволяет эффективно идентифицировать и классифицировать инциденты информационной безопасности, обеспечивая эффективные процессы обработки и реагирования на них. Обоснована целесообразность применения таксономии для описания и идентификации атрибутов недопустимых событий, что способствует разработке эффективных стратегий защиты и обеспечивает повышение уровня безопасности. Предложена обобщенная схема обработки недопустимых событий, включающая совокупность взаимосвязанных этапов идентификации, категоризации, оценки влияния, реагирования, документирования и анализа. Разработан алгоритм структурированного описания и классификации инцидентов, что позволяет более точно и оперативно реагировать на угрозы информационной безопасности.*

Заключение: *Полученные результаты позволяют повысить эффективность решения задачи классификации инцидентов информационной безопасности за счет идентификации недопустимых событий, что позволяет снизить уровень негативных последствий инцидентов и повысить безопасность объектов КИИ.*

Ключевые слова: *Критическая информационная инфраструктура, недопустимые события, таксономия, классификация инцидентов, категоризация событий, реагирование на инциденты информационной безопасности.*

Darya A. Evdokimova, Andrei A. Mikryukov

Plekhanov Russian University of Economics, Moscow, Russia

Current Tasks in Identifying Invalid Events in Critical Information Infrastructure

The purpose of the study *is to develop an approach for identifying and processing invalid events in critical information infrastructure (CII) based on the concepts of taxonomy and categorization. The approach aims to improve the efficiency of identifying, classifying, and managing information security (IS) incidents. The article addresses the current tasks of ensuring the required level of CII protection and minimizing the negative consequences of information security incidents resulting from invalid events. The identification of these events is associated with the complexity of detecting such events, the need to process large volumes of data, insufficient speed in detecting IS events, as well as technological limitations.*

The relevance of identifying and classifying invalid events in information security, especially for CII, is driven by the need for timely detection and response to incidents that could lead to negative consequences. Understanding the nature and characteristics of such events allows for effective system protection and prevention of significant damage. To enhance the effectiveness of ensuring security, it is necessary to identify the class of invalid events among the numerous information

security events by considering the characteristics that define invalid events.

The novelty of the proposed approach lies in solving the task of identifying the class of invalid information security events based on taxonomy methods, involving the use of event categorization tools with the attributes of invalid events.

Materials and methods. *The approach to identifying invalid events in CII, based on the principles of information security event taxonomy, was used to solve the task. It was shown that identifying invalid information security events is directly related to solving the problem of searching for and analyzing their attributes, which represent the characteristics or parameters used to describe and classify security incidents. Based on the key principles of taxonomy, a model of the structure of the set of invalid events was developed to determine the characteristics that can be the basis for classifying invalid events. The process of identifying invalid information security events includes a sequence of stages: taxonomy, categorization, and classification, with appropriate methods and tools implemented at each stage.*

Results. *Approaches to identifying invalid events in CII have been analyzed. Problems related to large data volumes, the complexity of event processing, the considerable time required for their detection, and technological limitations were considered. It was shown that the concept of taxonomy and categorization allows for effective identification and classification of information security incidents, ensuring efficient processing and response. The feasibility of applying taxonomy for describing and identifying the attributes of invalid events was justified, contributing to the development of effective protection strategies and improving security levels. A generalized scheme for processing invalid events was proposed, including a set of interconnected stages of identification, categorization, impact assessment, response, documentation, and analysis. An algorithm for structured description and classification of incidents was developed, allowing for more accurate and timely responses to information security threats.*

Conclusion. *The results obtained increase the effectiveness of solving the task of classifying information security incidents by identifying invalid events, which reduces the level of negative consequences of incidents and enhances the security of CII objects.*

Keywords: *critical information infrastructure, invalid events, taxonomy, incident classification, event categorization, information security incident response.*

Введение

Выявление недопустимых событий информационной безопасности представляет собой сложную задачу из-за существующих проблем, связанных с большим объемом данных, сложностью событий, недостаточной оперативностью обнаружения и ограничениями технологических решений. Ключевым аспектом решения задачи идентификации недопустимых событий информационной безопасности является выявление их атрибутов, обеспечивающих решение задачи классификации, на основе которой реализуется эффективная стратегия обнаружения и реагирования на возникновение недопустимых событий.

Таким образом, задача выявления недопустимых событий информационной безопасности имеет решающее значение для обеспечения информационной безопасности организации и защите объектов КИИ.

В работе предложен подход к выявлению недопустимых событий на объектах КИИ, основанный на принципах таксономии событий информационной безопасности.

Разработка обобщенного алгоритма обработки недопустимых событий

Согласно ГОСТ Р 59548—2022 [3] событие безопасности представляет собой «зафиксированное в обрабатываемом виде состояние информационной (автоматизированной) системы, сетевого, телекоммуникационного, коммуникационного, иного прикладного сервиса или информационно-телекоммуникационной сети, указывающее на возможное нарушение целостности, доступности и (или) конфиденциальности информации, а также на сбой в работе средства защиты/обработки информации или иную ситуацию, которая может быть значимой для безопасности информации».

Термин недопустимое событие информационной безопасности предложен компанией Positive Technologies, одной из ведущих компаний в области информационной безопасности России, и достаточно активно используется в современных статьях и аналитических материалах. В методических материалах компании дается определение понятию недопустимое событие: «Недопустимое событие — событие в результате кибератаки, делающее невозможным достижение операционных и (или) стратегических целей организации или приводящее к значительному нарушению ее основной деятельности» [4]. В нормативно-правовой базе Российской Федерации такой термин не применяется.

Процесс выявления и обработки недопустимых событий в соответствии с методикой, представленной в [4] включает следующие этапы:

1. Определение недопустимых для организации событий.
2. Моделирование сценариев реализации недопустимых событий.
3. Определение критериев реализации недопустимых событий

Рассмотренный подход соответствует алгоритму действий по оценке угроз безопасности информации, представленному в Методике оценки угроз безопасности ФСТЭК России (далее – Методика ФСТЭК) [5]. В Методике ФСТЭК применяется термин «негативные последствия», которые напрямую связаны с наступлением недопустимых событий. На рисунке 1 представлены этапы оценки угроз безопасности информации в соответствии с [5].

Согласно пункту 1.3 Методики ФСТЭК она применяется для определения угроз безопасности информации на значимых объектах КИИ.

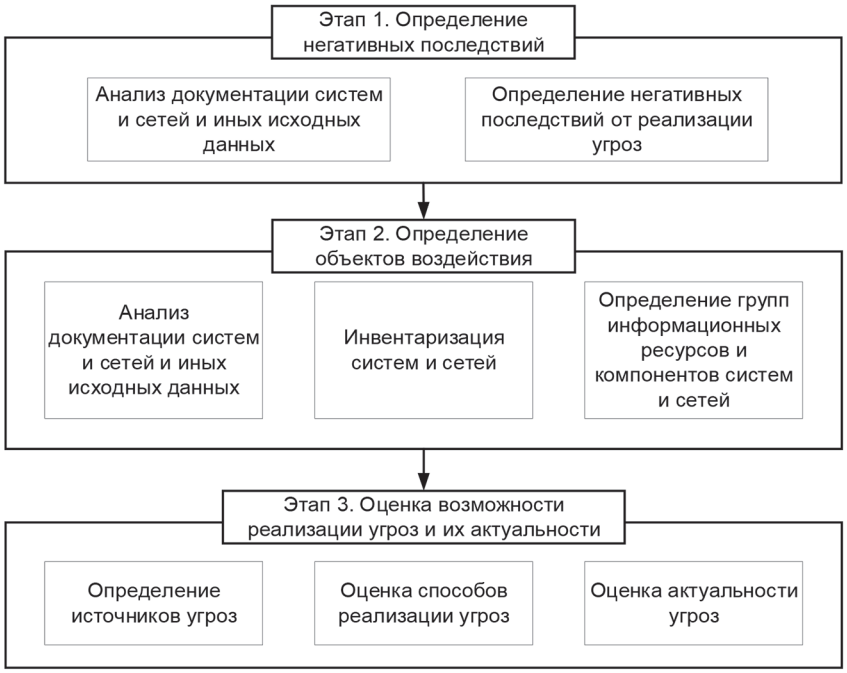

Рис. 1. Этапы оценки угроз безопасности информации [5]

Fig. 1. Stages of Information Security Threat Assessment [5]

Таблица 1 (Table 1)

Соотношение негативных последствий и недопустимых событий

Ratio of negative consequences and invalid events

№ п/п	Пример недопустимого события	Пример негативного последствия
1.	Остановка производственного процесса	Н.14 Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса.
2.	Кража денег со счета компании	Н.10 Потеря (хищение) денежных средств
3.	Срыв контрактных обязательств по поставке товара	Н.24 Неспособность выполнения договорных обязательств
4.	Утечка персональных данных клиентов	Н.7 Нарушение конфиденциальности (утечка) персональных данных.
5.	Разлив нефтепродукта	Н.41 Вредные воздействия на окружающую среду

Первоочередным этапом в оценке угроз безопасности информации является определение негативных последствий. В перечне негативных последствий [6] находятся последствия, напрямую связанные с объектами КИИ. Например, негативные последствия, обозначенные как: Н.31 – Н.41, относятся к критериям значимости объектов КИИ Российской Федерации.

В соответствии с Методикой ФСТЭК необходимо произвести инвентаризацию информационных активов, определить источники угроз безопасности информации и оценить возможность реализации сценариев реализации угроз безопасности информации. То есть, этапы Методики ФСТЭК соответствуют этапам методики определения недопустимых событий, сценариев и критериев их реализации компании «Positive Technology» В табл. 1 показана взаимосвязь понятий «недопустимые события» и «негативные последствия», и примеры их реализации.

Таким образом, понятия «недопустимое событие» и «негативное последствие» достаточно близки по смысловому содержанию и имеют причинно-следственную связь: недопустимое событие приводит к негативному последствию, то есть для предотвращения негативного последствия необходимо исключить проявление недопустимого события, а значит задача выявления возможности недопустимого события и реализация препятствующих этому мероприятий обеспечит повышение эффективности системы безопасности объектов КИИ.

Процесс выявления недопустимых событий информационной безопасности напрямую связан с решением задачи поиска и анализа атрибутов недопустимых событий. Атрибуты недопустимых событий информационной безопасности представляют собой характеристики или параметры, которые используются для описания и классификации инцидентов безопасности, и могут быть выявлены в результате наблюдения и анализа процессов, происходящих в системе.

На основе ключевых принципов таксономии разработана теоретическая модель структуры полного множества недопустимых событий для определения признаков, которые могут положены в основу классификации недопустимых событий информационной безопасности. Цепочка этапов по выявлению недопустимых событий информационной безопасности включает три основных шага: таксономия, категорирование и классификация. На каждом из них реализуются соответствующие методы и инструменты.

Таксономия подразумевает под собой процесс определения и создания структурированной системы для описания и систематизации различных видов событий, в том числе инцидентов, информационной безопасности. Одним из

способов реализации является создание структурированной иерархии, а именно разработка дерева таксономии, включающего категории и подкатегории инцидентов информационной безопасности.

На рисунке 2 представлен пример построения дерева таксономии негативного последствия, характерного для объекта КИИ «Н.14 Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса».

Дерево таксономии описывает различные виды событий, которые могут привести к нарушению штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса. В дереве выделены три основные категории: нарушение целостности, нарушение доступности и внутренние угрозы. Каждая из этих категорий имеет подкатегории, описывающие более конкретные виды нарушений.

Согласно статье 1 Федерального закона № 187-ФЗ [1] основная цель защиты критической информационной инфраструктуры – обеспечить ее устойчивое функционирование при проведении в отношении ее компьютерных атак, следовательно актуальными негативными событиями будут являться нарушение целостности и доступности. Такое свойство, как конфиденциальность, в данном случае не будет являться актуальным негативным событием. Важно отметить, что рассматриваемая в данном примере автоматизированная система управления является изолированным объектом информатизации, не подверженная внешним воздействиям.

На следующем этапе реализуется процедура категорирования, которая представляет собой процесс распределения инцидентов информационной

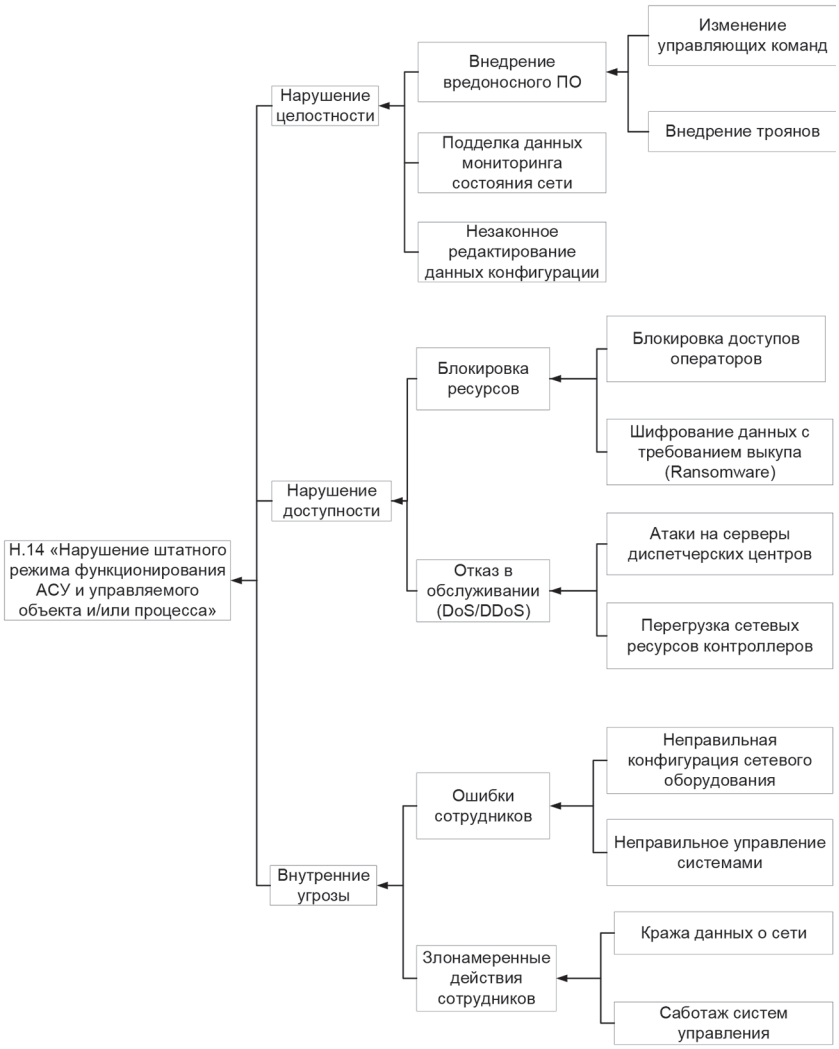

Рис. 2. Дерево таксономии для недопустимого события Н.14
Fig. 2. Taxonomy tree for an invalid H.14 event

безопасности по основным категориям, определенным на этапе таксономии. Данная процедура обеспечивает структурирование данных и упрощает управление инцидентами. Для подготовки к реализации этапа категорирования проводятся следующие мероприятия, описанные как в законодательных требованиях [1, 5], международных стандартах [2], так и в практических руководствах и исследованиях по управлению инцидентами информационной безопасности [7]:

1. Определение критериев. Установление четких критериев для каждой категории, таких как источник угрозы, вектор атаки, цели и последствия.

2. Автоматизация процесса. Настройка систем управления инцидентами (SIEM) для автоматического категорирования инцидентов информационной безопасности на основе установленных правил.

3. Обучение персонала. Проведение тренингов для сотрудников по правильной идентификации и категорированию инцидентов информационной безопасности.

Этап категорирования включает решение задачи распределения инцидентов по основным категориям, которые были определены на этапе таксономии. Категорирование инцидента информационной безопасности включает решение двух взаимосвязанных задач:

1. Определение категории инцидента. На основе описания инцидента определяется

основная категория. В рассматриваемом случае, нарушение штатного режима функционирования автоматизированной системы управления (АСУ) может касаться нескольких основных категорий, таких как нарушение целостности, нарушение доступности или внутренние угрозы.

2. Анализ деталей инцидента. Проанализировать контекст и детали инцидента для более точного определения подкатегории. Рассмотреть возможные причины и последствия нарушения режима работы АСУ.

Ниже приведен результат проведения категорирования инцидента информационной безопасности «Н.14 Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса».

Категория: Нарушение целостности.

Описание: Внедрение вредоносного программного обеспечения, изменившего конфигурацию АСУ, что привело к нарушению штатного режима функционирования системы и управляемого объекта.

Этап категорирования инцидентов информационной безопасности заключается в точном определении категории и подкатегории на основе подробного анализа инцидента. Это обеспечивает структурирование данных и упрощение процесса управления инцидентами.

Завершающим этапом является классификация инцидентов информационной безопасности. Детальное представление инцидентов информационной безопасности в рамках каждой категории, включающее специфические типы угроз и их характеристики. Существуют следующие способы реализации данного этапа [7-9]:

1. Разработка матриц классификации. Создание матриц, которые обеспечивают классификацию инцидентов информационной безопасности по совокупности параметров (тип угрозы, источник, метод, последствия).

2. Анализ данных. Применение аналитических инструментов для выявления паттернов и закономерностей в инцидентах информационной безопасности. Использование программного обеспечения для анализа больших данных (Big Data) для обнаружения трендов и аномалий, что позволяет предсказать и предотвратить будущие инциденты.

3. Внедрение систем машинного обучения. Обучение алгоритмов для автоматической классификации инцидентов информационной безопасности на основе исторических данных. Модель машинного обучения, обученная на основе исторических данных об инцидентах, может автоматически классифицировать новые инциденты, выявлять потенциальные угрозы и предлагать меры реагирования.

Ниже приведен результат проведения классификации инцидента информационной безопасности «Н.14 Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса»:

1. Причина инцидента: внешняя атака.

2. Тип инцидента: нарушение целостности данных.

3. Последствия инцидента: остановка или сбой в работе системы управления, нарушение технологического процесса.

4. Уровень критичности: высокий.

5. Вектор атаки: сетевая атака.

6. Средство атаки: вредоносное программное обеспечение.

Таблица 2 (Table 2)

Атрибуты недопустимых событий информационной безопасности
Attributes of invalid information security events

№ п/п	Класс атрибутов	Подкласс атрибутов
1	Причина недопустимого события	Внешние причины
		Внутренние причины
2	Тип недопустимого события	Нарушение конфиденциальности
		Нарушение целостности
		Нарушение целостности
3	Последствия недопустимого события	Экономические последствия
		Операционные последствия
		Репутационные последствия
4	Уровень критичности недопустимого события	Низкий
		Средний
		Высокий
5	Вектор атаки недопустимого события	Сетевая атака
		Локальная атака
		Социальная инженерия
6	Средство атаки недопустимого события	Вредоносное ПО
		Сетевые атаки
		Физическое повреждение
7	Время обнаружения недопустимого события	Мгновенное обнаружение
		Отложенное обнаружение
8	Продолжительность недопустимого события	Краткосрочный
		Долгосрочный
9	Целевые компоненты воздействия недопустимого события	Серверы
		Рабочие станции
		Сетевое оборудование
		Программное обеспечение
10	Методы восстановления после недопустимого события	Резервное копирование и восстановление данных
		Исправление уязвимостей
		Обновление и патчинг систем
		Обучение сотрудников

Таблица 3 (Table 3)

Перечень атрибутов недопустимого события информационной безопасности H.14

List of attributes of invalid information security event H.14

№ п/п	Класс атрибутов	Подкласс атрибутов
1	Причина недопустимого события	Внешняя атака (кибератака)
2	Тип недопустимого события	Нарушение целостности
3	Последствия недопустимого события	Экономические последствия
		Операционные последствия
		Репутационные последствия
4	Уровень критичности недопустимого события	Высокий
5	Вектор атаки недопустимого события	Сетевая атака
6	Средство атаки недопустимого события	Вредоносное ПО
7	Время обнаружения недопустимого события	Отложенное обнаружение
8	Продолжительность недопустимого события	Долгосрочный
9	Целевые компоненты воздействия недопустимого события	Серверы
		Рабочие станции
10	Методы восстановления после недопустимого события	Резервное копирование и восстановление данных
		Исправление уязвимостей
		Обновление и патчинг систем
		Обучение сотрудников

Таблица (4 Table 4)

Результаты оценки взаимосвязей недопустимого события информационной безопасности H.14 с угрозами БДУ ФСТЭК России

Results of evaluation of interrelationships of the invalid information security event H.14 with threats of the Threats Data Bank of the Federal Service for Technical and Export Control of Russia

№ п/п	Шаги процесса оценки взаимосвязи	Описание
1	Идентификация недопустимого события:	Нарушение штатного режима функционирования автоматизированной системы управления (АСУ) и управляемого объекта и/или процесса.
2	Категоризация недопустимого события	Нарушение целостности и доступности данных и систем. Подкатегории: a. Изменение конфигурации системы; b. Остановка или сбой в работе системы управления; c. Нарушение технологического процесса.
2	Категоризация недопустимого события	Нарушение целостности и доступности данных и систем.
3	Сопоставление недопустимого события угрозам из БДУ ФСТЭК России	Актуальные угрозы для рассматриваемого недопустимого события: 1. УБИ.001: Угроза вредоносного программного обеспечения (Malware); 2. УБИ.002: Угроза отказа в обслуживании (DoS/DDoS);
		3. УБИ.003: Внутренние угрозы, связанные с действиями сотрудников; 4. УБИ.004: Угроза утечки конфиденциальной информации.
4	Анализ потенциальных негативных последствий.	Результаты анализа потенциальных негативных последствий представлены в табл. 5.

Процесс классификации инцидента информационной безопасности включает в себя анализ и систематизацию различных аспектов инцидента, таких как причина, тип, последствия, уровень критичности и метод атаки.

Таким образом, применение вышеуказанной цепочки этапов структурирует подход к управлению инцидентами информационной безопасности, а также обеспечивает их обнаружение, анализ и выработку мероприятий по реагированию, в том числе обеспечивает описание атрибутов недопустимых событий.

В ГОСТ Р 59548—2022 [3] представлены требования к регистрируемой информации о событии информационной безопасности, которая используется при описании таксономии. На основе методов классификации и категоризации событий информационной безопасности выявлены атрибуты недопустимых событий информационной безопасности, представленные в табл. 2.

В табл. 3 представлен перечень выявленных атрибутов недопустимого события «H.14 Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса» (далее – H.14).

Идентификация атрибутов недопустимых событий информационной безопасности позволяют структурировать и систематизировать инциденты с целью более эффективного управления и реализации наиболее эффективного сценария реагирования. Процесс оценки взаимосвязей недопустимых событий с соответствующими угрозами из банка данных угроз безопасности информации ФСТЭК России, которые могут привести к негативным последствиям, включает следующие шаги:

1. Идентификация недопустимого события.

2. Категоризация недопустимого события.

3. Сопоставление недопустимого события с угрозами из банка данных угроз (БДУ) безопасности информации ФСТЭК России.

4. Анализ потенциальных негативных последствий.

Результаты реализации перечисленных шагов применительно к недопустимому событию Н.14 представлены в табл. 4.

В табл. 5 представлены потенциальные негативные последствия для каждой из актуальных угроз.

Таким, образом полученные результаты обеспечивают более эффективную обработку рисков, а также оперативную разработку и реализацию эффективных сценариев реагирования на недопустимые события информационной безопасности.

На основе проведенного анализа разработан обобщенный алгоритм обработки недопустимых событий информационной безопасности, который обеспечивает снижение уровня негативных последствий (рисунок 3).

На первом этапе Обнаружения и идентификации и недопустимого события проводится мониторинг систем и сетей с помощью систем обнаружения и предотвращения вторжений (IDS и IPS). Анализируются логи и события безопасности, а также принимаются сообщения о подозрительной активности от сотрудников или автоматизированных систем.

На втором этапе Категоризации и классификации недопустимых событий осуществляется определение типа недопустимого события (конфиденциальность, целостность, доступность). Далее проводится классификация события по критичности и сопоставление с угрозами из банка данных угроз безопасности информации ФСТЭК России.

Третий этап Анализа и оценки влияния недопустимого события включает анализ методов и средств атаки, опре-

Таблица 5 (Table 5)

Негативные последствия недопустимого события информационной безопасности Н.14

Negative consequences of an invalid information security event H.14

№ п/п	Угроза безопасности информации	Негативные последствия
1	УБИ.001: Угроза вредоносного программного обеспечения (Malware)	Нарушение конфигурации системы
		Остановка технологического процесса
		Финансовые убытки из-за простоев
2	УБИ.002: Угроза отказа в обслуживании (DoS/DDoS)	Перегрузка и сбои в работе автоматизированной системы управления
		Потеря доступности систем
		Нарушение технологического процесса
3	УБИ.003: Внутренние угрозы, связанные с действиями сотрудников	Ошибки конфигурации, приводящие к сбоям
		Злонамеренные действия, остановка системы
		Нарушение технологического процесса
4	УБИ.004: Угроза утечки конфиденциальной информации	Использование утекшей информации для атак
		Нарушение работы системы управления
		Финансовые и репутационные убытки

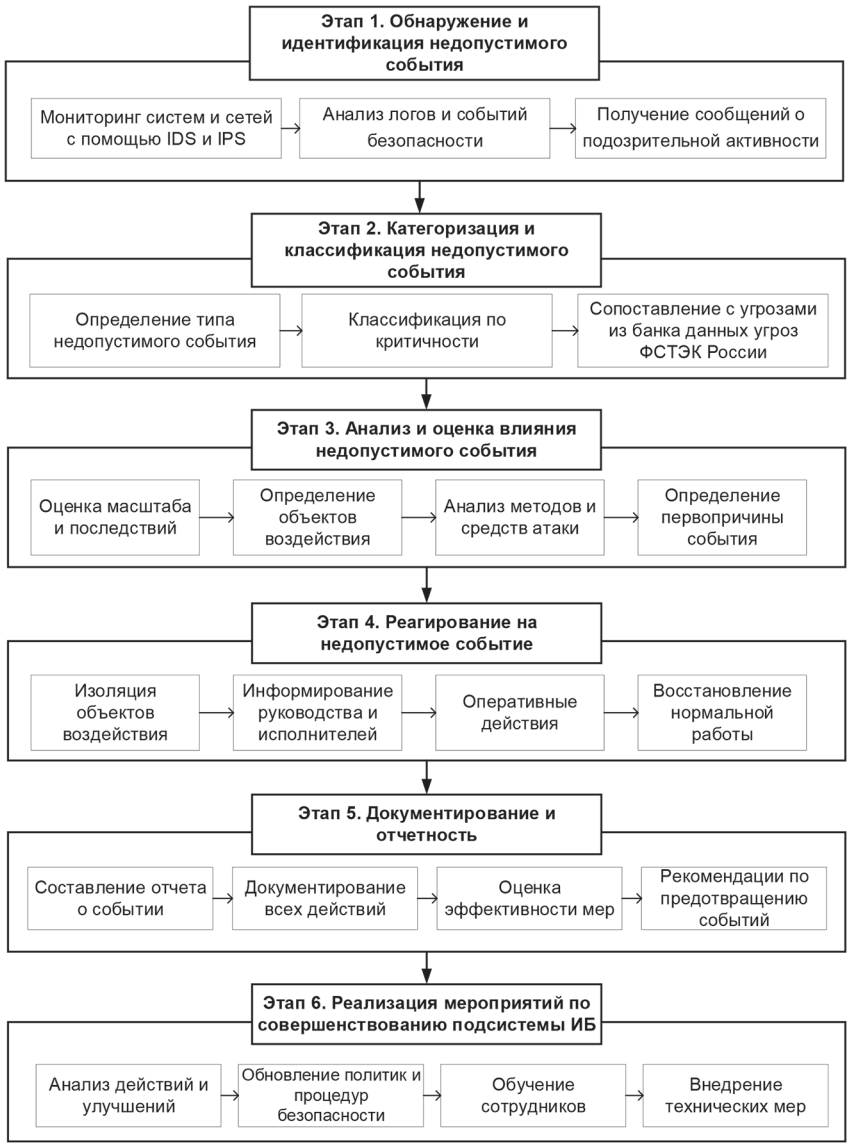

Рис. 3. Обобщенный алгоритм обработки недопустимых событий

Fig. 3. Generalized algorithm for processing invalid events

деление первопричины события и объектов воздействия, а также оценку масштаба и потенциальных последствий недопустимого события.

На четвертом этапе Реагирования на недопустимое событие проводится изоляция объектов воздействия для предотвращения распространения угрозы, информирование руководства организации и исполнителей, выполнение оперативных действий по устранению угрозы (например, удаление вредоносного ПО, применение патчей), и восстановление нормальной работы систем.

Пятый этап Документирование и отчетность включает составление детализированного отчета о недопустимом событии, документирование всех действий, предпринятых для устранения события, оценку эффективности принятых мер и выработку рекомендаций по предотвращению аналогичных событий в будущем.

На заключительном шестом этапе Реализации мероприятий по совершенствованию подсистемы ИБ проводится анализ действий и улучшений, обновление политик и процедур безопасности, обучение сотрудников на основе полученных данных и внедрение технических и организационных мер для предотвращения повторных недопустимых событий.

Разработанный обобщенный алгоритм обеспечивает комплексный подход к управлению инцидентами информационной безопасности, охватывающий все этапы от выявления недопустимого события до проведения его анализа и выработки необходимых мероприятий по повышению уровня информационной безопасности. Предложенный подход позволяет фокусироваться на мероприятиях по противодействию таким угрозам нарушителя, реализация которых может привести к наиболее тяжелым последствиям для КИИ.

Проведен сравнительный анализ предложенного подхода на основе разработанного обобщенного алгоритма с существующими известными подходами такими, как Методика ФСТЭК [5], Методика MITRE&ATTACK Framework [10] и Методика оценки угроз безопасности по таксономии инцидентов Ховарда-Лонгстаффа [11].

Предложенный подход имеет схожесть с Методикой ФСТЭК в части реализации этапов идентификации, анализа и реагирования на инциденты. В Методике ФСТЭК предусмотрено разделение угроз на актуальные и возможные, однако не обеспечивается определение ущерба от последствий угроз. Предложенный подход в отличие от Методики ФСТЭК имеет более гибкие возможности по выявлению и реагированию на недопустимые события и возможности выработки необходимых мероприятий по снижению степени негативных последствий при выявлении недопустимых событий.

Предложенный подход как и в Методике MITRE&ATTACK Framework использует возможности методов таксо-

Таблица 6 (Table 6)

Результаты реализации обобщенного алгоритма для недопустимого события информационной безопасности H.14

Results of implementation of the generalized algorithm for invalid information security event H.14

№ п/п	Наименование этапа	Описание этапа
1	Обнаружение и идентификация недопустимого события	Фиксация системой IDS аномальной активности на сервере управления
		Передача сообщения о нестабильной работе системы
2	Категоризация и классификация недопустимого события	Тип: Нарушение целостности
		Критичность: Высокая
		Угроза из банка данных угроз безопасности информации ФСТЭК России: Вредоносное ПО (УБИ.001).
3	Анализ и оценка влияния	Объекты воздействия: Серверы управления, рабочие станции операторов
		Последствия: Остановка технологического процесса, финансовые убытки.
		Метод атаки: Воздействие вредоносного ПО через уязвимость в сетевом протоколе
4	Реагирование на недопустимое событие	Изоляция объектов воздействия
		Информирование руководства и исполнителей
		Удаление вредоносного ПО, установка обновлений
		Восстановление нормальной работы автоматизированной системы управления
5	Документирование и отчетность	Составление отчета об инциденте, включая все предпринятые меры
		Оценка эффективности удаления вредоносного ПО
		Рекомендации по улучшению сетевой безопасности
6	Реализация мероприятий по совершенствованию подсистемы ИБ	Анализ действий команды реагирования
		Обновление процедур и политик безопасности
		Проведение обучения сотрудников по выявлению и предотвращению угроз.
		Внедрение новых средств защиты для предотвращения аналогичных атак.

номии и категоризации инцидентов ИБ, но Методика MITRE&ATTACK Framework не предусматривает идентификацию недопустимых событий и соответствующих им техник и тактик нарушителя.

Таксономия инцидентов Ховарда-Лонгстаффа использует набор из семи характеристик, на основе которых проводится анализ угроз безопасности информации: Атакующий, Средства. Уязвимости, Действия, Объекты воздействия, Результат несанкционированных действий и Цели. Методика оценки угроз безопасности по таксономии инцидентов Ховарда-Лонгстаффа обеспечивает эффективное категорирование угроз, но не связывает их с классом недопустимых событий.

Таким образом, предложенный комплексный подход, включает обобщенный алгоритм обработки недопустимых событий, обеспечивающий их обработку от этапа выявления до анализа и реагирования, а также улучшения процессов и процедур обеспечения результативной безопасности.

Разработанный обобщенный алгоритм обработки недопустимых событий информационной безопасности обеспечивает структурированный и систематизированный подход к управлению недопустимыми событиями, а также в целом обеспечивает повышение устойчивости КИИ к воздействию угроз.

Результаты реализации разработанного обобщенного алгоритма рассмотрены на примере недопустимого события «Н.14 Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса» и представлены в табл. 6.

Предложенный алгоритм направлен на создание целостного подхода к управлению инцидентами информационной безопасности в части выявления недопустимых событий, что обеспечивает эффективное реагирование на инциденты и результативную безопасность объектов КИИ.

Заключение

По результатам проведенного исследования можно сделать следующие выводы. Проанализированы подходы к выявлению недопустимых событий на объектах КИИ, включая существующие методики и технологии. Рассмотрены проблемы и сложности, связанные с большим объемом данных, сложностью событий, недостаточной оперативностью обнаружения и реагирования, а также ограничениями технологических решений.

Обоснована необходимость применения методов идентификации атрибутов недопустимых событий информационной безопасности для обеспечения результативной безопасности.

Предложен обобщенный алгоритм выявления и обработки недопустимых событий информационной безопасности, включающий этапы идентификации, категоризации, оценки влияния, реагирования, документирования, анализа и мероприятий, направленных на совершенствование подсистемы информационной безопасности.

Разработанный алгоритм выявления и обработки недопустимых событий информационной безопасности на основе принципов таксономии и категоризации включает обоснование и построение структурированной системы для описания инцидентов, их категоризацию и классификацию, что позволяет более эффективно реагировать на угрозы информационной безопасности.

Полученные результаты позволяют повысить эффективность идентификации и классификации инцидентов информационной безопасности за счет выявления и описания атрибутов недопустимых событий, что обеспечивает снижение уровня негативных последствий нарушения информационной безопасности на объектах КИИ.

Литература

1. Федеральный закон от 26 июля 2017 г. № 187-ФЗ (ред. от 10 июля 2023 г.) «О безопасности критической информационной инфраструктуры Российской Федерации».

2. ISO/IEC 27035-1:2016 Information technology – Security techniques – Information security incident management – Part 1: Principles of incident management. International Organization for Standardization, 2016.

3. ГОСТ Р 59548—2022 «Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации».

4. Методика определения недопустимых событий, сценариев и критериев их реализации компании «Positive Technology» [Электрон. ресурс]. Режим доступа: https://www.ptsecurity.com/upload/corporate/ru-ru/webinars/ics/metodika-opredeleniya-ns.pdf (Дата обращения: 10.05.2024).

5. Методика оценки угроз безопасности ФСТЭК России [Электрон. ресурс]. Режим доступа: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g (Дата обращения: 10.05.2024).

6. Перечень негативных последствий из нового раздела банка данных угроз ФСТЭК России [Электрон. ресурс]. Режим доступа: https://bdu.fstec.ru/threat-section/negatives (Дата обращения: 10.05.2024).

7. «Security Information and Event Management (SIEM) Implementation». Author: David Miller, 2010.

8. NIST Special Publication 800-61 Revision 2, «Computer Security Incident Handling Guide». National Institute of Standards and Technology, 2012.

9. «Data-Driven Security: Analysis, Visualization and Dashboards». Authors: Jay Jacobs, Bob Rudis, 2014.

10. MITRE ATT&CK Framework. [Электрон. ресурс]. Режим доступа: https://attack.mitre.org/ (Дата обращения: 10.07.2024).

11. Howard J. D., Longstaff T. A. A Common Language for Computer Security Incidents. Sandia National Laboratories [Электрон. ресурс]. 1998. Режим доступа: https://www.sandia.gov/app/uploads/sites/51/2021/05/SAND98-8667.pdf (Дата обращения: 10.07.2024).

References

1. Federal Law of July 26, 2017 N 187-FZ (as amended on July 10, 2023) «On the Security of Critical Information Infrastructure of the Russian Federation». (In Russ.)

2. ISO/IEC 27035-1:2016 Information technology — Security techniques — Information security incident management – Part 1: Principles of incident management. International Organization for Standardization; 2016.

3. GOST R 59548 - 2022 «Information protection. Registration of security events. Requirements for registered information». (In Russ.)

4. Metodika opredeleniya nedopustimykh sobytiy, stsenariyev i kriteriyev ikh realizatsii kompanii «Positive Technology» = Methodology for determining unacceptable events, scenarios and criteria for their implementation by Positive Technology [Internet]. Available from: https://www.ptsecurity.com/upload/corporate/ru-ru/webinars/ics/metodika-opredeleniya-ns.pdf (cited 10.05.2024). (In Russ.)

5. Metodika otsenki ugroz bezopasnosti FSTEK Rossii = Methodology for assessing security threats of the FSTEC of Russia [Internet]. Available from: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g (cited 10.05.2024). (In Russ.)

6. Perechen' negativnykh posledstviy iz novogo razdela banka dannykh ugroz FSTEK Rossii = List of negative consequences from the new section of the FSTEC of Russia threat database [Internet]. Available from: https://bdu.fstec.ru/threat-section/negatives (cited 10.05.2024). (In Russ.)

7. «Security Information and Event Management (SIEM) Implementation». Author: David Miller; 2010.

8. NIST Special Publication 800-61 Revision 2, «Computer Security Incident Handling Guide». National Institute of Standards and Technology; 2012.

9. «Data-Driven Security: Analysis, Visualization and Dashboards». Authors: Jay Jacobs, Bob Rudis; 2014.

10. MITRE ATT&CK Framework. [Internet]. Available from: https://attack.mitre.org/ (cited 10.07.2024).

11. Howard J. D., Longstaff T. A. A Common Language for Computer Security Incidents. Sandia National Laboratories [Internet]. 1998. Available from: https://www.sandia.gov/app/uploads/sites/51/2021/05/SAND98-8667.pdf (cited 10.07.2024).

Сведения об авторах

Дарья Александровна Евдокимова
Российский экономический университет им. Г.В. Плеханова, Москва, Россия
Эл. почта: Evdokimova.DA@rea.ru

Андрей Александрович Микрюков
Российский экономический университет им. Г.В. Плеханова, Москва, Россия
Эл. почта: mikrukov.aa@rea.ru

Information about the authors

Daria A. Evdokimova
Plekhanov Russian University of Economics, Moscow, Russia
E-mail: Evdokimova.DA@rea.ru

Andrey A. Mikryukov
Plekhanov Russian University of Economics, Moscow, Russia
E-mail: mikrukov.aa@rea.ru